IBM Cloud Application Performance Management
Juin 2019

Guide d'utilisation

Remarque

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant dans la rubrique «Remarques», à la page 1555.

Cette édition s'applique à la version de juin 2019 de IBM® Cloud Application Performance Management et à toutes les éditions et modifications ultérieures jusqu'à indication contraire dans les nouvelles éditions.

Table des matières

Chapitre 1. Nouveautés..... 1

Chapitre 2. Documentation au format PDF.....43

Chapitre 3. Présentation du produit..... 45
Présentation de l'architecture.....45
Interface utilisateur.....47
Offres et modules complémentaires.....47
Détails d'offre..... 50
Agents et collecteurs de données.....52
Historique des modifications..... 53
Fonctions..... 55
Descriptions.....59
Fonctions.....73
Intégration 81
Documentation..... 82
Conventions utilisées dans la documentation.....83

Chapitre 4. Planification du déploiement.....85
Configuration requise..... 85
Ports par défaut utilisés par les agents et collecteurs de données.....85
Scénarios.....90
Scénario : Surveillance d'IBM API Connect.....90
Scénario : Surveillance de la Liste d'applications Java IBM 91
Scénario : Surveillance de la Pile d'intégration IBM..... 99
Téléchargement de vos agents et de vos collecteurs de données..... 105
Tutoriel : Téléchargement et installation d'un agent.....106
Tutoriel : Téléchargement et configuration d'un collecteur de données..... 110

Chapitre 5. Déploiement d'agents et de collecteurs de données..... 115

Chapitre 6. Installation des agents.....123
Installation des agents sur les systèmes UNIX.....124
Préinstallation sur les systèmes AIX.....125
Préinstallation sur les systèmes Solaris.....127
Installation d'agents..... 128
Installation des agents sur les systèmes Linux.....130
Préinstallation sur les systèmes Linux..... 132
Installation d'agents..... 137
Installation des agents sur les systèmes Windows.....139
Préinstallation sur les systèmes Windows.....140
Installation d'agents..... 142
Installation des agents en tant qu'utilisateur non superutilisateur.....145
Sécurisation des fichiers d'installation de l'agent..... 146
Installation des agents en mode silencieux..... 147
Contournement de l'analyse des prérequis.....149
Désinstallation de vos agents.....150
Agent WebSphere Applications : Annulation de la configuration du collecteur de données..... 152
Agent Node.js : Retrait du plug-in de surveillance.....161
agent Microsoft .NET : Retrait du collecteur de données .NET..... 162

Chapitre 7. Configuration de votre environnement..... 163
Rubriques communes.....163
Connectivité réseau..... 163
Noms de systèmes gérés.....171
Modification du nom de système géré de l'agent..... 174
Configuration d'agents.....180
Procédure générale de configuration des collecteurs de données.....189
Configuration de la surveillance d'Amazon EC2.....194
Configuration de l'agent sur des systèmes Windows..... 195
Configuration de l'agent en répondant à des invites.....198
Configuration de l'agent à l'aide du fichier de réponses silencieux..... 199
Paramètres de configuration de l'agent Amazon EC2..... 200
Configuration de la surveillance d'AWS Elastic Load Balancer.....202
Configuration de l'agent sur des systèmes Windows..... 203
Configuration de l'agent en répondant aux invites..... 204
Configuration de l'agent à l'aide du fichier de réponses silencieux..... 205
Paramètres de configuration de l'agent Amazon ELB.....207
Configuration de la surveillance Azure Compute.....207
Informations de configuration d'Azure Compute.....208
Configuration de l'agent sur des systèmes Windows..... 209
Configuration de l'agent en répondant à des invites.....211
Configuration de l'agent à l'aide du fichier de réponses silencieux..... 213
Paramètres de configuration de l'Agent Azure Compute.....215
Configuration de la surveillance de Cassandra.....217
Configuration de l'agent sur des systèmes Windows..... 218
Configuration de l'agent sur des systèmes Linux.....218
Configuration de l'agent à l'aide du fichier de réponses silencieux..... 219
Paramètres de configuration de l'agent..... 220
Configuration de la surveillance de Cisco UCS..... 220
Configuration de l'agent sur des systèmes Windows..... 221
Configuration de l'agent à l'aide du fichier de réponses silencieux..... 222
Configuration de l'agent en répondant aux invites..... 223
Paramètres de configuration de l'agent..... 224
Paramètres de configuration pour le fournisseur de données..... 225
Activation de la communication SSL avec les sources de données Cisco UCS.....225
Augmentation de la taille de segment de mémoire Java.....226
Configuration de la surveillance de Citrix Virtual Desktop Infrastructure.....227
Activation des privilèges d'administrateur en lecture seule de Citrix..... 229
Configuration de l'agent sur des systèmes Windows..... 229
Configuration de l'agent en répondant à des invites.....232
Configuration de l'agent à l'aide du fichier de réponses silencieux..... 233
Paramètres de configuration de l'agent Citrix VDI.....234
Activation de la surveillance des événements Windows et des mesures PowerShell..... 236
Configuration de la surveillance DataPower.....237
Configuration des dispositifs DataPower..... 237
Configuration de l'agent DataPower.....246
Configuration de la surveillance de Db2 249
Configuration de l'agent sur des systèmes Windows..... 251
Configuration de l'agent sur des systèmes Linux ou UNIX.....252
Configuration de l'agent à l'aide du fichier de réponses silencieux..... 253
Octroi de privilèges pour l'affichage des mesures Db2..... 255
Configuration des variables d'environnement local.....256
Prérequis pour la surveillance à distance..... 259
Configuration de la surveillance de Hadoop.....261
Configuration de l'agent sur des systèmes Windows 262
Configuration de l'agent sur des systèmes Linux et AIX.....265

Configuration de l'agent à l'aide du fichier de réponses silencieux..... 268
Configuration du tableau de bord pour visualiser des événements Hadoop..... 269
Attribution de droits aux utilisateurs non administrateurs.....270
Configuration de la surveillance de HMC Base..... 270
Configuration de la connexion SSH..... 272
Préparation du kit SDK pour HMC.....273
Configuration du serveur de la console HMC pour la surveillance des entrées-sorties virtuelles.. 274
Activation de la surveillance de l'utilisation d'UC et de mémoire..... 275
Configuration de la surveillance de HTTP Server..... 275
module IBM HTTP Server Response Time..... 277
Exemples de code pour l'agent HTTP Server..... 278
Configuration de la surveillance d'IBM Cloud.....279
Configuration de l'agent sur des systèmes Windows..... 280
Configuration de l'agent en répondant à des invites.....281
Configuration de l'agent à l'aide du fichier de réponses silencieux..... 281
Paramètres de configuration de l'agent IBM Cloud..... 283
Configuration de la surveillance d'IBM Integration Bus..... 283
Configuration de l'agent IBM Integration Bus.....284
Configuration d'IBM Integration Bus pour l'activation des données..... 288
Désactivation de la collecte de données d'image instantanée pour l'agent..... 295
Configuration du suivi des transactions pour l'agent IBM Integration Bus.....296
Spécification d'un nom de système géré unique pour agent IBM Integration Bus..... 296
Suppression de l'exit utilisateur KQIUserExit..... 298
Configuration de la surveillance d'IBM MQ Appliances.....298
Configuration de l'agent en répondant à des invites.....299
Configuration de l'agent à l'aide du fichier de réponses silencieux..... 300
Paramètres de configuration de l'Agent MQ Appliance..... 301
Configuration de la surveillance d'InfoSphere DataStage..... 304
Configuration de l'agent sur les systèmes Windows..... 304
Configuration de l'agent sur des systèmes Linux.....304
Configuration des variables d'environnement..... 305
Configuration de l'agent à l'aide du fichier de réponses silencieux..... 305
Paramètres de configuration de l'agent..... 306
Configuration d'Internet Service Monitor..... 307
Configuration d'Internet Service Monitoring par le biais de l'interface utilisateur..... 308
Configuration de l'agent sur des systèmes Windows..... 456
Activation de Netcool/OMNIbus.....460
Configuration de la surveillance de J2SE.....461
Vérification du statut du suivi des transactions et de la collecte des données de diagnostic..... 465
Changement du statut du suivi des transactions et de la collecte des données de diagnostic..... 466
Configuration de la surveillance de JBoss..... 467
Activer les connexions au serveur JMX MBean.....469
Ajouter un utilisateur de gestion de serveur JBoss..... 470
Activation de la collecte des statistiques Web/HTTP..... 471
Configuration de l'agent sur des systèmes Windows..... 472
Configuration de l'agent en répondant à des invites.....474
Configuration de l'agent à l'aide du fichier de réponses silencieux..... 475
Paramètres de configuration de l'agent JBoss..... 477
Configuration du collecteur de données de suivi des transactions de l'agent agent JBoss.....478
Configuration de la surveillance de Linux KVM.....482
Création d'un utilisateur et attribution des droits nécessaires..... 483
Configuration des protocoles.....483
Configuration d'une connexion au serveur RHEVM.....488
Configuration d'une connexion au serveur RHEVH..... 489
Paramètres de configuration pour la connexion au serveur RHEVM.....490
Paramètres de configuration pour la connexion au serveur RHEVH..... 492
Configuration de la surveillance de MariaDB.....494
Configuration de l'agent sur les systèmes Windows..... 495

Configuration de l'agent sur des systèmes Linux....496
Configuration de l'agent à l'aide du fichier de réponses silencieux.... 496
Configuration de la surveillance de Microsoft Active Directory.... 497
Exécution de l'agent Microsoft Active Directory en tant qu'administrateur.... 498
Configuration des variables d'environnement local....498
Exécution de l'agent Microsoft Active Directory en tant qu'utilisateur non-administrateur.... 500
Configuration des services de domaine pour le groupe d'attributs AD_Services_Status....503
Mise à niveau de l'agent Microsoft Active Directory.... 504
Configuration de la surveillance de Microsoft Cluster Server.... 505
Création d'une ressource de cluster de service générique sur les systèmes Windows Server 2008, 2012, 2016 et 2019 505
Configuration de l'agent à l'aide du fichier de réponses silencieux.... 506
Modification du compte utilisateur....506
Configuration de la surveillance de Microsoft Exchange....507
Création d'utilisateurs....507
Affectation des droits d'administrateur à l'utilisateur d'Serveur Exchange 510
Attribution à l'utilisateur de Serveur Exchange des droits d'administrateur local.... 512
Configuration du Serveur Exchange pour l'accessibilité....514
Configuration de l'agent pour qu'il s'exécute sous l'utilisateur de domaine.... 515
Configuration de l'agent en local.... 515
Configuration de l'agent à l'aide du fichier de réponses silencieux.... 520
Configuration des variables de l'environnement local pour l'agent.... 520
Configuration de la surveillance de Microsoft Hyper-V.... 521
Saisie de la stratégie de sécurité locale pour l'exécution de Monitoring Agent for Microsoft Hyper-V Server sous Windows par un utilisateur non-administrateur.... 522
Octroi de droits de la stratégie de sécurité locale.... 523
Modification des droits DCOM.... 524
Ajout d'un utilisateur non-administrateur dans le groupe d'utilisateurs administrateurs Hyper-V524
Ajout d'un utilisateur non-administrateur dans le groupe d'utilisateurs Performance Business Monitor.... 525
Configuration de la surveillance de Microsoft IIS....525
Configuration de l'agent sur des systèmes Windows.... 526
Configuration de l'agent à l'aide du fichier de réponses silencieux.... 526
Modification du compte utilisateur....527
Configuration de la surveillance de Skype for Business Server (anciennement Microsoft Lync Server)....528
Droits et droits d'accès d'un utilisateur non-administrateur....528
Configuration de l'agent sur des systèmes Windows.... 529
Configuration de l'agent à l'aide du fichier de réponses silencieux.... 530
Modification du compte utilisateur....531
Paramètres de configuration de l'agent.... 531
Configuration de la surveillance de Microsoft .NET....533
Droits nécessaires pour exécuter un agent à l'aide d'un compte local ou de domaine....534
Enregistrement du collecteur de données.... 535
Utilisation du module de temps de réponse IIS de l'agent .NET....536
Activation de la collecte des données de suivi des transactions et de diagnostic.... 538
Activation de la collecte des données de diagnostic à l'aide de la commande configdc.... 539
Activation du suivi des transactions dans l'environnement de coexistence d'agent....540
Activation des mises à jour de configuration.... 540
Optimisation des performances du collecteur de données....541
Configuration de la surveillance de Microsoft Office 365.... 544
Vérification de l'accessibilité des utilisateurs configurés....545
Configuration de l'agent sur des systèmes Windows.... 546
Configuration de l'agent à l'aide du fichier de réponses silencieux.... 546
Modification du compte utilisateur....547
Surveillance de la qualité de service Skype.... 548
Définition des variables d'environnement local....549
Configuration de la surveillance de Microsoft SharePoint Server 550

Modification du compte utilisateur....551
Exécution de Monitoring Agent for Microsoft SharePoint Server en tant qu'utilisateur non-administrateur....551
Droits de la stratégie de sécurité locale....552
Configuration de la surveillance de Microsoft SQL Server....553
Création d'un utilisateur et attribution des droits d'accès....554
Variables d'environnement local....558
Paramètres de configuration de l'agent....564
Configuration de l'agent sur des systèmes Windows....565
Configuration de l'agent sur des systèmes Linux....578
Configuration de l'agent à l'aide du fichier de réponses silencieux....579
Exécution de l'agent dans un environnement cluster....581
Configuration de l'agent à l'aide de l'utilitaire Cluster....583
Configuration de plusieurs classements pour le fichier ERRORLOG....584
Configuration de la surveillance de MongoDB....586
Configuration de l'agent avec les paramètres par défaut....588
Configuration de l'agent à l'aide du fichier de réponses silencieux....589
Configuration de l'agent en répondant à des invites....590
Configuration de la surveillance de MySQL....591
Configuration de l'agent sur des systèmes Windows....592
Configuration de l'agent sur des systèmes Linux....592
Configuration de l'agent à l'aide du fichier de réponses silencieux....593
Configuration de la surveillance de NetApp Storage....594
Téléchargement et installation du fichier JAR de NetApp Manageability SDK....595
Configuration de l'agent sur des systèmes Windows....596
Configuration de l'agent à l'aide du fichier de réponses silencieux....596
Configuration de l'agent en répondant à des invites....598
Paramètres de configuration du fournisseur de données....598
Paramètres de configuration d'OnCommand Unified Manager....600
Paramètres de configuration d'OnCommand API Service....600
Configuration de la surveillance de Node.js....601
Configuration de l'Agent Node.js....602
Configuration du collecteur de données Node.js autonome pour les applications IBM Cloud(anciennement Bluemix)....608
Configuration du collecteur de données Node.js autonome pour les applications sur site....615
Configuration du collecteur de données Node.js autonome pour les applications Kubernetes....621
Configuration de la surveillance d'OpenStack....626
Configuration de l'Agent OpenStack....626
Activation de la collecte des informations liées aux processus et des connexions SSH....628
Ajout des valeurs de configuration....630
Configuration de la surveillance d'Oracle Database....631
Configuration de l'agent sur des systèmes Windows....633
Configuration de l'agent en répondant à des invites....637
Configuration de l'agent à l'aide du fichier de réponses silencieux....641
Accord de privilèges à l'utilisateur de l'agent de base de données Oracle....644
Configuration de la surveillance du système d'exploitation....647
Exécution des agents de système d'exploitation en tant qu'utilisateur non superutilisateur....647
Configuration de la surveillance des fichiers journaux de l'agent de système d'exploitation....649
Configuration du scriptage personnalisé de l'agent de système d'exploitation....675
Configuration de la collecte de données du système de fichiers de l'agent du système d'exploitation Linux....682
Configuration de la surveillance de PHP....682
Configuration de la surveillance PostgreSQL....685
Configuration de l'agent sur des systèmes Windows....686
Configuration de l'agent sur des systèmes Linux....687
Configuration de l'agent à l'aide du fichier de réponses silencieux....687
Configuration de la surveillance Python....689
Configuration du collecteur de données Python pour les applications IBM Cloud....689

Configuration du collecteur de données Python pour les applications sur site....695
Configuration de la surveillance de RabbitMQ....701
Configuration de l'agent sur des systèmes Windows....702
Configuration de l'agent sur des systèmes Linux....702
Configuration de l'agent à l'aide du fichier de réponses silencieux....703
Paramètres de configuration de l'agent....704
Configuration de la surveillance des temps de réponse....704
Affichage des tableaux de bord de transactions....705
Response Time Monitoring Composants....706
Planification de l'installation....706
Planification de la configuration....708
Injection JavaScript....709
Reconfiguration de la Response Time Monitoring sous Windows....710
Reconfiguration de la Response Time Monitoring sur AIX et Linux....711
Configuration à l'aide de la page Configuration d'agent....711
Ajout d'applications....713
Configuration de l'module IBM HTTP Server Response Time....714
Organigramme de l'Analyseur de paquets....724
Reconfiguration de l'environnement depuis le module IBM HTTP Server Response Time vers l'Analyseur de paquets....732
Personnalisation des valeurs de localisation Transaction utilisateur final....733
Suivi des applications Web supplémentaires....734
Spécification d'un nom de système géré unique pour l'Agent de surveillance des temps de réponse....737
Configuration de la surveillance de Ruby....737
Configuration de l'Agent Ruby....738
Configuration du collecteur de données Ruby pour les applications IBM Cloud....745
Configuration de la surveillance de SAP....750
Configuration de l'agent sur des systèmes Windows....751
Configuration de l'agent sur des systèmes Linux ou AIX....752
Configuration de l'agent à l'aide du fichier de réponses silencieux....753
Paramètres de configuration de l'agent....753
Le nom d'hôte SAP est tronqué pour respecter les restrictions de longueur de nom du système géré....757
Importation du transport ABAP dans le système SAP....758
Suppression du transport ABAP du système SAP....764
Vérification de la configuration de l'agent....765
Ajout du numéro de port de communication de base de données....769
Installation et configuration avancées de l'agent SAP....770
Configuration de la surveillance de SAP HANA Database....784
Configuration de la surveillance de SAP NetWeaver Java Stack....786
Configuration de l'agent sur des systèmes Windows....787
Configuration de l'agent sur des systèmes Linux ou AIX....788
Configuration de l'agent à l'aide du fichier de réponses silencieux....788
Configuration du collecteur de données....789
Activation de la collecte des données de suivi des transactions et de diagnostic....791
Suppression de la configuration du collecteur de données....792
Restauration de l'instance SAP NetWeaver Application Server....792
Paramètres de configuration de l'agent....793
Configuration de la surveillance de Siebel....793
Vérification du compte utilisateur Siebel....794
Activation du paramètre "Per Component Statistics Monitoring"....795
Configuration de l'agent sur des systèmes Windows....796
Configuration de l'agent en répondant à des invites....800
Configuration de l'agent à l'aide du fichier de réponses silencieux....801
Paramètres de configuration de l'agent Siebel....802
Journaux de composant Siebel toujours surveillés....805
Configuration de la surveillance Sterling Connect Direct....805

Configuration de l'agent sur des systèmes Windows..... 806
Configuration de l'agent sur des systèmes Linux.....806
Configuration de l'agent à l'aide du fichier de réponses silencieux..... 807
Paramètres de configuration de l'agent..... 807
Configuration de la surveillance Sterling File Gateway..... 808
Installation de l'API REST B2B.....808
Configuration de l'Agent Sterling File Gateway sur des systèmes Windows..... 809
Configuration de l'Agent Sterling File Gateway sur les systèmes Linux.....809
Configuration de l'Agent Sterling File Gateway à l'aide du fichier de réponses silencieux..... 810
Configuration de variables d'environnement d'agent pour le fournisseur de données sous Linux.811
Configuration de variables d'environnement d'agent pour le fournisseur de données sous Windows.....811
Variables d'environnement du fournisseur de données..... 812
Paramètres de configuration des détails de l'API B2B.....813
Paramètres de configuration des détails de la base de données.....814
Paramètres de configuration de l'API Java..... 814
Configuration de la surveillance de Sybase Server.....815
Octroi de droits d'accès..... 815
Configuration de l'agent à l'aide de l'interface de ligne de commande..... 817
Configuration de l'agent à l'aide du fichier de réponses silencieux..... 818
Désactivation de la lecture de pages modifiées pour la requête..... 820
Configuration de la surveillance de Synthetic Playback.....821
Activation de la prise en charge de proxy en amont pour l'Agent Synthetic Playback.....822
Configuration de la surveillance de Tomcat..... 823
Configuration de l'Agent Tomcat avec les paramètres par défaut..... 824
Configuration de l'agent sur des systèmes Windows..... 824
Configuration de l'Agent Tomcat sur les systèmes Linux..... 828
Configuration de l'Agent Tomcat à l'aide du fichier de réponses silencieux.....829
Activation de la collecte des données de suivi des transactions et de diagnostic..... 829
Mise à jour ou modification du serveur d'applications Tomcat 830
Configuration de la surveillance de VMware VI..... 831
Définition de la taille et planification du déploiement de l'Agent VMware VI.....832
Activation de la communication SSL avec les sources de données VMware VI..... 833
Configuration de l'agent sur des systèmes Windows..... 834
Configuration de l'agent à l'aide du fichier de réponses silencieux..... 835
Configuration de l'agent en répondant à des invites.....836
Paramètres de configuration de la source de données..... 837
Paramètres de configuration du fournisseur de données.....838
Augmentation de la taille de segment de mémoire Java.....839
Configuration de la surveillance de WebLogic.....840
Configuration de l'agent sur des systèmes Windows..... 842
Configuration de l'agent en répondant à des invites.....846
Configuration de l'agent à l'aide du fichier de réponses silencieux..... 846
Paramètres de configuration de l'Agent WebLogic..... 848
Configuration du suivi des transactions pour l'Agent WebLogic..... 849
Configuration de votre Tableau de bord d'Application Performance pour l'affichage des données de suivi des transactions de l'Agent WebLogic.....855
Configuration de la surveillance des applications WebSphere..... 856
Configuration du collecteur de données pour l'Agent WebSphere Applications..... 857
Configuration du collecteur de données Liberty pour les applications sur site..... 906
Configuration du collecteur de données Liberty pour les applications IBM Cloud.....910
Configuration avancée du collecteur de données..... 916
Configuration de l'Agent WebSphere Applications pour surveiller WebSphere Extreme Scale.....947
Configuration de la surveillance de WebSphere Infrastructure Manager.....956
Configuration de la surveillance de WebSphere MQ..... 957
ID utilisateur autorisés à exécuter l'agent..... 957
Configuration d'IBM MQ (WebSphere MQ) pour l'activation des données.....959
Configuration de l'agent WebSphere MQ..... 961

Spécification de noms de systèmes gérés uniques pour plusieurs gestionnaires de files d'attente....964
Configuration du suivi des transactions pour l'agent WebSphere MQ....966
Activation de la collecte de données pour l'historique à long terme de files d'attente et de canal967
Activation de la surveillance des statistiques de file d'attente pour le gestionnaire de files d'attente IBM MQ....968
Surveillance à distance des gestionnaires de file d'attente sur MQ Appliance....969
Surveillance à distance des gestionnaires de file d'attente haute disponibilité sur MQ Appliance 970

Chapitre 8. Intégration à d'autres produits et composants....975
Intégration à Cloud Event Management....975
Intégration à IBM Tivoli Monitoring V6.3....975
Coexistence des agents....976
Passerelle hybride....979
Intégration à OMEGAMON....991
Intégration à Netcool/OMNIbus....992
Installation et configuration de l'agent d'intégration pour Netcool/OMNIbus....992
Configuration de l'intégration pour Netcool/OMNIbus....995
Intégration à Operations Analytics - Log Analysis....996
Intégration à Operations Analytics - Predictive Insights....997
Intégration à Alert Notification....998
Intégration à Control Desk....999
Intégration à IBM Cloud....1000
Intégration à IBM Agent Builder....1001

Chapitre 9. Gestion....1003
Démarrage de la console Cloud APM....1003
Seuils et groupes de ressources....1004
Informations de référence....1004
Gestionnaire de groupes de ressources....1008
Tutoriel : Définition d'un seuil....1010
Tutoriel : Définition d'un seuil pour exécuter une commande sur la ressource gérée....1013
Gestionnaire de seuils....1014
Personnalisation d'un événement à transmettre à un récepteur EIF....1019
Envoi d'un courrier électronique en réponse à un événement....1026
Utilisation de l'API Resource Group Management Service....1026
Utilisation de l'API Threshold Management Service....1028
Gestion des accès utilisateur....1030
Rôles et droits....1031
Accès et utilisation de l'API Role-Based Access Control Service....1041
Administration de vos agents....1042
Démarrage des agents en tant qu'utilisateur non superutilisateur....1042
Seuils d'événement pour la surveillance des transactions....1043
Gestion des événements d'agent de système d'exploitation....1047
Gestion des transactions et des événements synthétiques avec Website Monitoring....1057
Instructions pour la maximisation des performances du serveur et des agents dans le cadre de la surveillance des fichiers journaux....1072
Availability Monitoring....1076
A propos d'Availability Monitoring....1076
Accès à Availability Monitoring....1077
Création et configuration des tests....1078
Examen des informations de disponibilité et de performance de l'application sur le tableau de bord Surveillance....1091
Utilisation d'Availability Monitoring....1103
Exploration des API....1103
Configuration avancée....1104
E-mail d'événement....1106

Chapitre 10. Utilisation des tableaux de bord..... 1109
Toutes mes applications - Tableau de bord d'Application Performance..... 1109
Recherche dans les fichiers journaux.....1111
Application - Tableau de bord d'Application Performance.....1112
Manipulation du widget Agréger une topologie de transaction.....1116
Groupe et Instance - Tableau de bord d'Application Performance.....1117
Edition des widgets de groupe du tableau de bord Composants.....1120
Ajustement et comparaison de mesures dans le temps..... 1121
Affichage et gestion de graphiques et tableaux personnalisés.....1123
Gestion des applications.....1129
Ajout d'une application.....1130
Edition d'une application..... 1133
Suppression d'une application..... 1134
Affichage et suppression des agents en ligne.....1135
Statut de l'événement..... 1140
Recherche d'anomalies à l'aide d'Operations Analytics - Predictive Insights.....1143
Vues personnalisées..... 1144
Création et gestion de pages personnalisées..... 1144
Affichage de pages personnalisées.....1151
Utilitaires de tableau de bord.....1154
Copie de l'URL du tableau de bord..... 1154
Définition d'une trace.....1154
Verrouillage de la console Cloud APM.....1155
Rapports..... 1156
Rapports de l'Agent de surveillance des temps de réponse..... 1156
Génération de rapports sur l'Agent Synthetic Playback.....1161
Rapports de l'Agent WebSphere Applications.....1166

Chapitre 11. Mise à niveau..... 1171
Mise à niveau de vos agents.....1171
Conservation des changements apportés à la configuration des agents.....1173
Agents sous AIX : arrêt de l'agent et exécution de **slibclean** avant la mise à niveau..... 1174
agent HMC Base sous AIX : Arrêt de l'agent en tant qu'utilisateur non superutilisateur et exécution de **slibclean** avant la mise à niveau.....1175
Agent Node.js : suppression des plug-in de collecteur de données avant la mise à niveau..... 1175
Agent Response Time Monitoring : mise à niveau de module IBM HTTP Server Response Time 1176
agent Microsoft .NET : suppression du collecteur de données .NET avant la mise à niveau..... 1178
Agent OpenStack : reconfiguration des instances de l'agent pour utiliser OpenStack Identity API v3.....1178
Agent Ruby : suppression des plug-in de collecteur de données avant la mise à niveau..... 1178
Agent WebSphere Applications : migration du collecteur de données.....1179
Agent Tomcat : mise à niveau de TEMA Core Framework sous Windows..... 1183
Mise à niveau de vos collecteurs de données..... 1184

Chapitre 12. Traitement des incidents et support.....1187
Traitement des incidents liés aux agents..... 1187
Internet Service Monitoring.....1187
Surveillance de Microsoft Active Directory..... 1188
Surveillance de Microsoft IIS..... 1188
Surveillance de Microsoft .NET.....1189
Surveillance de Microsoft SharePoint Server.....1189
Surveillance de PostgreSQL.....1190
Collecte des journaux d'agent de surveillance pour le support IBM..... 1190

Chapitre 13. Agent Builder..... 1193
Présentation d'Agent Builder..... 1193

Procédures Agent Builder communes....1194
Sources de données et fichiers.... 1195
Surveillance de plusieurs serveurs ou instances de serveur....1196
Test, installation et configuration d'un agent.... 1197
Configuration requise pour le système d'exploitation....1198
Fonctions spécifiques à IBM Tivoli Monitoring.... 1198
Installation et démarrage d'Agent Builder.... 1199
Conditions préalables à l'installation et l'exécution d'Agent Builder....1199
Installation d'Agent Builder....1199
Démarrage d'Agent Builder.... 1202
Définition du navigateur par défaut dans Agent Builder....1202
Définition de l'autorité d'horodatage par défaut dans Agent Builder.... 1203
Désinstallation d'Agent Builder....1203
Désinstallation en mode silencieux....1204
Création d'un agent.... 1204
Désignation et configuration de l'agent.... 1204
Définition de sources de données initiales.... 1206
Utilisation de l'éditeur d'agent pour modifier l'agent....1207
Systèmes d'exploitation par défaut.... 1208
Agent autodescriptif.... 1209
Variables d'environnement....1209
Informations sur le programme de surveillance....1221
Informations Cognos.... 1222
Lien vers l'assistant de génération d'agent....1223
Page **Définition de la source de données**....1223
Page **Informations sur la configuration d'exécution**....1224
Page Editeur XML d'agent....1224
Enregistrement de vos modifications....1225
Validation d'une version de l'agent.... 1225
Définition d'un nouveau numéro de version pour votre agent.... 1226
Modification du code produit....1226
Modification des propriétés de sources de données et d'attributs.... 1227
Création, modification et suppression d'attributs.... 1228
Filtrage des groupes d'attributs.... 1237
Editeur de formule.... 1237
Opérateurs et fonctions de formule.... 1242
Spécification des systèmes d'exploitation....1249
Configuration et optimisation de la collecte de données.... 1249
Définition et test de sources de données.... 1255
Surveillance d'un processus....1256
Surveillance d'un service Windows....1260
Surveillance de données à partir de Windows Management Instrumentation (WMI)....1261
Surveillance d'un Windows Performance Monitor (Perfmon)....1264
Surveillance de données à partir d'un serveur SNMP (Simple Network Management Protocol).. 1266
Surveillance d'événements à partir d'expéditeurs d'événements SNMP (Simple Network Management Protocol).... 1271
Surveillance de beans gérés (MBeans) JMX (Java Management Extensions).... 1277
Surveillance de données à partir d'un modèle CIM (Common Information Model).... 1296
Surveillance d'un fichier journal.... 1299
Surveillance d'un journal binaire AIX.... 1311
Surveillance d'un journal des événements Windows.... 1312
Surveillance d'un code retour de commande.... 1315
Surveillance de la sortie d'un script.... 1319
Surveillance de données à partir de JDBC (Java Database Connectivity).... 1325
Surveillance de la disponibilité du système avec des commandes Ping.... 1333
Surveillance de la disponibilité et du temps de réponse HTTP....1336
Surveillance des données à partir d'une source de données SOAP ou d'une autre source de données HTTP....1344

Surveillance de données à l'aide d'un socket ... 1352
Utilisation de l'API Java pour surveiller des données ... 1363
Création de jeux de données à partir de sources existantes ... 1377
Jointure de deux groupes d'attributs ... 1378
Manipulation des attributs de groupes d'attributs joints ... 1382
Attributs joints ... 1382
Création d'un groupe d'attributs filtré ... 1383
Création d'un groupe de navigation ... 1385
Utilisation des sous-noeuds ... 1386
Création de sous-noeuds ... 1393
Configuration de sous-noeud ... 1394
Personnalisation de la configuration de l'agent ... 1404
Modification des propriétés de configuration à l'aide de l'éditeur d'agent ... 1407
Configuration d'une connexion distante Windows ... 1407
Création d'un utilisateur avec les droits Windows Management Instrumentation (WMI) ... 1408
Configuration d'une connexion distante SSH (Secure Shell) ... 1410
Création d'espaces de travail, de commandes Action et de situations ... 1411
Création de situations, de commandes Action et de requêtes ... 1412
Création d'espaces de travail ... 1412
Préparation de l'agent pour Cloud APM ... 1417
Test de votre agent dans Agent Builder ... 1420
Test des groupes d'attributs ... 1420
Test complet de l'agent ... 1424
Variables d'environnement de test ... 1428
Installation de votre agent dans une infrastructure de surveillance à des fins de test et d'utilisation ... 1429
Installation d'un agent ... 1430
Agent de post-génération et résultats de l'installation ... 1438
Désinstallation d'un agent ... 1445
Importation des fichiers de prise en charge de l'application ... 1447
Exportation et importation de fichiers pour les agents Tivoli Enterprise Monitoring ... 1447
Exportation et importation de fichiers pour les agents Tivoli System Monitor ... 1448
Filtrage et récapitulatif des événements ... 1449
Contrôle des événements en double ... 1450
Affichage des données de filtrage et de récapitulation d'événements dans Tivoli Enterprise Portal ... 1451
Traitement des incidents et support ... 1456
Partage des fichiers de projet ... 1457
Partage d'un projet Solution Installer ... 1457
Options de ligne de commande ... 1457
Commande - **generatelocal** ... 1459
Commande - **generatemappingfile** ... 1459
Commande - **generatezip** ... 1460
Guide de référence des attributs ... 1461
Noeud de disponibilité ... 1461
Noeud de statut d'objet de performances ... 1466
Groupe d'attributs de statut du pool d'unités d'exécution ... 1472
Groupe d'attributs Journal des événements ... 1475
Synthèse du fichier journal ... 1477
Groupe d'attributs du journal binaire AIX ... 1479
Groupes d'attributs Surveillance et notification ... 1483
Groupes d'attributs d'événements SNMP ... 1492
Groupes d'attributs d'événements JMX ... 1494
Groupe d'attributs Ping ... 1495
Groupes d'attributs HTTP ... 1498
Groupes d'attributs de reconnaissance ... 1503
Groupe d'attributs Statut d'action ... 1505
Groupe d'attributs de statut du fichier journal ... 1508
Groupe d'attributs Statistiques RegEx du fichier journal ... 1512

Création d'extensions de prise en charge d'application pour des agents existants..... 1516
Création d'un projet d'extension de prise en charge d'application..... 1516
Ajout de fichiers de prise en charge dans un projet..... 1516
Génération de l'image d'installation de l'extension de prise en charge d'application..... 1517
Installation de l'extension de prise en charge d'application..... 1518
Conversion d'un **projet d'installation de solution** en un projet d'extension de prise en charge d'application..... 1518
Génération d'un modèle de données Cognos..... 1519
Prérequis à la génération d'un modèle de données Cognos..... 1519
Création de rapports..... 1523
Expressions régulières ICU..... 1534
Création d'ensembles de fichiers sans agent..... 1540
Editeur de regroupement de déploiement à distance 1541
Ajout de commandes au regroupement..... 1542
Ajout de prérequis à un regroupement..... 1542
Ajout de fichiers à un regroupement..... 1543
Génération d'un regroupement..... 1543
Création de regroupements déployables pour les sondes Tivoli Netcool/OMNIbus..... 1544
Prise en charge des noms de fichier dynamiques..... 1544
Configuration des alertes SNMP..... 1548
Guide de référence des commandes Action..... 1551
Action SSHEXEC..... 1552

Fonctions d'accessibilité..... 1553

Remarques..... 1555
Marques..... 1556
Dispositions relatives à la documentation du produit..... 1557
Déclaration IBM de confidentialité sur Internet..... 1557

Chapitre 1. Nouveautés

De nouvelles fonctions, fonctionnalités et offres sont disponibles dans la dernière édition.

- Pour plus d'informations sur la version de l'agent dans chaque édition ou actualisation, voir «Historique des modifications», à la page 53.

Décembre 2019

Nouvel agent

Agent MariaDB

Monitoring Agent for MariaDB offre un point central de gestion pour votre environnement ou application MariaDB. Ce logiciel offre une solution complète permettant de rassembler les informations dont vous avez besoin pour détecter les incidents de manière précoce et vous en prémunir. Les informations sont standardisées à travers le système. Vous pouvez surveiller plusieurs serveurs à partir d'une seule console. En utilisant Monitoring Agent for MariaDB, vous pouvez aisément collecter et analyser des informations sur MariaDB.
Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de MariaDB», à la page 494

Prise en charge de la plateforme étendue pour les agents

Les agents et plateformes suivants sont désormais pris en charge :

Solaris X86-64

- Agent Oracle Database
- Agent WebLogic

Améliorations au niveau des agents

agent Cassandra

Ajout de deux nouveaux attributs appelés `Agent Hostname` et `Agent Instance Name` dans les groupes d'attributs `Cluster Details`, `Node Statistics` et `Keyspace Details`.

agent Db2

Ajout de la prise en charge de la surveillance de `Current Running SQL`.

agent IBM Integration Bus

Ajout de deux nouveaux widgets de groupe, `TCPIP Client Connections` et `TCPIP Server Connections` dans la page `Integration Server Status - Detail`.

Internet Service Monitoring

- Ajout de deux nouvelles variables de panneau de configuration :
  - *Active* : permet de sélectionner un état actif ou inactif pour un élément de profil.
  - *sniServerName* : indique le nom d'hôte/du serveur pour lequel un certificat du serveur Web activé pour SNI est requis.
- Les **Paramètres par défaut** sous l'onglet **Validation des données** pour les surveillances HTTP, HTTPS et DNS sont désormais éditables
- L'agent prend désormais en charge le caractère & dans la zone **page** pour les surveillances HTTP et HTTPS
- L'agent prend désormais en charge les caractères danois dans la zone **regex** des surveillances HTTP et HTTPS

  Remarque : Définissez l'environnement local sur da_DK sur la plateforme Linux avant l'installation de l'agent pour utiliser cette fonction

agent Microsoft Active Directory

- Ajout d'un nouveau widget appelé `KCC details` dans la page `Status Overview`.

- Ajout des nouveaux groupes d'attributs suivants dans l'onglet Détails d'attribut :
  - Services d'annuaire
  - Vérificateur de cohérence kerberos
  - Centre de distribution de clés kerberos
  - Fournisseur de service d'annuaire
  - Service d'annuaire Exchange

agent Microsoft .NET

Ajout d'un nouvel attribut appelé Request Name dans le groupe d'attributs Database Call Details. Cet attribut affiche le nom de la demande qui déclenche la requête de base de données.

agent Microsoft Exchange Server

- Ajout d'un nouveau widget appelé Transport SMTP Receive dans la page Status Overview.
- Ajout de nouveaux groupes d'attributs suivants dans l'onglet Détails d'attribut :
  - MSExchange AB
  - Processus MSExchange ADAccess
  - Caches MSExchange ADAccess
  - Contrôleurs de domaine MSExchange ADAccess
  - Détection de forêt ADAccess MSExchange

agent Microsoft Hyper-V Server

Ajout de la prise de charge de Windows Server 2019.

agent Microsoft IIS

- Ajout de nouveaux widgets de groupe :
  - Statistiques de mémoire principale-système
  - Utilisation de la mémoire attribuée IIS Server
  - Utilisation de l'unité centrale attribuée IIS Server
  - Détails du processus de travail
  - Gestion de la mémoire .Net
- Sur chaque nom de pool d'applications dans le widget de groupe Détails du processus de travail, une page qui affiche la tendance historique des Demandes traitées par seconde, du Temps écoulé, des Demandes en file d'attente, et de la Mémoire et Utilisation de l'UC est créée.
- Sur chaque nom de pool d'applications dans le widget de groupe Gestion de la mémoire .Net, une fenêtre en incrustation qui affiche la tendance historique du pourcentage de temps en récupération de place est ajoutée.

agent MicrosoftSharePoint Server

- Ajout d'un nouvel attribut appelé Trace_Log qui fournit des informations sur les journaux de gravité élevée.
- Ajout de deux nouveaux widgets de groupe appelés Trace Log Details et Last 1 Hour Trace Log Count dans la page Présentation pour afficher les détails des 100 derniers événements du journal de trace et du nombre de journaux de trace inattendus et de niveau supérieur pendant la dernière heure.

Agent MySQL

L'agent collecte les données de manière cohérente après le redémarrage du serveur.

agent NetApp Storage

L'agent affiche désormais la liste exacte de Qtress mappée à Volume.

Agent PostgreSQL

L'agent prend désormais en charge PostgreSQL Server version 12.

Agent de surveillance des temps de réponse

- Un nouveau paramètre de configuration KT5AARIPTOUSERID est ajouté. Il permet de sauvegarder l'adresse IP client dans la propriété Nom d'utilisateur dans les données brutes d'AAR. Par défaut, il est défini sur NO. Pour modifier le paramètre, vous devez redémarrer l'Agent de surveillance des temps de réponse.
  - KT5AARIPTOUSERID=NO : si la valeur est NO, l'Agent de surveillance des temps de réponse enregistre le nom d'utilisateur de la transaction dans la propriété userID d'AAR.
  - KT5AARIPTOUSERID=YES : si la valeur est YES, l'Agent de surveillance des temps de réponse enregistre l'adresse IP source de la transaction dans la propriété userID d'AAR.
- L'Agent de surveillance des temps de réponse prend désormais en charge la spécification de la valeur KT5AARIPTOUSERID pour la configuration en mode silencieux.
- Le titre du widget de groupe existant `Les pires utilisateurs - 5 premiers` est remplacé par `Les pires utilisateurs - 20 premiers`. Le widget de groupe a été modifié pour afficher les 20 premiers utilisateurs avec le pourcentage le plus élevé d'échecs de transaction sur la période sélectionnée.

VMware

- L'agent prend désormais en charge l'extraction de l'adresse IP ou du nom d'hôte de vCenter à partir de l'appel d'API vSphere, au lieu d'afficher `Configured Address` tel qu'il est affiché dans le panneau de configuration. L'utilisateur peut activer cette fonction en définissant l'indicateur dans l'environnement d'agent sur Y. Par exemple, `KVM_RETRIEVE_HOSTNAME_FROM_API=Y`.
- Il est maintenant possible d'attribuer une limite au nombre de nouvelles tentatives de connexion avec la source de données. Par exemple, `KVM_DATA_PROVIDER_CONNECTION_RETRY_COUNT=1000`, l'ajout de cette variable dans le fichier d'environnement de l'agent verrouille le nombre de tentatives de connexion en cas d'échec de connexion avec vCenter. 1000 indique que l'agent peut tenter jusqu'à 1000 tentatives de connexion infructueuses à la suite avant d'envoyer au processus du fournisseur de données le message de journal `NO MORE ATTEMPTS OF CONNECTION ; STOPPING THE DATA COLLECTION, TO RESUME MONITORING PLEASE RESTART THE AGENT. TO HAVE MORE ATTEMPT OF CONNECTIONS, RESET THE VALUE OF THE VARIABLE KVM_DATA_PROVIDER_CONNECTION_RETRY_COUNT`. La valeur par défaut de réessai des tentatives de connexion est 6. L'utilisateur peut définir le seuil souhaité conformément à l'exigence.
- L'agent prend en charge la configuration de la taille de segment de mémoire spécifique à l'instance pour utiliser efficacement la mémoire allouée sur le système. Par exemple, `KVM_CUSTOM_JVM_ARGS= -Xmx512m`, en définissant cette variable dans le fichier d'environnement de l'instance, cela signifie que l'instance est configurée pour utiliser 512 Mo de mémoire dynamique. La taille peut être modifiée en fonction du nombre total d'objets vCenter surveillé par une instance.

Septembre 2019

Prise en charge de la plateforme étendue pour les agents

Les agents et plateformes suivants sont désormais pris en charge :

Solaris X86-64

- agent Db2
- Agent SAP
- agent Sybase
- Agent UNIX OS
- Agent WebSphere Applications

- agent WebSphere MQ
- agent IBM Integration Bus

RHEL on x86-64 (64 bits)

- Internet Service Monitoring agent
- agent Microsoft SQL Server
- agent Sybase

RHEL on POWER Little Endian (ppc64le)

- agent RabbitMQ

Améliorations au niveau des agents

agent Db2

- L'agent prend maintenant en charge le serveur Db2 version 11.5.

agent Hadoop

- Le panneau de configuration comporte un nouveau paramètre de configuration **Unique Cluster Name** qui est un nom unique pour un cluster Hadoop indiquant la version de celui-ci.
- L'agent Hadoop comporte un élément d'affichage pour les seuils créés dans les services Ambari.
- Il prend en charge la surveillance du service Streaming Analytics Manager dans le cluster Hadoop.
- Il prend en charge la surveillance du service Schema Registry dans le cluster Hadoop.

agent HTTP Server

- L'agent prend en charge le serveur Oracle HTTP sur Solaris Sparc.

Internet Service Monitoring

- L'agent prend en charge IBM Tivoli Netcool/OMNIbus.
- Il est amélioré pour supprimer des profils et renommer les profils existants.

Agent MongoDB

- L'agent prend en charge la base de données MongoDB version 4.x.

Agent MySQL

- L'attribut FQDN est ajouté pour Application Availability dans la section Aide.
- Affichage de l'infobulle fixe pour le paramètre IP Address Agent Configuration.
- Les nouveaux attributs suivants sont ajoutés pour la surveillance dans IBM Cloud App Management.
  - Informations de taille de base de données
  - Informations sur l'erreur
  - Nombre de verrous d'instance de base de données
  - Détails de la connexion de l'utilisateur
  - Détails de la liste de processus
  - Informations sur les événements

Agent PostgreSQL

- Deux nouvelles situations, `Deadlocks_Count_Crit` et `Deadlocks_Count_Warn`, sont ajoutées pour surveiller le nombre d'interblocages dans une base de données. Elles ont pour but de vous aider à traiter avec précision ces problèmes.
- Un nouveau groupe d'attributs, `Deadlocks_Info`, est ajouté pour vérifier les détails des interblocages.

agent Sybase

- L'attribut FQDN est ajouté pour Application Availability dans la section Aide.

Agent Synthetic Playback

- Firefox V68.0 ESR est désormais pris en charge.
- Le proxy système et le proxy PAC sont pris en charge, mais pas les configurations de proxy.

Agent Tomcat

- L'agent est amélioré avec des indicateurs et des vues d'interface utilisateur pour la surveillance de l'utilisation du pool de mémoire dynamique/non dynamique pour la JVM.
- L'agent est amélioré avec des indicateurs et des vues d'interface utilisateur pour la surveillance des unités d'exécution et les informations de chargement de classe pour la JVM.
- Le FQDN (nom de domaine complet) apparaît maintenant dans la vue Server Information de l'interface utilisateur de l'agent.

Agent UNIX OS

- L'agent est mis à jour avec la fonction de scriptage personnalisé. Les scripts Shell et PERL, ainsi que d'autres types de script peuvent être utilisés.

Agent VMware VI

- Une nouvelle zone de configuration, **KEY_STORE_PASSWORD**, est ajoutée. Elle permet à l'utilisateur de configurer l'agent avec le nouveau mot de passe du magasin de clés défini pour l'environnement JRE de l'agent.

Juin 2019

Prise en charge de la plateforme étendue pour les agents

Les agents et plateformes suivants sont désormais pris en charge :

Red Hat Enterprise Linux (RHEL) 8

Les agents et les collecteurs de données suivants prennent maintenant en charge RHEL 8. Avant d'installer les agents sur RHEL 8, n'oubliez pas de lire la section «Systèmes d'exploitation spécifiques», à la page 133 de la rubrique «Préinstallation sur les systèmes Linux», à la page 132.

RHEL 8 on x86-64 (64 bits)

- agent Cassandra
- agent Cisco UCS
- agent DataPower
- agent DataStage
- agent Db2
- agent Hadoop
- agent HTTP Server
- Agent d'intégration pour Netcool/OMNIbus
- Agent Internet Service Monitoring
- collecteur de données J2SE
- agent Linux KVM
- Linux OS
- Agent MongoDB
- Agent MQ Appliance
- Agent MySQL
- agent NetApp Storage
- collecteur de données Node.js

- Agent PHP
- collecteur de données Python
- Agent PostgreSQL
- agent RabbitMQ
- Agent de surveillance des temps de réponse
- Agent Ruby
- Agent SAP
- Agent SAP HANA Database
- Agent SAP NetWeaver Java™ Stack
- Agent Sterling Connect Direct
- Agent Sterling File Gateway
- agent Sybase
- Agent Tomcat
- Agent VMware VI
- Agent WebSphere Applications
- agent WebSphere MQ

RHEL 8 on System z

- agent Db2
- agent Hadoop
- Linux OS
- Agent MySQL
- collecteur de données Node.js
- collecteur de données Python
- Agent de surveillance des temps de réponse
- Agent WebSphere Applications
- agent WebSphere MQ

RHEL 8 on POWER Little Endian (ppc64le)

- agent Db2
- agent Hadoop
- collecteur de données J2SE
- Linux OS
- Agent MySQL
- collecteur de données Node.js
- Agent SAP NetWeaver Java Stack
- Agent WebSphere Applications
- agent WebSphere MQ

Solaris Sparc 10 et 11

- agent JBoss
- Agent Oracle Database
- Agent WebLogic

Windows Server 2019

- Agent WebSphere Applications

Améliorations au niveau des agents

agent Hadoop

- L'agent Hadoop prend en charge la surveillance du service Ambari HDF 3.3 (avec HDP 3.1.0) Big SQL 6.0.
- L'agent Hadoop prend en charge SUSE Linux Enterprise Server (SLES) 15 sur la plateforme x86-64.

agent HMC Base

L'agent HMC Base prend en charge HMC V9.1.

Agent d'intégration pour Netcool/OMNIbus

L'agent a été mis à jour pour prendre en charge Red Hat Enterprise Linux (RHEL) 8 et SUSE Linux Enterprise Server (SLES) 15

Agent Internet Service Monitoring

L'agent dispose du moniteur Service Assurance Agent qui surveille les sondes Cisco Service Assurance Agent.

agent Microsoft IIS

L'agent est étendu avec la prise en charge de la tolérance pour le serveur Windows 2019. Cette amélioration affiche les données du site FTP de l'agent qui est installé sur Windows 2019 server.

Agent MongoDB

L'agent prend en charge la plateforme Red Hat Enterprise Linux (RHEL) 8 on x86-64 (64 bits).

collecteur de données Python ifix02

Le collecteur de données prend en charge Django version 1.10 et ultérieure.

Agent SAP

L'Agent SAP prend en charge les plateformes suivantes :

- Red Hat Enterprise Linux (RHEL) 8 on x86-64 (64 bits)
- SAP NetWeaver Application Server 7.52 (SAP Basis 752)

Agent SAP HANA Database

L'Agent SAP HANA Database est amélioré avec les fonctions suivantes :

- Le nom d'hôte est ajouté dans le noeud :HDB Subnode de l'Agent SAP HANA Database pour son identification unique.
- L'agent prend en charge l'architecture évolutive.
- Plateformes Red Hat Enterprise Linux (RHEL) 8 on x86-64 (64 bits) et Linux ppc64le.
- Plateforme SUSE Linux Enterprise Server (SLES) 15 on x86-64 (64 bits).
- Un nouvel attribut Trimmed Host est ajouté sous le groupe d'attributs System Database.

Agent SAP NetWeaver Java Stack

L'Agent SAP NetWeaver Java Stack prend en charge les plateformes suivantes :

- Red Hat Enterprise Linux (RHEL) 8 on x86-64 (64 bits)
- SUSE Linux Enterprise Server (SLES) 15 on x86-64 (64 bits)
- Windows Server 2019 DE et SE
- Windows Server 2016 DE et SE

Agent Synthetic Playback

- Prend en charge le script .side enregistré par Selenium IDE 3.2.X, 3.3.X ou 3.5.X
- Prend en charge la lecture par Firefox ESR 60.5.1
- Prend en charge les commandes Selenium IDE **`wait`**, **`flow control`** et **`linkText locator type`**

Agent Skype for Business Server

L'Agent Skype for Business Server est amélioré avec les fonctions suivantes :

- L'agent prend en charge Skype for Business Server 2019.
- Deux nouveaux widgets de groupe, tels que `Database-Throttled Requests(DBStore)` et `Database-Throttled Requests(SHAREDDBStore)`, sont ajoutés sur la page Overview qui indique le nombre de demandes régulées par Skype for Business Server en raison du temps de latence élevée de la file d'attente de base de données pour le DBstore et le DBstore partagé.

Scanner de prérequis

La commande **`IGNORE_PRECHECK_WARNING`** est désormais disponible en tant que commande alternative à la commande **`SKIP_PRECHECK`**. Pour plus d'informations, voir «Contournement de l'analyse des prérequis», à la page 149.

Amélioration de la documentation

Une page est créée pour vous permettre d'obtenir rapidement les informations de version et l'historique des modifications de chaque agent et collecteur de données. Voir «Historique des modifications», à la page 53 .

Mars 2019

Prise en charge de la plateforme étendue pour les agents

Les agents et plateformes suivants sont désormais pris en charge :

Windows Server 2019

- agent Cassandra
- agent DataStage
- agent Db2
- agent Hadoop
- Internet Service Monitoring
- agent Microsoft Active Directory
- agent Microsoft Cluster Server
- agent Microsoft IIS
- agent Microsoft Exchange Server
- agent Microsoft SQL Server
- Agent MySQL
- Agent PostgreSQL
- agent RabbitMQ
- Agent SAP
- Agent SAP HANA Database
- agent Sybase
- Agent Tomcat
- agent Windows OS

Solaris SPARC 10 et 11

- agent Db2
- HTTP Server
- Agent MySQL
- Agent SAP

- agent Sybase
- Agent UNIX OS
- Agent WebSphere Applications

Monitoring Agent for Cassandra

L'agent Cassandra est amélioré avec les fonctions suivantes :

- Ajout de la prise en charge du système d'exploitation Windows Server 2019.
- Ajout de la consignation détaillée pour le traitement des incidents.

Monitoring Agent for Db2

L'agent Db2 est amélioré avec les fonctions suivantes :

- Il prend en charge Windows Server 2019.
- Il prend en charge les plateformes Solaris SPARC 10/11.

Monitoring Agent for Hadoop

L'agent Hadoop est amélioré avec les fonctions suivantes :

- Ajout de la prise en charge nécessaire à la surveillance des clusters Hadoop BigInsights activés pour SSL, Hortonworks et Cloudera.
- Ajout de la prise en charge pour tester la connexion au cluster Hadoop activé pour SSL.
- Ajout de la prise en charge du système d'exploitation Windows Server 2019 (Datacenter et Standard Editions).
- Ajout de la prise en charge de l'offre de surveillance de Hadoop : Cloudera 6.1.1 (CDH 6.1.1).
- Ajout de la prise en charge de l'offre de surveillance de Hadoop : Hortonworks 3.1.0 (HDP 3.1.0).

Monitoring Agent for IBM Integration Bus

L'agent IBM Integration Bus est amélioré avec la fonction suivante :

- Ajout de la prise en charge de la tolérance pour la surveillance d'IBM App Connect Enterprise V11. Pour plus d'informations, voir «Configuration de l'agent IBM Integration Bus», à la page 284.

Monitoring Agent for Microsoft Internet Information Services

L'agent Microsoft IIS prend en charge le système d'exploitation Windows Server 2019.

Monitoring Agent for InfoSphere DataStage

L'agent DataStage est amélioré avec les fonctions suivantes :

- Ajout de la prise en charge du système d'exploitation Windows Server 2019.
- Ajout d'un délai d'attente pour les requêtes de collecte de données dans le but d'améliorer les performances de l'agent.

Monitoring Agent for Microsoft Active Directory

L'agent Microsoft Active Directory est amélioré avec les fonctions suivantes :

- Ajout de la prise en charge de Windows Server 2019.
- Ajout du nouveau groupe d'attributs `AD_Services_Status` qui fournit l'état des services liés au serveur Active Directory.
  En fonction de l'état des services, il détermine le statut du serveur d'Active Directory.
- Ajout de la nouvelle situation `AD_Server_Status` qui surveille le statut du serveur Active Directory.
- Ajout du nouveau groupe d'attributs `Root_Directory_server` qui fournit la version active et le nom de système d'exploitation surveillé.

Monitoring Agent for Microsoft Cluster Server

L'agent Microsoft Cluster Server est amélioré avec les fonctions suivantes :

- Ajout de la prise en charge du système d'exploitation Windows Server 2019.
- Ajout de l'attribut CLUSTER_SERVICE_VERSION.

Monitoring Agent for Microsoft Exchange Server

L'agent Microsoft Exchange Server est amélioré avec les fonctions suivantes :

- Ajout de la prise en charge de MS Exchange Server 2019.
- Ajout du nouveau groupe d'attributs MSExchange MAPIoverHTTP qui fournit des informations relatives aux statistiques sur le protocole MAPI via HTTP.

Monitoring Agent for Internet Services

L'Internet Service Monitoring est amélioré avec les fonctions suivantes :

- Ajout de la prise en charge des moniteurs LDAP, NTP, NNTP, SOAP, SNMP, SIP, RTSP, RPING, RADIUS et TFTP.
- Ajout de la prise en charge du système d'exploitation Windows 2008 R2 Server et Windows Server 2019.

Monitoring Agent for Microsoft SQL Server

L'agent Microsoft SQL Server prend en charge Windows Server 2019.

Monitoring Agent for MySQL

Monitoring Agent for MySQL est amélioré avec les fonctions suivantes :

- Ajout de la prise en charge de Windows Server 2019.
- Ajout de la prise en charge des plateformes Solaris SPARC 10/11.
- Ajout de la fonctionnalité de définition de propriétés supplémentaires à la connexion JDBC initiée par l'agent au serveur MySQL.

Monitoring Agent for PostgreSQL

L'Agent PostgreSQL prend en charge le système d'exploitation Windows Server 2019.

Monitoring Agent for RabbitMQ

L'agent RabbitMQ prend en charge le système d'exploitation Windows Server 2019.

Monitoring Agent for Skype for Business Server

L'Agent Skype for Business Server est amélioré avec les fonctions suivantes :

- Ajout de la prise en charge du système d'exploitation Windows Server 2019.
- Ajout du nouveau groupe d'attributs KQL_Server pour afficher les informations liées au produit Skype for Business Server.
- Ajout d'une nouvelle situation, Skype_Server_Down, permettant de surveiller le statut de Skype for Business Server en fonction du statut des services front-end et de conférence IM du serveur.

Monitoring Agent for SAP Applications

L'Agent SAP est amélioré avec les fonctions suivantes :

- Ajout de la fonction de mot de passe sensible à la casse pour l'utilisateur de l'application exécutée entre l'agent SAP et le serveur SAP.
- Ajout de la prise en charge du système d'exploitation Windows Server 2019 (Datacenter et Standard Editions).
- Ajout de la prise en charge nécessaire pour afficher les travaux à exécution longue présents dans SAP System pendant plus de 24 heures.
- Amélioration des performances du module de fonction /IBMMON/ITM_MAIALRT_INX.
- Ajout de la prise en charge des systèmes d'exploitation Solaris v10 et v11 SPARC

- Ajout de la fonction de troncature du nom d'hôte SAP afin de respecter la limite fixée à 32 caractères pour le nom du système géré.

Monitoring Agent for SAP HANA Database

L'Agent SAP HANA Database est amélioré avec les fonctions suivantes :

- Ajout de la prise en charge nécessaire pour reconnaître les bases de données titulaires lorsque leur nom et l'ID source du système HANA sont identiques.
- Ajout de la prise en charge du système d'exploitation Windows Server 2019 (Datacenter et Standard Editions).

Monitoring Agent for Sybase Server

L'agent Sybase est amélioré avec les fonctions suivantes :

- Ajout de la prise en charge de Windows Server 2019.
- Ajout de la prise en charge des plateformes Solaris SPARC 10/11.
- Requête Sybase étendue pour améliorer les accès concurrents et réduire les verrouillages.

Monitoring Agent for Tomcat

L'Agent Tomcat prend en charge le système d'exploitation Windows Server 2019 (Datacenter et Standard Editions).

Monitoring Agent for UNIX OS

L'Agent UNIX OS est amélioré avec la fonction suivante :

- Ajout de la prise en charge de Solaris SPARC 10 et 11.

Monitoring Agent for VMware VI

L'Agent VMware VI a été actualisé pour ignorer les valeurs unavailable(-1) lors de l'affichage de la tendance moyenne sur le graphique dans tous les diagrammes multi-lignes.

Monitoring Agent for WebSphere Applications

L'Agent WebSphere Applications est amélioré avec les fonctions suivantes :

- Ajout de la prise en charge de Solaris SPARC 10 et 11.
- Ajout de la prise en charge de la surveillance de WebSphere Extreme Scale. Vous pouvez configurer la surveillance d'une ou plusieurs zones Extreme Scale, sous le noeud de tout serveur appartenant à ces zones. Vous pouvez explorer les informations relatives aux différents serveurs, ensembles de mappes et partitions, à l'intérieur de ces zones. Pour plus d'informations, voir «Configuration de l'Agent WebSphere Applications pour surveiller WebSphere Extreme Scale», à la page 947.

Monitoring Agent for WebSphere MQ

L'agent WebSphere MQ est amélioré avec les fonctions suivantes :

- Ajout de la prise en charge de SLES 15 xLinux.
- Ajout de la prise en charge nécessaire à la collecte des statistiques pour le gestionnaire de files d'attente et l'affichage de ces données. Pour plus d'informations, voir «Activation de la surveillance des statistiques de file d'attente pour le gestionnaire de files d'attente IBM MQ», à la page 968.

Améliorations apportées au collecteur de données

collecteur de données J2SE

L'collecteur de données J2SE est amélioré avec les fonctions suivantes :

- Ajout de la prise en charge d'OpenJDK version 9, 10 et 11.
- Ajout de la prise en charge du système d'exploitation Windows Server 2019 (Datacenter et Standard Editions).
- Ajout de la fonction de reconnaissance automatique des classes et méthodes spécifiques des applications J2SE pour le suivi des transactions et la surveillance des données de diagnostic.

Selenium IDE 3.2.X et 3.3.X pour les scripts synthétiques

Si votre abonnement inclut le module complémentaire IBM Website Monitoring on Cloud, Selenium IDE versions 3.2X et 3.3.X est pris en charge ; les scripts et les suites de tests sont sauvegardés au format `.side` plutôt qu'au format `.html` qui est utilisé par les versions précédentes de Selenium IDE. Les scripts `.html` existants sont toujours utilisables. Dans certains cas, il peut s'avérer nécessaire de modifier les scripts `.html` ou de les enregistrer à nouveau dans le nouveau format `.side`.

Pour plus d'informations, voir les sous-rubriques de «Gestion des transactions et des événements synthétiques avec Website Monitoring», à la page 1057 : «Enregistrement de scripts synthétiques», à la page 1058, «Structuration des scripts complexes», à la page 1060 et «Mise à jour des scripts à partir des versions Selenium IDE antérieures», à la page 1061.

Décembre 2018

Nouvel agent

Monitoring Agent for IBM Cloud

Monitoring Agent for IBM Cloud collecte l'inventaire de machine virtuelle et les métriques auprès de votre compte IBM Cloud (Softlayer). L'agent IBM Cloud permet de suivre le nombre de périphériques virtuels que vous avez configurés et qui sont en cours d'exécution dans IBM Cloud. Vous pouvez visualiser les ressources allouées à chaque périphérique virtuel sur la page du tableau de bord détaillé, qui contient également certaines informations telles que le centre de données dans lequel se trouve un périphérique, le système d'exploitation et la bande passante de réseau public prévisionnelle pour le mois.

Améliorations au niveau des agents

Monitoring Agent for Cassandra

L'agent Cassandra a été amélioré et inclut désormais les fonctions suivantes :

- Ajout d'un nouveau seuil nommé `Cassandra_Cluster_Down` qui surveille l'état de l'instance surveillée.
- Ajout de la prise en charge du système d'exploitation Ubuntu 18.04.
- Ajout de la prise en charge de la plateforme SUSE Linux Enterprise Server 15.

Monitoring Agent for Db2

L'agent Db2 est amélioré avec les fonctions suivantes :

- L'agent Db2 prend désormais en charge les fonctions de surveillance HADR pour plusieurs machines de secours.
- L'agent Db2 prend désormais en charge la nouvelle valeur `Stopped` pour l'attribut Database Status.
  Le statut `Stopped` indique que la base de données n'est pas active et qu'aucune connexion active n'est établie bien qu'elle soit opérationnelle et prête à accepter de nouvelles connexions.
- Ajout du nouveau widget `Db2 Server Information` pour afficher des détails sur le serveur Db2.
- Ajout de la nouvelle page `HADR Status – Local Databases` pour afficher des informations sur les bases de données partenaires dans les nouveaux widgets suivants :
  - `HADR Databases Details` est le widget de table qui affiche les valeurs d'attribut importantes pour la base de données partenaire.
  - `Log Gap (History)` est le widget de graphique qui affiche la tendance d'intervalle entre les journaux au fil du temps.
  - `Standby Flag Status` est le widget de table qui affiche les valeurs de statut indicatif pour les machines de secours.
- Ajout du nouveau seuil prédéfini `UDB_HADR_Aux_Standby_Disconnect` pour surveiller les bases de données de secours secondaires dans l'environnement HADR.
- Le widget des 5 premières utilisations de mémoire de base de données a été mis à jour pour afficher la valeur correcte.

- L'agent Db2 prend en charge les plateformes suivantes :
  - Ubuntu zLinux 18.04
  - SUSE Linux Enterprise Server 15 on x86-64 (64 bits)
  - SUSE Linux Enterprise Server 15 for zLinux
  - SUSE Linux Enterprise Server 15 for Power Linux Little Endian

Monitoring Agent for InfoSphere DataStage

L'agent InfoSphere DataStage est amélioré avec les fonctions suivantes :

- Ajout de la capacité à désactiver la collecte de données pour les groupes d'attributs sélectionnés.
- Optimisation de la collecte de données pour le groupe d'attributs d'exécution de travail.
- Ajout de la prise en charge de la plateforme SUSE Linux Enterprise Server 15.

Monitoring Agent for Internet Services

L'Internet Service Monitoring prend désormais en charge les plateformes Windows 64 bits et Linux 64 bits.

Monitoring Agent for Microsoft .NET

L'agent .NET a été amélioré et inclut désormais les fonctions suivantes :

- L'agent .NET permet désormais de suivre les demandes ayant échoué. Le statut de ces demandes est affiché comme `failed` sous le widget de groupe Dernières demandes sur la page Détails des transactions de middleware. De plus, le widget de groupe Dernières erreurs répertorie les demandes récentes ayant échoué ainsi que le code de statut et la description de l'erreur.
- L'agent .NET permet également de surveiller les données utilisateur disponibles via les sessions ASP.NET Identity et ASP.NET. Les données utilisateur s'affichent dans le widget de groupe des 5 premiers utilisateurs sur la page Détails des transactions de middleware.

Monitoring Agent for MongoDB

Agent MongoDB prend en charge la plateforme SUSE Linux Enterprise Server 15.

Monitoring Agent for NetApp Storage

L'agent NetApp Storage est amélioré à l'aide des fonctions suivantes :

- Une nouvelle zone de recherche a été ajoutée sur la page de détails d'événement. Elle permet de filtrer les données d'événement en fonction de critères de recherche.
- Une nouvelle page de détails a été ajoutée pour les numéros d'unité logique.
- L'utilisateur peut désormais vérifier les détails d'un périphérique mappé à chaque objet d'archivage sur la page **Détails**.

Monitoring Agent for OpenStack

Une prise en charge a été ajoutée pour la surveillance des instances de machine virtuelle, comme l'utilisation de l'UC des instances de machine virtuelle, de la mémoire, du disque et du contrôleur d'interface réseau.

Monitoring Agent for PostgreSQL

- Ajout de la prise en charge de SUSE Linux Enterprise Server 15
- Optimisation de la collecte de données pour les groupes d'attributs UC et Mémoire

Monitoring Agent for RabbitMQ

Ajout de la prise en charge de SUSE Linux Enterprise Server 15

Monitoring Agent for SAP Applications

L'Agent SAP prend désormais en charge les plateformes suivantes :

- Plateforme SUSE Linux Enterprise Server 15
- SAP NW RFC SDK 7.50

Monitoring Agent for Skype for Business Server

L'agent Skype for Business Server a été amélioré et inclut désormais les fonctions suivantes :

- Les commandes de transaction synthétique du module Transaction synthétique sont désormais exécutables par les utilisateurs de test déjà configurés. Pour utiliser cette fonction, désactivez l'option permettant d'`utiliser les valeurs de configuration de l'agent` dans le panneau de configuration de l'agent et saisissez une valeur pour `Pool FQDN` pour lequel les commandes synthétiques doivent être exécutées. Assurez-vous que l'utilisateur de test a été configuré à l'aide de la commande NewCsHealthMonitoringConfiguration pour l'identité fournie dans la zone Pool FQDN du panneau de configuration de l'agent.
- Les utilisateurs peuvent désormais désactiver les commandes synthétiques. Pour désactiver l'exécution d'une commande en particulier, saisissez `false` en regard du nom de la commande dans le fichier `LyncSyntheticTrans.exe.config` situé dans `<CANDLE_HOME>\tmaitm6` pour la version 32 bits et dans `<CANDLE_HOME>\TMAITM6_x64` pour la version 64 bits.

Monitoring Agent for Tomcat

- Ajout du nouveau groupe d'attributs Cluster. Il contient des informations sur les propriétés d'un cluster.
- Ajout du nouveau widget Informations du Cluster. Ce widget affiche des informations sur le groupe d'attributs Cluster. Il n'affiche aucune donnée si l'agent surveille une configuration Tomcat non cluster.
- Ajout de la variable *Port du serveur Tomcat* dans le panneau de configuration. Cette variable représente le port sur lequel le serveur Tomcat s'exécute. La valeur par défaut de la variable est 8080.

Monitoring Agent for VMware VI

- La page de composant a été améliorée pour afficher l'adresse IP ou le nom d'hôte du vCenter configuré et sa connectivité avec l'agent.

Agent WebSphere Infrastructure Manager

L'agent WebSphere Infrastructure Manager prend en charge AIX.

Agent WebSphere MQ

L'agent WebSphere MQ est pris en charge sur IBM WebSphere MQ 9.1.

Améliorations apportées au collecteur de données

collecteur de données J2SE

L'collecteur de données J2SE est amélioré avec les fonctions suivantes :

- Ajout de la prise en charge de SUSE Linux Enterprise Server 11 for Power Linux Big Endian (64 bits).
- Ajout de la prise en charge de Power Linux Big Endian (pLinux BE) (64 bits).
- Ajout de la prise en charge de Power Linux Little Endian (pLinux LE) (64 bits).
- Ajout du module de configuration et de la surveillance du serveur Jetty.

Prise en charge de la plateforme étendue pour les agents

Les agents et plateformes suivants sont désormais pris en charge :

Plateforme SUSE Linux Enterprise Server 15

- agent Cassandra
- agent DataPower
- agent DataStage
- agent Db2
- HTTP Server
- agent IBM Integration Bus
- Linux OS

- Agent MongoDB
- Agent OpenStack
- Agent PostgreSQL
- Monitoring Agent for RabbitMQ
- Agent SAP
- agent WebSphere MQ

Power Linux

- collecteur de données J2SE

Ubuntu 18.04

- agent Cassandra
- agent IBM Integration Bus
- Agent OpenStack
- Linux OS
- agent RabbitMQ
- agent WebSphere MQ

Prise en charge de Power 9
Power 9 est maintenant pris en charge pour tous les agents.

Nouveautés de la version 8.1.4 actualisée en octobre 2018

Intégration à Cloud Event Management
Cloud Event Management permet de gérer les incidents en temps réel dans vos services, applications et infrastructure. Désormais, avec l'intégration entre Cloud Event Management et IBM Cloud Application Performance Management, tous les événements générés dans Cloud APM sont envoyés à Cloud Event Management.

Septembre 2018

Nouvel agent disponible
Monitoring Agent for MQ Appliance
L'agent MQ Appliance fournit des informations de surveillance relatives au niveau de MQ Appliances, telles que des informations récapitulatives sur l'UC, la mémoire, le stockage, les capteurs et les gestionnaires de files d'attente.

Améliorations au niveau des agents

Monitoring Agent for Db2
L'agent Db2 prend en charge le système d'exploitation Power Linux Big Endian.

Monitoring Agent for Hadoop

- L'agent Hadoop surveille maintenant l'état de deux autres services : SmartSense et Druid.
- L'agent Hadoop prend maintenant en charge Hortonworks Data Platform (HDP) 3.0.0.

Internet Service Monitoring agentAgent
Les fonctionnalités d'édition de l'agent Internet Service Monitoring agent sont améliorées. Tous les moniteurs qui possèdent des paramètres configurables peuvent être modifiés.

Monitoring Agent for MySQL
L'agent MySQL prend maintenant en charge la surveillance de MySQL v8.0.11.

Monitoring Agent for NetApp Storage
L'agent NetApp Storage est amélioré à l'aide des fonctions suivantes :

- Un nouveau widget, Overall Events Summary, est ajouté à la page Instance de stockage NetApp. Il affiche le nombre total d'événements. Vous pouvez afficher tous les événements survenus

dans l'environnement, indépendamment de leur gravité ou de leur objet en cliquant sur la barre d'état, sous le nom Total Events.

De plus, une colonne Statut de l'événement est ajoutée dans chaque table d'objets. Elle affiche l'état des événements, classés en fonction de l'heure et du niveau de gravité.

La page Instance de stockage NetApp affiche maintenant la table Events Summary au lieu d'un graphique.

- La page Aggregate Details est mise à jour pour afficher les périphériques connexes qui sont associés à l'agrégat sélectionné.

Monitoring Agent for SAP Applications
Ajout de la prise en charge de SAP NW RFC SDK 750.

Monitoring Agent for SAP HANA Database
Ajout de deux nouvelles fonctions :

- La base de données SAP HANA peut être surveillée en mode veille.
- Agent SAP HANA Database prend en charge la plateforme Big Endian pour Power System.

Monitoring Agent for VMware VI

- La surveillance de **`HostVFlashManager`** est maintenant prise en charge
- Le tableau de bord du serveur ESX affiche maintenant le nombre de machines virtuelles dont l'utilisation de l'UC est à l'état Critique, Avertissement et Normal.

Nouvelle plateforme : Linux on POWER Big Endian
Une nouvelle plateforme est disponible. Les agents suivants sont désormais pris en charge sous Linux on POWER Big Endian :

- agent Db2
- agent IBM Integration Bus
- Linux OS
- Agent SAP HANA Database
- agent WebSphere MQ
- Agent WebSphere Applications

Juillet 2018

Nouveaux agents disponibles

Monitoring Agent for Sybase Server

L'agent Sybase offre un point central de gestion des bases de données réparties. Il collecte les informations requises pour que les administrateur de base de données et système puissent examiner les performances du système Sybase Server, détecter rapidement les problèmes et les empêcher.

Améliorations au niveau des agents

Monitoring Agent for Hadoop

- Ajout de la prise en charge de la surveillance des services Hadoop, tels que Mahout, Atlas et Falcon.
- Ajout de la prise en charge de la surveillance de l'offre Hadoop : Cloudera CDH 5.13.
- Ajout de la prise en charge de la surveillance de l'offre Hadoop : Hortonworks HDP 2.6.4.

Monitoring Agent for HMC Base

HMC V8 R8.7.0 est désormais pris en charge.

Monitoring Agent for HTTP Server
Ajout de la prise en charge d'Apache HTTP Server 64 bits sous Windows.

Monitoring Agent for Microsoft .NET

Monitoring Agent for Microsoft .NET a été étendu comme suit :

- Le module de temps de réponse IIS surveille maintenant la répartition des temps de rendu et des sous-transactions via l'injection JavaScript pour les formulaires Web ASP.NET (pages .aspx) et les vues MVC Razor ASP.NET, qui remplissent les conditions suivantes :
  - La page respecte les normes HTML W3C.
  - Les en-têtes de réponse contiennent `Content-Type: text/html, application/xml,application/json`.
  - Le contenu de réponse inclut l'élément *<head>*.
- L'agent .NET télécharge les données d'analyse approfondie sur le service DQE (Diagnostic Query Engine), sur le serveur APM. Le tableau de bord d'analyse approfondie du service DQE charge et affiche rapidement les données.
- Le nouveau seuil **`NET_Slow_IIS_Request_Crit`** a été ajouté. Il est déclenché si le widget des 10 demandes les plus lentes contient des demandes dont le temps de réponse est supérieur à 500 millisecondes.
- L'outil de filtrage sélectif est mis à jour avec la zone de recherche pour rechercher un pool d'applications dans la liste des pools d'applications.
- L'utilitaire **`ProcListCaller`** est ajouté pour fournir la liste des processus ayant chargé le profileur CLR de l'agent .NET (`CorProfLog.dll`).

Monitoring Agent for Microsoft SQL Server

- L'agent Microsoft SQL Server prend désormais en charge plusieurs classements dans l'analyse syntaxique ERRORLOG en fonction des paramètres de classement du fichier `koqErrConfig.ini`. Si le fichier `koqErrConfig.ini` ne contient pas de paramètres de classement valides, vous ne pourrez voir que le message d'erreur anglais par défaut dont le niveau de gravité est supérieur au niveau de gravité par défaut (s'il en existe un). Le niveau de gravité par défaut est de 17. Tous les classements qui se trouvent dans le fichier `koqErrConfig.ini` sont pris en compte lors de l'analyse syntaxique du fichier ERRORLOG. Par conséquent, les classements en cours d'utilisation doivent être ajoutés dans le fichier `koqErrConfig.ini`. L'analyse syntaxique du fichier ERRORLOG étant sensible à la casse, vous devez vous assurer que les valeurs des mots clés de classement dans le fichier `koqErrConfig.ini` sont identiques à celles du fichier ERRORLOG ou du fichier `koqErrConfigSample.ini` de référence. Notez que les modifications apportées au fichier `koqErrConfig.ini` ne sont pas conservées lors de la mise à niveau de l'agent ; vous devez effectuer une sauvegarde au préalable.
- L'agent fournit également l'utilitaire **`koqVerifyPermissions.exe`** pour vérifier si un utilisateur SQL Server existant dispose de droit suffisants pour surveiller Microsoft SQL Server. Si un utilisateur SQL Server existant ne dispose pas de droits suffisants, vous pouvez utiliser l'utilitaire **`permissions.cmd`** comme autre moyen d'octroyer les droits minimaux à un utilisateur SQL Server existant pour la collecte des données.

Monitoring Agent for NetApp Storage

Monitoring Agent for NetApp Storage a été étendu comme suit :

- La nouvelle page Composant a été ajoutée pour afficher les détails de l'état de connexion de l'agent que le fournisseur de données soit actif ou inactif, avec l'adresse IP des sources de données surveillées. La barre de statut individuelle représente le nombre de noeuds, d'agrégats, de volumes et de disques à l'état critique, normal, avertissement ou inconnu.
- La nouvelle page Instance de stockage NetApp a été ajoutée pour mettre en évidence les principales propriétés des clusters, agrégats, volumes, disques et serveurs virtuels. Elle affiche également un graphique Events Summary qui indique le nombre d'événements correspondant à chaque entité de l'environnement. Par exemple, si 12 volumes sont configurés et que chacun comporte deux événements de niveau de gravité Critique, le diagramme Event Summary illustre le nombre total d'événements survenus dans tous les volumes disponibles dans un

environnement. Dans ce cas, le diagramme affiche une barre comportant 24 événements critiques comparés au volume sous forme d'entité tracée sur l'axe des X.

- La page Node Details a été mise à jour pour afficher les détails des ports réseau.
- La page Volume Detail a été mise à jour pour afficher les détails des miroirs des instantanés associés et le nombre d'unités logiques de chaque volume sélectionné.
- La page vServers Details a été mise à jour pour afficher les informations sur les interfaces logiques du réseau.

Monitoring Agent for Tomcat

Le serveur Tomcat V9.0.5 est désormais pris en charge.

Monitoring Agent for WebSphere MQ

La surveillance éloignée est prise en charge. Deux paramètres de configuration ont été ajoutés pour que l'agent puisse collecter les données de surveillance d'un gestionnaire de files d'attente éloignées. Toutefois, ces paramètres de configuration n'ont aucun impact sur un gestionnaire de files d'attente locales. Si vous souhaitez configurer l'agent pour qu'il surveille un gestionnaire de files d'attente locales, vous pouvez appuyer sur Entrée pour ignorer la spécification de ces paramètres.

Pour plus d'informations sur la configuration de l'agent, voir «Configuration de l'agent WebSphere MQ», à la page 961.

Amélioration de la personnalisation de l'emplacement de la fonction d'intégration d'événements

Vous pouvez désormais ajouter plusieurs valeurs d'attribut et valeurs littérales à l'emplacement de la fonction d'intégration d'événements. Ainsi, par exemple, au lieu d'un message `Disk free percent is` **`Disk_Free_Percent`** pour un seuil qui vérifie si l'espace disque disponible est faible, vous pourriez avoir le message `Disk free percent is` **`Disk_Free_Percent`** `and inodes free percent is` **`Inodes_Free_Percent`**. Le message transmis peut se présenter comme suit : `Disk free percent is 13 and inodes free percent is 9`. Pour plus d'informations, voir «Personnalisation d'un événement à transmettre à un récepteur EIF», à la page 1019.

Avril 2018

Nouvel agent disponible

Monitoring Agent for AWS Elastic Load Balancer

L'agent Amazon ELB permet de surveiller de manière centralisée la santé, la disponibilité et les performances de vos équilibreurs de charge élastiques AWS. L'agent affiche un ensemble complet de mesures pour chaque type d'équilibreur de charge, application, réseau et classique, qui vous aident à prendre des décisions avisées concernant votre environnement AWS Elastic Load Balancer.

Améliorations au niveau des agents

Agent de surveillance des temps de réponse

Le module IBM HTTP Server Response Time prend en charge IBM HTTP Server versions 7, 8 et 9 sous Windows.

Monitoring Agent for Node.js

Par défaut, les informations sensibles de l'utilisateur, telles que les cookies, les contextes de demande HTTP et les contextes de requête de base de données, ne sont plus collectées par le collecteur de données Node.js. Vous pouvez modifier ce comportement par défaut en spécifiant la nouvelle variable d'environnement, *SECURITY_OFF*.

Monitoring Agent for Amazon EC2

Le nom du composant reflète désormais le nom de l'agent.

La conservation étendue des données est désormais prise en charge.

Monitoring Agent for WebLogic

Le suivi des transactions et le diagnostic approfondi sont activés sous AIX. Auparavant, ces fonctions n'étaient activées que sous Linux et Windows.

L'analyse détaillée Récapitulatif des demandes pour les servlets implémentés avec des annotations pour le suivi des transactions et le diagnostic approfondi a été améliorée.

Monitoring Agent for Skype for Business Server
Prise en charge de Windows Server 2016.

Monitoring Agent for Sterling File Gateway
Par défaut, l'agent extrait les événements relatifs au transfert de fichier ayant échoué. Vous pouvez modifier ce comportement par défaut en spécifiant la valeur appropriée pour la nouvelle variable d'environnement **KFG_ALL_FGEVENTS**.

Monitoring Agent for Sterling Connect Direct
La fonction de consignation de l'agent a été améliorée. Pour plus d'informations, voir la section de traitement des incidents.

Améliorations apportées au collecteur de données

collecteur de données Node.js
Par défaut, les informations sensibles de l'utilisateur, telles que les cookies, les contextes de demande HTTP et les contextes de requête de base de données, ne sont plus collectées par le collecteur de données Node.js. Vous pouvez modifier ce comportement par défaut en spécifiant la nouvelle variable d'environnement, *SECURITY_OFF*.

A faire : Pour obtenir cette amélioration, vous devez télécharger et appliquer le correctif temporaire 1 du collecteur de données Node.js IBM Cloud Application Performance Management à partir d'IBM Fix Central. Pour plus d'informations, voir Interim Fix 1 Readme File.

collecteur de données J2SE
La reconnaissance automatique de la classe de point d'entrée (classe Main) et du nom d'alias de l'application J2SE est désormais prise en charge.

Le suivi des transactions et le diagnostic approfondi peuvent être activés et désactivés en local à l'aide des scripts de configuration.

Améliorations apportées à la documentation
Une page Web a été créée dans Application Performance Management Developer Center pour vous aider à trouver le niveau de l'agent dans chaque révision ou édition. Pour plus d'informations, voir Agent version in Cloud APM releases.

Le tableau Fonctions de l'agent et du collecteur de données dans chaque offre a été simplifié pour une meilleure lisibilité. Pour plus d'informations, voir «Fonctions», à la page 55.

Février 2018

Nouvel agent disponible

Monitoring Agent for Azure Compute

L'Agent Azure Compute permet de surveiller de manière centralisée la santé, la disponibilité et les performances de vos instances Azure Compute. L'agent affiche un ensemble complet de mesures qui vous aident à prendre des décisions avisées concernant votre environnement Azure Compute. Ces métriques incluent l'utilisation de l'UC, l'utilisation du réseau et les performances du disque.

Monitoring Agent for Sterling Connect Direct

Vous pouvez utiliser l'Agent Sterling Connect Direct pour surveiller la santé et les performances du serveur Sterling Connect Direct. Il surveille les fonctions du serveur Sterling Connect Direct, telles que les activités de transfert de fichiers, les processus planifiés et les processus de mise en attente et de file d'attente. Cet agent multi-instance prend en charge la surveillance à distance.

Monitoring Agent for Sterling File Gateway

L'Agent Sterling File Gateway surveille l'application Sterling File Gateway, utilisée pour transférer des fichiers entre les partenaires internes et externes à l'aide de différents protocoles, différentes conventions de dénomination de fichier et différents formats de fichier. Il prend également en charge la fonction de surveillance à distance.

Améliorations au niveau des agents

Monitoring Agent for DataPower
Le suivi des transactions entre l'agent WebSphere MQ et l'agent DataPower est pris en charge.

Monitoring Agent for Db2
Ajout de la prise en charge de la surveillance à distance.

Monitoring Agent for Hadoop
Ajout de la prise en charge de la surveillance du statut des services Hadoop, tels que HBase, MapReduce2, Tez et Ranger.

La prise en charge de la surveillance de l'offre Hadoop : Cloudera CDH 5.12 a été ajoutée.

Monitoring Agent for InfoSphere DataStage
Ajout de la prise en charge de MS SQL en tant que référentiel de métadonnées.

La prise en charge du système d'exploitation Windows a été ajoutée.

Monitoring Agent for Tomcat
Prise en charge du suivi des transactions et de l'analyse approfondie pour PLinux en mettant à niveau l'infrastructure de l'agent avec le correctif 8.1.4.0-IBM-APM-SERVER-IF0001.

Monitoring Agent for SAP Applications
Amélioration de la fonction CCMS : automatisation de la suppression du fichier `idx`. Cette automatisation fonctionne uniquement lorsque le système SAP est redémarré.

Monitoring Agent for Microsoft .NET
La prise en charge des transactions d'utilisateur final à l'aide du module de temps de réponse IIS a été ajoutée.

Monitoring Agent for Skype for Business Server
Le nom de l'agent Monitoring Agent for Microsoft Lync Server est modifié en Monitoring Agent for Skype for Business Server.

Monitoring Agent for Linux KVM
Ajout de la prise en charge de RHEV-M 4.x.

Monitoring Agent for Linux OS
L'intervalle de transfert de mémoire est redéfini sur 1 minute.

L'adresse IP associée à l'interface réseau s'affiche sur le tableau de bord du système d'exploitation Linux et sur le widget System Information.

Monitoring Agent for UNIX OS
L'intervalle de transfert de mémoire est redéfini sur 1 minute.

Améliorations apportées au collecteur de données

collecteur de données J2SE
Ajout de la prise en charge des applications Spring Boot.

Améliorations apportées à Availability Monitoring
Grâce au module complémentaire Availability Monitoring, vous pouvez désormais créer des listes blanches et des listes noires répertoriant les URL auxquelles vos tests peuvent et ne peuvent pas accéder. Votre liste blanche et votre liste noire contrôlent les dépendances et ressources qui contribuent aux temps de réponse de vos applications Web testées, par exemple, des mesures tierces. Filtrez les URL par schéma, domaine ou type de fichier en utilisant des caractères génériques.

Décembre 2017

Nouvel agent disponible

Monitoring Agent for InfoSphere DataStage

L'agent DataStage permet de surveiller la santé et les performances des ressources du serveur DataStage, telles que les services de moteur, les systèmes de moteur, l'activité des tâches,le statut d'exécution des tâches et les détails d'exécution des tâches. Cet agent prend en charge la surveillance à distance.

Améliorations au niveau des agents

Monitoring Agent for Hadoop

Ajout de la prise en charge de la surveillance d'un cluster Hadoop sécurisé avec l'authentification basée sur Kerberos SPNEGO, qui utilise le centre de distribution de clés (KDC) Active Directory.

Ajout de la prise en charge des tests de connexion aux hôtes d'un cluster Hadoop sécurisé avec l'authentification basée sur Kerberos SPNEGO, qui utilise le centre de distribution de clés (KDC) MIT ou Active Directory.

Ajout de la prise en charge de la surveillance des offres Hadoop suivantes : Cloudera CDH 5.10 et CDH 5.11.

Ajout de la prise en charge de la surveillance du statut des services Hadoop tels que Flume, Kafka, Titan, Spark, Knox, Pig, Slider et Solr.

Monitoring Agent for HTTP Server

Ajout de la prise en charge de IBM HTTP Server et d'Apache HTTP Server Windows 32 bits.

Ajout de la prise en charge de Linux for System z (le suivi des transactions n'est pas supporté).

Ajout de la prise en charge d'Oracle HTTP Server sous Linux for System.

Monitoring Agent for IBM Integration Bus

Ajout de la prise en charge de Linux for Power Systems (Little Endian).

Monitoring Agent for Microsoft .NET

Ajout de la prise en charge de la surveillance d'ODP.NET.

Ajout des détails de trace de la méthode HttpWebRequest.GetResponse().

Monitoring Agent for Microsoft SQL Server

Ajout de la prise en charge de la tolérance pour SQL Server 2017.

Ajout de la prise en charge de la fonction Always On pour l'édition SQL Server destinée aux développeurs.

Monitoring Agent for MySQL

Ajout de la prise en charge de la tolérance des tables de schéma d'informations migrées vers le schéma de performances.

Ajout de la prise en charge des tables obsolètes du schéma d'informations via le schéma de performances.

Monitoring Agent for Microsoft Internet Information Services

Ajout de la prise en charge de la surveillance des sites Web FTP.

Monitoring Agent for MongoDB

Ajout de la prise en charge de la surveillance à distance.

Ajout de la prise en charge de la surveillance du moteur de stockage en mémoire.

Monitoring Agent for OpenStack

Ajout de la prise en charge de l'API OpenStack Authentication version 3.

Monitoring Agent for Oracle Database

La version d'agent est passée à la version 8.0.

Ajout du paramètre de configuration **Oracle JDBC jar file** et suppression des paramètres de configuration **Oracle Home Directory** et **Oracle Instant Client Installation Directory**.

Monitoring Agent for PostgreSQL

Ajout de la prise en charge de la surveillance à distance.

Monitoring Agent for SAP Applications

Ajout de la prise en charge de la communication SNC.

Ajout d'un nouveau seuil pour l'arrêt des systèmes SAP.

Monitoring Agent for SAP NetWeaver Java Stack
Ajout de la fonction de restauration de l'instance SAP NetWeaver Application Server.

Monitoring Agent for Tomcat
Ajout de la prise en charge de Linux for Power Systems (Little Endian) (surveillance des ressources uniquement).

Monitoring Agent for VMware VI
Ajout des paramètres Résumé de réseau et Nombre de disques sur la page de présentation du serveur ESX Server.

Ajout du widget de groupe Evénements sur la page Récapitulatif de cluster.

Monitoring Agent for WebSphere Applications
Ajout de la prise en charge du suivi des transactions pour Linux for Power Systems (Little Endian) et Linux for System z.

A faire : Pour bénéficier de la prise en charge du suivi des transactions sous Linux for Power Systems (Little Endian) et Linux for System z, procédez comme suit :

1. Téléchargez l'image d'installation de l'agent.
2. Installez l'Agent WebSphere Applications.
3. Téléchargez le correctif temporaire 2 pour l'Agent WebSphere Applications à partir de Fix Central.
4. Suivez les instructions indiquées dans le fichier Readme du correctif temporaire pour l'appliquer.

Monitoring Agent for WebSphere MQ
Ajout du widget de groupe Statut de service MQ qui fournit des détails sur le service MQ.

Ajout de la prise en charge de Linux for Power Systems (Little Endian).

Améliorations apportées au collecteur de données

collecteur de données Liberty
Modification du nom de système géré (MSN) enregistré par le collecteur de données Liberty afin de refléter le nom d'hôte et le nom du serveur Liberty. Le nouveau MSN de ce collecteur de données est `BI:`*`nomserveur_nomhôte_md5`*`:BLP`, où *md5* est le GUID de l'application locale basé sur MD5. La longueur de *nomserveur_nomhôte_md5* est de 25 caractères.

A faire : Pour obtenir cette amélioration, vous devez télécharger et appliquer le correctif intermédiaire 1 du collecteur de données IBM Cloud Application Performance Management Liberty à partir de Fix Central.

collecteur de données J2SE
Ajout de la prise en charge du suivi des transactions des applications J2SE.

Améliorations apportées à la documentation
Ajout d'informations sur les ports par défaut utilisés par les agents et les collecteurs de données afin de vous aider à préparer l'environnement. Voir «Ports par défaut utilisés par les agents et collecteurs de données», à la page 85 .

Ajout d'informations sur les noms de système gérés (MSN) des agents Cloud APM. Des instructions sur la procédure de modification de la chaîne de nom d'hôte du MSN sont également fournies. Voir «Noms de systèmes gérés», à la page 171 .

Ajout d'informations sur l'exécution d'un agent en tant qu'utilisateur non-administrateur ou sur les droits requis à cet effet dans les rubriques de configuration associées aux agents suivants :

- agent Microsoft .NET
- agent Microsoft Active Directory
- agent Microsoft Exchange Server
- Agent Skype for Business Server
- agent MicrosoftSharePoint Server

- agent Microsoft SQL Server
- Agent Tomcat

Août 2017

IBM Cloud Application Performance Management, Availability Monitoring

Le module complémentaire Availability Monitoring offre une surveillance synthétique améliorée de vos applications Web à partir de plusieurs points de présence dans le monde. Créez des tests synthétiques qui imitent le comportement utilisateur à des intervalles réguliers. Exécutez vos tests à partir de points de présence publics, ou téléchargez et déployez vos propres points de présence sur des serveurs locaux ou privés. Utilisez le tableau de bord Availability Monitoring pour surveiller la disponibilité, les performances et les alertes des applications à l'aide de graphiques, de tables de répartition et de vues de carte. Utilisez l'analyse en cascade pour identifier les problèmes de performance et de disponibilité et savoir pour quelles raisons ils surviennent.

Surveillance d'IBM API Connect

Les agents et les collecteurs de données Cloud APM prennent maintenant en charge la surveillance de l'environnement IBM API Connect. Vous pouvez déployer les agents et les collecteurs de données correspondants pour obtenir un aperçu de la santé et des performances des composants de votre environnement. Les données de suivi des transactions sont également disponibles, en plus des données de surveillance et de diagnostic approfondi des transactions, ce qui vous permet d'afficher les informations de topologie concernant votre environnement IBM API Connect. Pour plus d'informations, voir «Scénario : Surveillance d'IBM API Connect», à la page 90.

Prise en charge de systèmes d'exploitation

Linux for System z

Ajout de la prise en charge de Linux for System z pour les agents de surveillance suivants : Linux OS, WebSphere Application, Db2, WebSphere MQ, IBM Integration Bus, Tomcat et Surveillance des temps de réponse.

Linux for Power Systems (Little Endian)

Ajout de la prise en charge de Linux for Power Systems (Little Endian) pour les agents de surveillance suivants : Linux OS, WebSphere Application et Db2.

Linux for System x

Ajout de Linux on System x pour prendre en charge le collecteur de données Liberty.

Prise en charge de l'agent de système d'exploitation IBM i

Les données de l'agent de système d'exploitation IBM i peuvent maintenant être affichées dans la console Cloud APM. Cet agent est un agent IBM Tivoli Monitoring V6 et reste un agent V6 pour la version 8.1.4. Vous pouvez utiliser la Passerelle hybride pour extraire les données d'agent et les envoyer au serveur Cloud APM. Ainsi, vous pouvez visualiser les données de surveillance et les événements associés à cet agent dans la console Cloud APM. Pour plus d'informations sur l'agent de système d'exploitation IBM i, voir Hybrid Gateway supported agents (APM Developer Center).

Nouveaux agents disponibles

Monitoring Agent for OpenStack

Vous pouvez utiliser l'Agent OpenStack pour surveiller la santé et les performances de vos applications OpenStack et afficher des informations, par exemple, sur les noeuds finaux d'API, la connexion au serveur SSH, les processus et les hyperviseurs.

Collecteurs de données nouveaux et améliorés disponibles

Vous pouvez utiliser les collecteurs de données pour surveiller la santé et les performances des applications suivantes sur IBM Cloud et/ou sur site :

collecteur de données J2SE

Vous pouvez utiliser le collecteur de données J2SE pour surveiller la santé et les performances des applications Java et afficher les données de diagnostic, telles que le temps de réponse, la capacité de traitement, le contexte de demande et la trace de méthode des demandes.

collecteur de données Liberty
Le collecteur de données Liberty surveille à la fois le profil Liberty dans l'environnement IBM Cloud et le profil Liberty local sur Linux for System x.

collecteur de données Node.js
Le collecteur de données Node.js surveille à la fois les applications IBM Cloud et sur site. Vous pouvez visualiser à la fois les données de surveillance des ressources et des diagnostics, telles que l'utilisation des ressources, le débit, et les informations détaillées au sujet des requêtes et des méthodes.

collecteur de données Python
Le collecteur de données Python surveille les applications IBM Cloud. Vous pouvez visualiser à la fois les données de surveillance des ressources et des diagnostics, telles que l'utilisation des ressources, le débit, et les informations détaillées au sujet des requêtes et des méthodes.

L'Agent Python est supprimé du module d'installation d'agent dans Cloud APM version 8.1.4. Pour pouvez utiliser uniquement le collecteur de données Python pour surveiller vos applications Python.

collecteur de données Ruby
Le collecteur de données Ruby surveille uniquement les applications IBM Cloud. Vous pouvez visualiser à la fois les données de surveillance des ressources et des diagnostics, telles que l'utilisation des ressources, le débit, et les informations détaillées au sujet des requêtes et des méthodes.

Améliorations au niveau des agents

Monitoring Agent for Amazon EC2

- L'agent peut traiter correctement les dates de fin null pour les événements planifiés.
- Ajout de la prise en charge d'un proxy direct entre l'agent Amazon EC2 et Amazon Web Services.

Monitoring Agent for Citrix Virtual Desktop Infrastructure

- Ajout de la surveillance des événements Windows et des métriques PowerShell même si l'agent est installé sur un système Linux.
- Ajout de la page **Sessions VDA**, accessible par l'intermédiaire de la page **Détails de la machine VDA**.
- Ajout du widget des métriques de machine à la page **Détails de la machine VDA**.
- Amélioration de la configuration DDC (Desktop Delivery Controller) pour permettre à l'agent de traiter la reprise DDC dans un environnement distribution.

Monitoring Agent for Db2

- Ajout du support pour Linux for System z.

Monitoring Agent for Hadoop

- Ajout du support pour la surveillance des offres Hadoop suivantes : Hortonworks HDP 2.6 et Cloudera CDH 5.9, 5.10 et 5.11
- Ajout du support pour la surveillance du statut des services Hadoop, tels que ZooKeeper, Sqoop, Hive, HDFS, YARN, Ambari Metrics et Oozie.
- Ajout du support pour la surveillance d'un cluster Hadoop sécurisé avec l'authentification basée sur Kerberos SPNEGO qui utilise uniquement le centre de distribution de clés (KDC) de MIT Kerberos V5.

Monitoring Agent for IBM Integration Bus

Ajout de la prise en charge de Linux for System z (le suivi des transactions n'est pas supporté).

Monitoring Agent for JBoss

- Le processus de configuration du suivi et des diagnostics approfondis des transactions a été simplifié pour l'agent JBoss dans l'offre Advanced Agents.

- Ajout de deux widgets de tableau de bord à la page **Détails sur la récupération de place**. L'un d'eux affiche la quantité de segment de mémoire libérée depuis la dernière récupération de place, et l'autre affiche les tailles historiques du pool de mémoire dynamique Eden/Survivor/Tenured (ancienne génération).

Monitoring Agent for Linux OS

Ajout du support pour Linux for Power Systems (Little Endian).

Monitoring Agent for Skype for Business Server

- Ajout du widget de groupe Lync Usage Summary au tableau de bord Lync Server Overview pour afficher le statut d'enregistrement en avant-plan et la qualité des appels médiocres.
- Ajout d'un tableau de bord pour afficher les détails de l'utilisation de Microsoft Lync Server.

Monitoring Agent for SAP NetWeaver Java Stack

Les améliorations suivantes ont été ajoutées au tableau de bord de l'Agent SAP NetWeaver Java Stack :

- Des ensembles de données, des widgets de groupe et des pages ont été ajoutés pour collecter et afficher les données de diagnostic et de suivi des transactions.
- Ajout du support pour l'installation et la configuration de l'agent sur les systèmes Windows 2016.
- Ajout du widget de groupe Cinq premières demandes les plus lentes par temps de réponse au tableau de bord SAP NW Java Instance pour fournir des informations sur les 5 premières demandes envoyées par l'utilisateur à l'application dont le temps de réponse est le plus élevé.
- Les informations de diagnostic sur les demandes qui s'affichent dans le widget de groupe Cinq premières demandes les plus lentes par temps de réponse sont visibles dans la page Instances de demande en cliquant sur la demande. Le support pour l'affichage des informations de diagnostic sur les demandes figurant dans le widget de groupe Cinq premières demandes les plus lentes par temps de réponse a été ajouté.
- Le widget de groupe Cinq premières sessions utilisateur par temps de réponse est supprimé.

Monitoring Agent for MongoDB

Ajout du support pour la surveillance du cluster MongoDB ou de la configuration de réplication en cas de défaillance du noeud principal.

Monitoring Agent for MySQL

Ajout de jeux de données et d'un paramètre de configuration pour surveiller les ressources MySQL à distance.

Monitoring Agent for NetApp Storage

- Mise à jour de la page des composants pour afficher les informations récapitulatives des clusters et serveurs virtuels.
- Mise à jour de la page Instance de stockage NetApp pour afficher les informations sur les clusters.

Monitoring Agent for Node.js

Les améliorations suivantes ont été ajoutées à l'Agent Node.js pour optimiser les mesures d'application des noeuds (Appmetrics) :

- Nouveaux widgets de tableau de bord et de groupe pour afficher les détails de la récupération de place
- Nouveaux widgets de tableau de bord et de groupe pour afficher les détails des boucles d'événements

Monitoring Agent for PostgreSQL

- Support pour l'installation et la configuration de l'agent sur les systèmes Windows.
- Support pour la surveillance de PostgreSQL V9.6.

- Mise à jour de la page **Présentation des statuts** de façon à ce que le statut ne soit pas critique lorsque le taux de réussite en mémoire tampon est égal à zéro.

Monitoring Agent for SAP HANA Database

L'attribut Nombre de jours avant expiration de la licence et les seuils HANA_License_Expiry_Crit_SYS et HANA_License_Expiry_Warn_SYS ont été ajoutés pour surveiller le nombre de jours restants avant l'expiration de la licence.

Monitoring Agent for Tomcat

- Ajout du support pour Linux for System z
- Ajout de jeux de données, tableaux de bord et widgets de groupe pour le suivi et les diagnostics approfondis des transactions.

Monitoring Agent for VMware VI

Mise à jour du widget de groupe Serveur ESX dans le tableau de bord Récapitulatif du serveur pour afficher le statut SSH.

Monitoring Agent for WebLogic

Le suivi et les diagnostics approfondis des transactions ont été ajoutés à l'agent dans l'offre Advanced Agents.

Monitoring Agent for WebSphere Applications

Ajout de la prise en charge de Linux for System z (le suivi des transactions n'est pas supporté).

Monitoring Agent for WebSphere MQ

Ajout de la prise en charge de Linux for System z (le suivi des transactions n'est pas supporté).

Les données d'historique à long terme de file d'attente et de canal sont prises en charge. Une fois le gestionnaire de files d'attente configuré pour collecter les données statistiques de file d'attente ou de canal, vous pouvez configurer l'agent pour activer la collecte des données d'historique à long terme de file d'attente ou de canal. Bien qu'il n'existe pas de tableau de bord ni de widget prédéfini pour afficher les données d'historique à long terme, vous pouvez utiliser l'onglet **Détails d'attribut** pour demander les données collectées dans vos tables personnalisées.

Agent de surveillance des temps de réponse

- Ajout de la prise en charge du IBM HTTP Server Windows 32 bits et d'Apache HTTP Server.
- Ajout d'une prise en charge de la configuration du suivi d'utilisateur pour les applications sur la page **Configuration d'agent**.
- Ajout d'une prise en charge de la configuration du suivi de session pour les applications sur la page **Configuration d'agent**.

Amélioration de la visualisation

Vues personnalisées

Vous pouvez utiliser la vue Vue universelle d'IBM Cloud Application Business Insights pour créer des pages personnalisées pour les applications que vous surveillez. Dans l'onglet Vues personnalisées, vous pouvez utiliser un modèle existant ou créer des modèles personnalisés pour votre page. Vous avez le choix entre plusieurs options de graphique et de mesure pour créer des widgets permettant de surveiller les données en fonction de vos besoins.

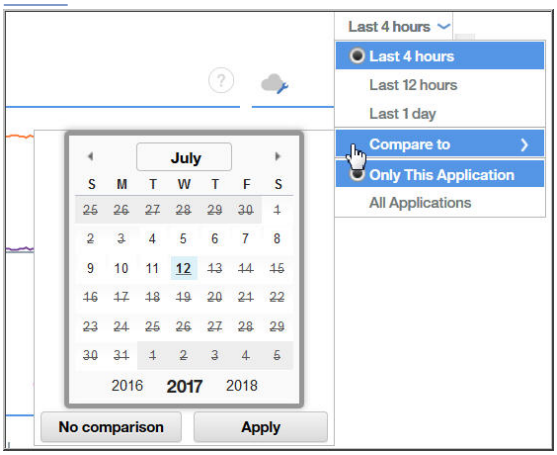
En utilisant la Vue universelle, vous pouvez créer des tableaux de bord pour surveiller les données de plusieurs agents. Vous pouvez exporter les données de pages personnalisées dans un fichier de données brutes.

Pour plus d'informations, voir «Vues personnalisées», à la page 1144.

Calendrier pour la comparaison des données d'un jour précédent

Lorsque vous affichez des graphiques à courbes contenant des données d'historique, un calendrier s'ouvre une fois que vous avez choisi une option de sélecteur de temps pour comparer

une plage horaire d'un jour précédent. Les jours disponibles pour la comparaison sont barrés. Pour plus d'informations, voir «Ajustement et comparaison de mesures dans le temps», à la page 1121.



Amélioration d'Agent Builder

Si vous créez un agent pour surveiller les données d'une base de données JDBC (Java Database Connectivity), vous pouvez modifier les valeurs d'énumération définies pour Erreur, Données manquantes et Aucune valeur, pour éviter tout chevauchement avec les valeurs légitimes de la base de données.

Vous pouvez définir l'autorité d'horodatage des fichiers JAR dans la fenêtre **Préférences** d'Agent Builder. Si le certificat signataire de l'autorité d'horodatage par défaut arrive à expiration, en définissant une nouvelle autorité, vous pouvez continuer de vérifier les fichiers JAR.

Amélioration de l'intégration

Emplacements personnalisables de la fonction d'intégration d'événements pour les événements
Après avoir configuré la transmission d'événements, vous pouvez personnaliser le message d'emplacement de base de la fonction d'intégration d'événements pour les événements envoyés à un récepteur, tel que Netcool/OMNIbus. L'éditeur de seuil comporte une nouvelle zone **Acheminer l'événement de fonction d'intégration d'événements EIF ?** et le bouton **Personnalisation de l'attribut EIF** permettant de personnaliser comment les événements sont mappés vers des événements transmis. Pour plus d'informations, voir «Personnalisation d'un événement à transmettre à un récepteur EIF», à la page 1019.

Plusieurs Passerelles hybrides
Dans les précédentes éditions, vous pouvez installer la Passerelle hybride dans un seul domaine IBM Tivoli Monitoring comportant un Tivoli Enterprise Monitoring Server concentrateur. Vous pouvez maintenant installer une Passerelle hybride dans plusieurs domaines Tivoli Monitoring. La catégorie de la Passerelle hybride dans la page **Configuration avancée** de la console Cloud APM a été déplacée vers sa propre page **Gestionnaire de passerelle hybride**. Vous pouvez créer et modifier les profils Passerelle hybride pour les systèmes gérés de surveillance à partir de plusieurs domaines Tivoli Monitoring, un profil pour chaque domaine. Pour plus d'informations, voir «Passerelle hybride», à la page 979.

Evolutivité améliorée

Augmentation du nombre maximal de systèmes gérés que vous pouvez surveiller à partir d'un Cloud APM de 4 000 à 10 000 systèmes gérés.

Versions précédentes

Pour plus d'informations sur les nouvelles fonctions et options des éditions précédentes, reportez-vous aux rubriques *Nouveautés* suivantes :

- «Nouveautés : avril 2017», à la page 28
- «Nouveautés : septembre 2016», à la page 34

- Nouveautés : avril 2016

Nouveautés : avril 2017

De nouvelles fonctions, options et offres sont disponibles depuis l'édition d'avril 2017 de Cloud APM.

Nouvel Application Performance Management Developer Center

L'APM Developer Center est un emplacement central à partir duquel vous pouvez accéder à des ressources pour les produits APM : blogues, vidéos, documentation, support, événements, IBM Marketplace, et d'autres ressources. Le menu **Aide** de la console Cloud APM contient un lien pratique vers Application Performance Management Developer Center.

Nouvelle stratégie de marque et simplification du produit

IBM Performance Management on Cloud a été rebaptisé en IBM Cloud Application Performance Management. Les noms de composant ont également changé. Par exemple, la console Cloud APM et le serveur Cloud APM étaient la console Performance Management et le serveur Performance Management dans les éditions précédentes.

Les offres de l'abonnement IBM Performance Management on Cloud ont été consolidées et renommées :

Nom de l'offre - Edition d'octobre 2016 et antérieure	Nom de l'offre - Edition de mars 2017 et ultérieure
Monitoring on Cloud	Cloud APM, Base
Application Performance Management Advanced on Cloud	Cloud APM, Advanced

Certaines extensions de produit ont été consolidées et renommées :

Nom de l'extension - Edition d'octobre 2016 et antérieure	Nom de l'extension - Edition de mars 2017 et ultérieure
Base Extension Pack (agent Hadoop)	Base Extension Pack (ajout du nouvel agent Cassandra et du nouvel agent Microsoft Office 365)
Advanced Extension Pack (Agent SAP HANA Database et Agent SAP NetWeaver Java Stack)	Advanced Extension Pack (ajout du nouvel agent RabbitMQ)

Prise en charge de systèmes d'exploitation

Systèmes d'exploitation Windows 2016

Ajout de la prise en charge pour les systèmes d'exploitation Windows 2016. Pour plus d'informations, voir le Rapport de compatibilité des produits logiciels (SPCR) pour tous les agents : http://ibm.biz/agents-pm-systemreqs
Recherchez votre système d'exploitation dans la section Windows du rapport et cliquez sur l'icône du composant pour obtenir une liste des agents pris en charge.

Nouveau module d'extension disponible

IBM Cloud Application Performance Management z Systems Extension Pack

z Systems Extension Pack active la prise en charge de vos agents IBM OMEGAMON dans votre offre Cloud APM. Les données de l'agent OMEGAMON sont envoyées au serveur Cloud APM par la Passerelle hybride. La Passerelle hybride récupère les données de l'agent OMEGAMON et les événements depuis l'infrastructure IBM Tivoli Monitoring à laquelle les agents OMEGAMON sont connectés. Ainsi, vous pouvez visualiser les données de surveillance et les événements associés à vos agents OMEGAMON dans la console Cloud APM.

Cloud APM z Systems Extension Pack est disponible si vous disposez de l'une des offres Cloud APM.

Pour intégrer ce module d'extension à Cloud APM, procédez comme décrit dans «Intégration à OMEGAMON», à la page 991.

Nouveaux agents et collecteurs de données disponibles

Monitoring Agent for Cassandra

Vous pouvez utiliser l'agent Cassandra pour surveiller l'état de santé et les performances des ressources du cluster Cassandra, telles que les noeuds, les espaces de clés et les familles de colonne.

Monitoring Agent for Microsoft Office 365

Vous pouvez utiliser l'agent Microsoft Office 365 pour surveiller l'état de santé et les performances des ressources Office 365, telles que les services souscrits d'Office 365, le portail Office 365, les utilisateurs de boîte aux lettres, les sites SharePoint et le stockage OneDrive.

Monitoring Agent for NetApp Storage

Vous pouvez utiliser l'agent NetApp Storage pour surveiller la santé, la disponibilité et les performances des systèmes de stockage NetApp à l'aide de NetApp OnCommand Unified Manager (OCUM). L'agent de surveillance effectue les tâches suivantes :

- Identifie les objets du système de stockage dont les performances sont faibles
- Effectue une reconnaissance et une surveillance à l'aide du serveur OCUM au point focal

Monitoring Agent for RabbitMQ

Vous pouvez utiliser l'agent RabbitMQ pour surveiller l'état de santé et les performances des ressources du cluster RabbitMQ, telles que les noeuds, les files d'attente et les canaux du cluster.

Collecteurs de données pour applications Bluemix

Vous pouvez utiliser les collecteurs de données des applications Bluemix pour surveiller l'état de santé et les performances des types suivants de vos applications sur Bluemix :

- Applications Liberty
- Applications Node.js
- Applications Python
- Applications Ruby

Vous pouvez visualiser à la fois les données de surveillance des ressources et des diagnostics, telles que l'utilisation des ressources, le débit, et les informations détaillées au sujet des requêtes et des méthodes.

Monitoring Agent for Siebel

Vous pouvez utiliser l'agent Siebel pour surveiller l'état de santé et les performances des ressources Siebel, notamment les statistiques Siebel, les sessions utilisateur, les composants, les tâches, le serveur d'application, le serveur de noms de passerelle Siebel, l'utilisation de la mémoire et de l'UC de processus et la surveillance des événements du journal.

Améliorations au niveau des agents

Monitoring Agent for Amazon EC2

Les améliorations suivantes ont été ajoutées à l'agent Amazon EC2 :

- Remplacer l'ID instance par le nom de balise quand un nom de balise est disponible
- Autoriser le filtrage et le regroupement des données en fonction du nom de balise

Monitoring Agent for Db2

Les améliorations suivantes ont été ajoutées à l'agent Hadoop :

- Linux on Power Little Endian (pLinux LE) est pris en charge

- Un fichier script a été ajouté pour octroyer des privilèges à un utilisateur Db2 afin qu'il puisse visualiser des données pour l'ensemble des attributs de l'agent Db2 pour une instance surveillée

Monitoring Agent for Hadoop

Les améliorations suivantes ont été ajoutées à l'agent Hadoop :

- Support pour l'installation et la configuration de l'agent sur les systèmes Windows 2016 et AIX 7.2
- Support pour la surveillance des offres Hadoop suivantes : Hortonworks HDP 2.5, Cloudera CDH 5.6, 5.7 et 5.8, et IBM BigInsights 4.2
- Ajout du bouton de test de connexion qui permet de vérifier la connexion aux démons Hadoop que vous indiquez lorsque vous configurez l'agent
- Amélioration du processus de configuration d'agent pour réduire la durée et la complexité de configuration. La configuration a été simplifiée car les tâches de configuration et les prérequis suivants ne sont pas requis :
  - Installation du plug-in sur chaque noeud du cluster Hadoop
  - Configuration et mise à jour du fichier `hadoop-metrics2.properties`
  - Redémarrage des démons Hadoop après la configuration du fichier `hadoop-metrics2.properties`
  - Configuration de tous les DataNodes et NodeManagers dans le cluster
  - Redémarrage de l'agent lors de l'ajout de noeuds au cluster

Monitoring Agent for JBoss

Les améliorations suivantes ont été ajoutées à l'agent JBoss :

- Ajout du suivi des transactions et de la surveillance par analyse approfondie dans l'offre Advanced Agents
- Ajout d'une page de tableau de bord pour surveiller les mesures des sources de données
- Ajout de la prise en charge de la surveillance des offres JBoss suivantes : WildFly 8.x/9.x/10.x, JBoss EAP 7.x, JBoss AS 7.x
- Ajout de la prise en charge de l'exécution de l'agent sur le système d'exploitation Windows

Monitoring Agent for Linux KVM

Les améliorations suivantes ont été ajoutées au tableau de bord de l'agent Linux KVM :

- Mise à jour du widget de groupe Hôtes sur la page Hôtes, clusters et stockage pour afficher les indicateurs clés de performance Mémoire de planification max (Go) et Image instantanée opérationnelle
- Ajout de la page Détails de stockage pour afficher des détails au sujet des disques et des images instantanées de disque dans le pool de stockage
- Ajout du widget de groupe Données transmises/reçues sur le réseau (Go) dans la page Détail d'hôte pour afficher des informations historiques sur les données totales (en Go) transmises et reçues sur le réseau

Monitoring Agent for Linux OS

L'amélioration suivante a été ajoutée à l'Linux OS :

- Linux on Power Little Endian (pLinux LE) est pris en charge

Monitoring Agent for Microsoft Exchange Server

Les améliorations suivantes ont été ajoutées au tableau de bord de l'agent Microsoft Exchange Server :

- Ajout des attributs de temps entrant et sortant dans le jeu de données Accessibilité
- Ajout de pages et de widgets de groupe pour afficher les détails d'accessibilité
- Ajout d'un seuil de génération d'événement pour l'accessibilité

- Ajout d'une prise en charge pour l'installation et la configuration de l'agent sur Exchange Server 2016 et sur le système Windows Server 2016

Monitoring Agent for Microsoft Internet Information Services

L'amélioration suivante a été ajoutée à l'agent Microsoft IIS :

- Ajout d'une prise en charge pour l'installation et la configuration de l'agent sur le système Microsoft Windows Server 2016

Monitoring Agent for Microsoft Active Directory

Les améliorations suivantes ont été ajoutées à l'agent Microsoft Active Directory :

- Ajout de widgets de groupe et de pages pour afficher les détails des objets Group Policy Object, de Netlogon, de Local Security Authority et de LDAP
- Ajout des ensembles de données suivantes que vous pouvez afficher dans l'onglet **Détails d'attribut** :
  - Ensemble de données de services
  - Réplication
  - File Replication Service (FRS)
  - Unité d'org déplacée ou supprimée
  - Attributs LDAP
  - Gestionnaire de comptes de la sécurité
  - DFS
  - Carnet d'adresses
  - Journal des événements
  - Objets de configuration de mot de passe
- Ajout d'ensembles de données pour ADFS, pour le proxy ADFS et pour la file d'attente des unités d'exécution asynchrones
- Ajout de widgets de groupe et de pages pour afficher les détails des services ADFS et du proxy ADFS
- Ajout d'une prise en charge pour l'installation et la configuration de l'agent sur les systèmes Windows Server 2016

Monitoring Agent for Microsoft .NET

Les améliorations suivantes ont été ajoutées au tableau de bord de l'agent Microsoft .NET :

- Mise à jour du widget de groupe de statut MS .NET sur la page Composant pour afficher les temps de réponse des appels de la base de données, le statut des processus .NET dotés d'un nombre d'unités d'exécution élevé et les échecs de compilation Just in Time (JIT)
- Ajout de jeux de données, de pages et de widgets de groupe pour afficher les détails de compilation JIT, les détails d'appel de base de données, la collecte des indicateurs GC et des objets réservés pour un processus .NET sélectionné, le taux de conflits d'unité d'exécution et la longueur de la file d'attente d'unités d'exécution
- Ajout de seuils de génération d'événement pour les échecs JIT, les échecs de demande .NET, les commandes lentes, la récupération de place et les unités d'exécution actives dans les processus .NET

Monitoring Agent for Microsoft SQL Server

Les améliorations suivantes ont été ajoutées au tableau de bord de l'agent Microsoft SQL Server :

- Ajout du widget de groupe Expensive Queries dans la page Server Performance - Detail pour afficher les 10 premiers plans de requête mis en cache conformément aux statistiques de performance de Microsoft SQL Server
- Ajout d'un support pour la surveillance de Microsoft SQL Server 2016

- Ajout d'un support pour l'installation et la configuration de l'agent Microsoft SQL Server sur le système Microsoft Windows Server 2016
- Ajout de la nouvelle variable d'environnement *COLL_ERRORLOG_RECYCLE_WAIT* pour définir l'intervalle de temps (en secondes) pendant lequel l'agent attend de collecter les données du groupe d'attributs MS SQL Error Event Detail

Monitoring Agent for MongoDB

Les améliorations suivantes ont été ajoutées au tableau de bord de l'Agent MongoDB :

- Mise à jour de la page Composant pour afficher le nombre d'instances MongoDB et leur statut
- Ajout de pages pour afficher les détails des moteurs de stockage MMAPv1 et WiredTiger
- Ajout de la page Input Output Information pour afficher les détails de curseur et les données d'historique des opérations mises en file d'attente, des connexions actives, du flux de données et de l'accès aux données de l'hôte sélectionné
- Ajout de pages pour afficher les détails des verrous version 2.x et version 3.x ou ultérieure
- Ajout de la page Détails de la réplication pour afficher les détails du membre de réplication, d'oplog et des données d'historique du décalage de réplication et de l'espace utilisé par oplog

Monitoring Agent for Node.js

Les améliorations suivantes sont ajoutées à l'Agent Node.js pour optimiser les mesures d'application des noeuds (Appmetrics) :

- Ajout de nouveaux widgets de tableau de bord et de groupe pour afficher les détails de la récupération de place
- Ajout de nouveaux widgets de tableau de bord et de groupe pour afficher les détails des boucles d'événements

Monitoring Agent for PostgreSQL

Les améliorations suivantes ont été ajoutées à l'Agent PostgreSQL :

- Ajout d'une prise en charge pour l'installation et la configuration de l'agent sur les systèmes Windows
- Ajout d'une prise en charge pour la surveillance de PostgreSQL V9.6
- Mise à jour de la page Présentation des statuts de façon à ce que le statut ne soit pas critique lorsque le taux de réussite en mémoire tampon est égal à zéro

Monitoring Agent for SAP NetWeaver Java Stack

Les améliorations suivantes ont été ajoutées à l'Agent SAP NetWeaver Java Stack :

- Ajout d'ensembles de données, de widgets de groupe et de pages pour collecter et afficher les données de diagnostic et de suivi des transactions
- Ajout d'une prise en charge pour l'installation et la configuration de l'agent sur les systèmes Windows 2016

Monitoring Agent for Synthetic Playback

L'amélioration suivante a été ajoutée à l'Agent Synthetic Playback :

- L'Agent Synthetic Playback inclut une nouvelle fonction de filtrage pour les transactions synthétiques. Dans Synthetic Script Manager, configurez des listes noires et des listes blanches pour vos transactions synthétiques qui excluent ou incluent des requêtes vers les URL et les domaines spécifiés. Utilisez des listes noires et des listes blanches pour filtrer ou inclure les dépendances qui affectent les temps de réponse pour votre application, telles que les métriques de tiers

Monitoring Agent for Tomcat

L'amélioration suivante a été ajoutée à l'Agent Tomcat :

- Ajout d'une prise en charge pour l'installation et la configuration de l'Agent Tomcat sur les systèmes Windows et SUSE Linux Enterprise 12

Monitoring Agent for WebSphere Applications

Les améliorations suivantes ont été ajoutées à l'Agent WebSphere Applications :

- Linux on Power Little Endian (pLinux LE) est pris en charge. (Le suivi des transactions n'est pas pris en charge sur les systèmes pLinux LE.)
- Ajout d'une prise en charge pour IBM WebSphere Application Server Traditional V9.
- Le tableau de bord Analyse de mémoire a été ajouté pour vous aider à diagnostiquer les fuites de mémoire potentielles en vérifiant les informations d'utilisation des segments de mémoire présentées pour chaque cliché de tas. Le mode de diagnostic doit être activé pour que ce tableau de bord contienne des données.
- Ajout d'une prise en charge pour utiliser l'ensemble de données Application Health Status afin de créer des seuils d'événement pour la surveillance du statut de l'application. La collecte de données pour cette utilisation est désactivée par défaut. Vous devez modifier le fichier de propriétés du collecteur de données de façon à l'activer avant de créer des seuils d'événement.
- La configuration manuelle du collecteur de données a été simplifiée. Pour WebSphere Applications Server, vous devez seulement ajouter des arguments JVM et des variables pour le serveur d'applications sur la console d'administration WebSphere. Pour Liberty, vous devez uniquement modifier trois fichiers pour le serveur.

Agent de surveillance des temps de réponse

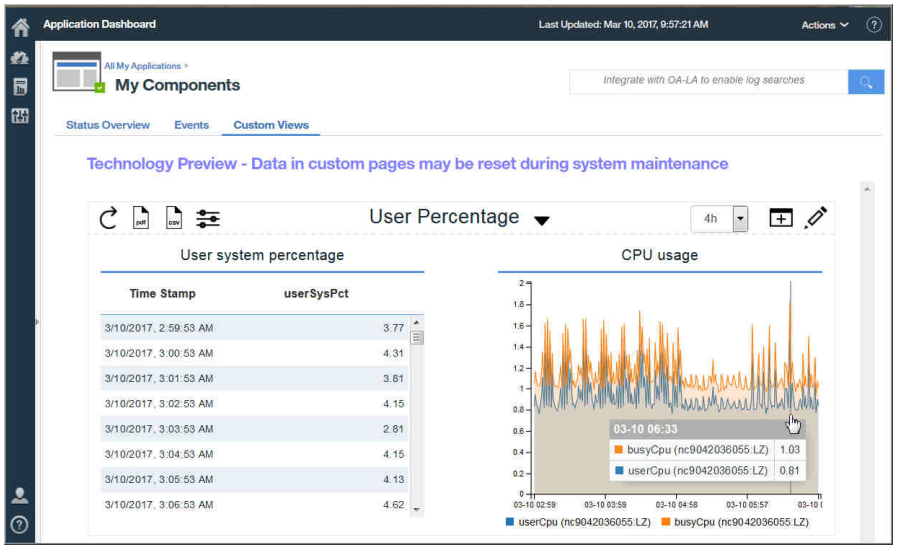
Les améliorations suivantes ont été ajoutées à l'Agent de surveillance des temps de réponse :

- Ajout d'une prise en charge de la configuration du suivi d'utilisateur pour les applications dans la page **Configuration d'agent**.
- Ajout d'une prise en charge de la configuration du suivi de session pour les applications dans la page **Configuration d'agent**.

Améliorations apportées à console Cloud APM

Plusieurs améliorations ont été apportées aux interfaces d'installation et de configuration d'agent, ainsi que les améliorations de console suivantes :

- Aperçu technique: Un nouvel onglet **Vues personnalisées** est disponible pour vos pages Tableau de bord des applications. Vous pouvez créer une variété de vues pour présenter des rapports sur les mesures obtenues à partir d'une ressource gérée et appliquer des fonctions telles que le calcul de moyenne et le comptage. Après avoir ouvert une page enregistrée, vous pouvez régénérer cette page avec des données issues d'une ressource différente, et télécharger les métriques sous forme de ficher PDF ou CSV. Pour plus d'informations, voir «Vues personnalisées», à la page 1144.

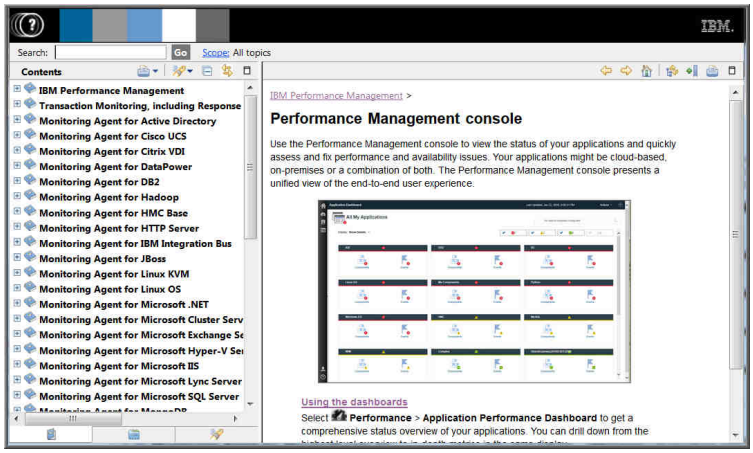


Si vous ne voyez pas **Vues personnalisées** dans votre abonnement Cloud APM et que vous souhaitez essayer cette nouvelle fonction, veuillez ouvrir une demande de service auprès du IBM Support afin d'activer l'aperçu technique des **Vues personnalisées**. Gardez à l'esprit que les pages

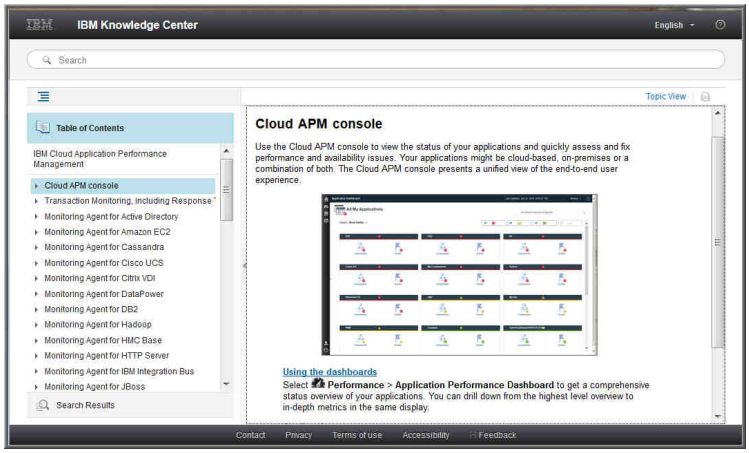
de votre tableau de bord personnalisé et les données d'historique qui les remplissent ne sont pas enregistrées au cours de la maintenance du système.

- Lorsque vous ouvrez le système d'aide de la console Cloud APM, notez qu'il est hébergé par l'IBM Knowledge Center. Vous disposez de l'outil **Masquer la table des matières**, de fonctionnalités de recherche et d'impression, et de liens vers des informations de support et des commentaires en retour.

Avant



Après



Amélioration d'Agent Builder

La prise en charge est améliorée pour la création de tableaux de bord récapitulatifs de Cloud APM pour les agents Agent Builder. Vous devez utiliser des ensembles de données à ligne unique pour fournir des données aux tableaux de bord récapitulatifs. Vous pouvez fournir de tels ensembles de données à partir de fichiers journaux entiers et à partir de tout ensemble de données pouvant être filtré en une ligne unique.

Nouveautés : septembre 2016

De nouvelles fonctions, options et offres sont disponibles depuis l'édition de septembre 2016 de Performance Management on Cloud.

Nouveaux agents disponibles

Monitoring Agent for Amazon EC2

Vous pouvez utiliser l'agent Amazon EC2 pour surveiller la santé, la disponibilité et les performances des ressources de votre instance Amazon Elastic Compute Cloud (EC2). Vous pouvez surveiller les ressources suivantes :

- Utilisation de l'UC
- Utilisation de l'EBS (Elastic Block Store)
- Utilisation du réseau

- Mises à jour de maintenance d'AWS (Amazon Web Services)
- Performances des disques

Cet agent se trouve dans Infrastructure Extension Pack et il est disponible dans les offres suivantes : IBM Monitoring, IBM Application Performance Management et IBM Application Performance Management Advanced.

Monitoring Agent for SAP NetWeaver Java Stack

Vous pouvez utiliser l'Agent SAP NetWeaver Java Stack pour surveiller la santé, la disponibilité et les performances de vos ressources SAP NetWeaver Java Stack Cluster et d'instance. Vous pouvez utiliser l'agent pour surveiller les ressources du cluster, comme les clichés de tas, l'instance de machine virtuelle Java, les temps de réponse des sessions utilisateur, les détails de transaction, les informations système et les détails de licence. Vous pouvez utiliser l'agent pour surveiller les ressources d'instance, comme l'utilisation de l'UC, l'utilisation de disque, l'utilisation de mémoire, la collecte de bases de données, la récupération de place, les clichés de tas, les applications ayant échoué, le conteneur Web et les informations de session. Cet agent se trouve dans Advanced Extension Pack et est disponible si vous avez l'une des offres suivantes : IBM Application Performance Management et IBM Application Performance Management Advanced.

Améliorations au niveau des agents

Monitoring Agent for Citrix Virtual Desktop Infrastructure

Ajout de la capacité à récupérer les événements du journal des événements Windows pour les machines Virtual Delivery Agent (VDA) et Desktop Delivery Controller (DDC).

Monitoring Agent for Linux KVM

Les tableaux de bord sont disponibles pour que l'agent puisse surveiller le déploiement des machines virtuelles basées sur le noyau Linux. Ils offrent les fonctionnalités de surveillance suivantes :

- Le tableau de bord récapitulatif affiche le statut global des hôtes en fonction de l'utilisation de l'UC et de mémoire de votre application ou environnement de machines virtuelles basées sur le noyau Linux.
- Le tableau de bord des détails d'hôte affiche les détails relatifs à l'hôte sélectionné.
- Le tableau de bord des hôtes, des clusters et du stockage affiche les détails relatifs aux machines virtuelles surveillées.
- Le tableau de bord des détails de la machine virtuelle affiche les détails relatifs à la machine virtuelle sélectionnée sur la page des détails d'hôte.

Monitoring Agent for Linux OS

Docker version 1.8.0 ou ultérieure est pris en charge. De nouveaux groupes d'attributs et widgets ont été ajoutés afin de permettre à l'agent de système d'exploitation Linux de fournir des fonctionnalités de surveillance Docker.

Monitoring Agent for Oracle Database

Le tableau de bord de l'agent Oracle Database inclut les nouvelles fonctions suivantes sur la page Détails de l'instance :

- Un tableau contenant des informations sur la contention de verrouillage de l'instance sélectionnée.
- Un tableau contenant des informations sur les services GCS et GES d'Oracle Real Application Clusters.
- Un tableau contenant des informations détaillées sur les groupes de disques de gestion de stockage automatique joints à l'instance sélectionnée.
- Une vue présentant des informations détaillées par espace table, qui s'affiche lorsque vous cliquez sur **Bottom 5 Free**.
- Un tableau contenant des détails historiques sur les processus d'avant-plan et d'arrière-plan joints à l'instance sélectionnée. Vous pouvez cliquer sur l'entité dans le tableau et afficher un tableau détaillé de tous les processus associés à cette instance.

- Un tableau contenant les 5 pires requêtes SQL (par temps d'exécution) associées à l'instance sélectionnée. Vous pouvez cliquer dans le tableau et afficher un tableau détaillé des 50 pires requêtes SQL suivantes associées à cette instance.

Monitoring Agent for Synthetic Playback

L'Agent Synthetic Playback inclut une nouvelle fonction de sécurité. Vous pouvez empêcher l'affichage dans Synthetic Script Manager des mots de passe stockés dans des scripts synthétiques.

Monitoring Agent for VMware VI

Outre la fonction de découplage de l'agent, vous pouvez afficher et sélectionner le noeud agent et ses sous-noeuds dans la même vue.

Lorsque vous sélectionnez le composant d'infrastructure virtuelle VMware dans la fenêtre Sélectionner le composant, l'éditeur de composant affiche une structure arborescente du noeud agent avec l'ensemble de ses sous-noeuds.

- Si vous développez l'arborescence et que vous sélectionnez le noeud agent, tous les sous-noeuds sont automatiquement sélectionnés. Vous pouvez également développer l'arborescence et sélectionner individuellement les sous-noeuds que vous voulez surveiller.
- Si vous sélectionnez le noeud agent alors que l'arborescence est réduite, tous les sous-noeuds sont automatiquement exclus.

Lorsque vous sélectionnez le composant Serveur ESX dans la fenêtre Sélectionner le composant, les serveurs ESX autonomes s'affichent dans l'éditeur de composant en plus des sous-noeuds. Outre les sous-noeuds, vous pouvez sélectionner des serveurs ESX autonomes pour la surveillance.

Lorsque l'application est créée, le tableau de bord Interface graphique APM affiche une structure arborescente de l'instance d'agent en tant que parent et ses noeuds en tant qu'enfants.

Agent de surveillance des temps de réponse

Vous pouvez personnaliser les localisations appliquées aux adresses IP ou aux plages d'adresses IP spécifiques dans les tableaux de bord Transaction utilisateur final pour votre environnement spécifique. Utilisez l'onglet **Geolocation** sous **Configuration d'agent** pour personnaliser les valeurs de localisation.

Améliorations apportées à console Cloud APM

- Plusieurs améliorations ont été apportées aux interfaces d'installation et de configuration d'agent.
- Une option de **journal de tableau de bord** a été ajoutée au menu **Actions** pour contrôler la liste des tableaux de bord d'agent mis à jour depuis le dernier redémarrage du serveur. Pour plus d'informations, voir «Toutes mes applications - Tableau de bord d'Application Performance», à la page 1109.
- La page du Tableau de bord d'Application Performance pour l'application sélectionnée a été rationalisée afin d'améliorer l'affichage. Un comptage des événements de gravité de niveau Avertissement et Critique apparaît sur le titre de l'onglet Evénements et remplace le graphique à barres **Récapitulatif de la gravité de l'événement**. Dans le cas des applications pour lesquelles des vues de topologie sont activées, la vue **Agréger la topologie d'application** comporte un bouton bascule permettant de passer au graphique Statut de composant en cours. Pour plus d'informations, voir «présentation des statuts», à la page 1112.
- Dans les précédentes éditions, l'onglet **Détails d'attribut** du Tableau de bord d'Application Performance n'était disponible que pour les instances de composant. L'onglet **Détails d'attribut** est disponible pour la création de tables historiques des instances de transaction de l'Agent de surveillance des temps de réponse et de l'Agent Synthetic Playback. Pour les utilisateurs malvoyants, la possibilité de créer des tables historiques fournit une alternative aux graphiques à courbes que les technologies d'assistance aux personnes handicapées, telles les logiciels de lecteur d'écran, ne peuvent pas interpréter. Pour plus d'informations, voir «Affichage et gestion de graphiques et tableaux personnalisés», à la page 1123.

API

Vous pouvez utiliser les API pour créer des scripts afin d'automatiser l'intégration de votre environnement Performance Management. Pour plus d'informations, voir «Exploration des API», à la page 1103.

Nouveautés : avril 2016

De nouvelles fonctions, options et offres sont disponibles depuis l'édition d'avril 2016 de Performance Management on Cloud.

IBM Marketplace

Les offres IBM Performance Management on Cloud sont disponibles à partir d'IBM Marketplace. Inscrivez-vous pour un essai gratuit ou un compte d'abonnement. Pour plus d'informations, voir «Téléchargement de vos agents et de vos collecteurs de données», à la page 105.

Nouveaux agents disponibles

Monitoring Agent for Citrix Virtual Desktop Infrastructure

Vous pouvez utiliser l'agent Citrix VDI pour surveiller la santé, la disponibilité et les performances des ressources Citrix XenDesktop ou XenApp, comme des sites, des machines, des applications, des bureaux, des sessions et des utilisateurs. Cet agent se trouve dans Infrastructure Extension Pack et il est disponible pour les offres suivantes : IBM Monitoring, IBM Application Performance Management et IBM Application Performance Management Advanced.

Monitoring Agent for Skype for Business Server

Vous pouvez utiliser l'Agent Skype for Business Server pour surveiller la santé, la disponibilité et les performances des ressources Microsoft Lync Server, comme la base de données, le serveur de médiation, les transactions synthétiques, la messagerie instantanée, les opérations d'écriture du service CDR et les homologues SIP.

Monitoring Agent for WebLogic

Vous pouvez utiliser l'Agent WebLogic pour surveiller la santé, la disponibilité et les performances des ressources de serveur WebLogic, comme les machines virtuelles Java, JMS (Java Messaging Service) et JDBC (Java Database Connectivity).

Améliorations de l'intégration

Coexistence des agents

La coexistence des agents est prise en charge. Vous pouvez installer les agents IBM Performance Management sur le même ordinateur que les agents IBM Tivoli Monitoring. Les deux agents ne peuvent toutefois pas être installés dans le même répertoire. Voir «Coexistence de l'agent Cloud APM et de l'agent Tivoli Monitoring», à la page 976 .

IBM Alert Notification

La notification d'alertes inclut une application mobile qui fournit un sous-ensemble de fonctions de notification d'alertes sur des périphériques iOS et Android.

Surveillance de la Pile d'intégration IBM

Vous pouvez surveiller la Pile d'intégration IBM afin de visualiser les informations de suivi des transactions pour les produits middleware des dispositifs IBM MQ, IBM Integration Bus et DataPower et les services qu'ils exposent, et résoudre les incidents lorsqu'un problème survient. Voir «Scénario : Surveillance de la Pile d'intégration IBM», à la page 99 .

Améliorations au niveau des agents

Monitoring Agent for Db2

Des commandes ont été ajoutées pour l'octroi de privilèges à l'utilisateur par défaut (pour les systèmes Windows) et à l'utilisateur propriétaire de l'instance (pour les systèmes Linux et AIX) pour la visualisation des données pour certains des attributs de l'agent Db2.

Monitoring Agent for Hadoop

L'agent Hadoop est pris en charge sur les systèmes d'exploitation Linux, Windows et AIX.

Monitoring Agent for HMC Base
Des fonctionnalités de surveillance sont prévues pour les E-S virtuelles et pour les événements matériels.

Monitoring Agent for IBM Integration Bus

Le chemin d'accès à la bibliothèque de la dernière version d'IBM MQ (WebSphere MQ) peut être automatiquement reconnu lors de la configuration d'agent sur les systèmes Linux et AIX.

Monitoring Agent for Microsoft Cluster Server
L'agent Microsoft Cluster Server est automatiquement configuré après son installation.

Monitoring Agent for Microsoft Exchange Server
Un certain nombre de services ont été ajoutés dans l'onglet **Services Exchange** de la fenêtre de configuration d'agent pour déterminer le statut du serveur Exchange.

Monitoring Agent for Microsoft Hyper-V Server
Le panneau de configuration d'agent a été supprimé. La configuration de l'agent n'est pas nécessaire.

Monitoring Agent for SAP HANA Database
Le widget de groupe Cache Information Details du tableau de bord **SAP HANA Database Details** a été ajouté pour fournir des informations sur le pourcentage de mémoire utilisée, le pourcentage de mémoire disponible et le taux d'accès en mémoire cache de la base de données surveillée.

Monitoring Agent for Synthetic Playback
Agent Synthetic Playback inclut les fonctions suivantes :

- Vous pouvez installer et configurer l'Agent Synthetic Playback pour surveiller les performances et la disponibilité des applications privées internes dans le tableau de bord d'Application Performance, en plus des applications publiques externes.
- Utilisez Synthetic Script Manager pour générer un script simple afin de tester la disponibilité et les performances de vos applications.
- Configurez la réexécution simultanée ou échelonnée des transactions synthétiques dans différents emplacements.
- Surveillez l'utilisation de la réexécution mensuelle dans Synthetic Script Manager.
- Affichez des métriques HTTP et de rapports de disponibilité dans les rapports de l'Agent Synthetic Playback.
- Deux nouveaux rapports sont disponibles : Tendance des transactions et Tendance des sous-transactions.
- Organisez vos transactions synthétiques dans un groupe de ressources et appliquez des seuils à toutes les transactions de ce groupe de ressources.
- Affichez les données de transaction de synthèse dans la fenêtre **My Transactions** dans le tableau de bord d'Application Performance, sans avoir besoin de créer une application qui contient des transactions synthétiques associées.
- Téléchargez des scripts synthétiques de Synthetic Script Manager.

Monitoring Agent for VMware VI
Le tableau de bord de l'Agent VMware VI a été amélioré pour inclure les nouvelles fonctions suivantes :

- Le nombre d'alarmes déclenchées à l'état Critique ou Avertissement est également affiché dans la page **Composant**.
- Un nouveau tableau de la page **Récapitulatif de cluster** fournit des informations sur les alarmes proactives et les alarmes liées à des défaillances. Vous pouvez cliquer sur l'entité déclenchée dans le tableau et afficher la page de détails associée.
- Un nouveau tableau de la page **Détails du cluster** affiche les détails des serveurs ESX qui font partie du cluster sélectionné. Vous pouvez cliquer sur le serveur ESX et afficher la page de détails de ce serveur ESX.

- Le tableau Magasin de données de la page **Détails du cluster** inclut une mesure de la surcharge du magasin de données.
- Le tableau Machines virtuelles de la page VM Detail inclut des mesures de performances, notamment pour la taille de la mémoire, les cartes NIC et les disques. Vous pouvez cliquer sur ces mesures et afficher les pages de détails associées.
- Des widgets et des pages ont été ajoutés pour afficher des mesures de performances importantes de la mémoire, des disques et du réseau pour la machine virtuelle sélectionnée.
- Un nouveau tableau de la page **Détails du serveur ESX** affiche les performances du réseau de serveurs.
- Le tableau Magasin de données de la page **VM Detail** et **ESX Server Detail** affiche la mesure du temps d'attente du magasin de données.
- Un nouveau tableau de la page **Détail du magasin de données** affiche des informations sur la machine virtuelle associée au magasin de données. Vous pouvez cliquer sur la machine virtuelle et afficher la page **Détails de la machine virtuelle**.
- Le titre du diagramme % mémoire (historique) de la page **Détails de la machine virtuelle** a été remplacé par Mémoire invité (historique).

Monitoring Agent for WebSphere Applications

Le tableau de bord récapitulatif des demandes en cours fournit la capacité d'identifier les instances de demande qui sont actuellement lentes ou suspendues. Vous pouvez effectuer une opération d'annulation douce sur une demande en cours en sélectionnant la demande, puis en cliquant sur **Cancel Thread** dans le widget des demandes en cours de ce tableau de bord.

Tous les seuils de génération d'événements prédéfinis ont été affinés afin de fournir une meilleure expérience utilisateur. Les améliorations et mises à jour comprennent la condition qui déclenche une alerte, l'intervalle d'échantillonnage et la gravité du seuil.

L'interface utilisateur de Monitoring Agent for WebSphere Applications est accessible aux utilisateurs ayant un handicap physique.

Le processus de configuration a été affiné en fonction des commentaires des clients et des révisions techniques afin d'offrir une meilleure expérience utilisateur.

Monitoring Agent for WebSphere MQ

Un certain nombre de modifications ont été apportées aux seuils de génération d'événement prédéfinis :

- Tous les seuils prédéfinis possèdent le préfixe MQ_ au lieu du préfixe MQSeries_ dans les versions précédentes.
- Deux seuils, MQ_Channel_Initiator_Crit et MQ_Queue_Manager_Crit, ont été ajoutés pour déclencher des alertes critiques pour le statut du serveur initiateur de canal et le statut du gestionnaire de files d'attente.
- La condition de déclenchement de l'événement MQ_Queue_Depth_High passe de 80 % statique à la valeur de profondeur élevée de la file d'attente.

Le nom du widget **Files d'attente non lues - 5 premières** a été remplacé par le nom **Files d'attente utilisées non lues - 5 premières**. Ce widget fournit la liste des cinq premières files d'attente qui incluent des messages et qui sont connectées par une ou plusieurs applications pour placer des messages dans la file d'attente mais qui ne sont lues par aucune application.

Le chemin d'accès à la bibliothèque de la dernière version d'IBM MQ (WebSphere MQ) peut être automatiquement reconnu lors de la configuration d'agent. Vous pouvez laisser le paramètre **WMQLIBPATH** vide dans le fichier de réponses silencieux ou accepter la valeur par défaut lorsque vous configurez l'agent en mode interactif.

Agents de système d'exploitation

Les agents de système d'exploitation incluent une nouvelle fonction pour surveiller les fichiers journaux d'application. La fonctionnalité permet de configurer la surveillance des fichiers journaux basée sur des expressions régulières.

Pour des raisons de compatibilité, l'agent de système d'exploitation utilise les informations et les formats suivants :

- Les informations de configuration et le fichier de format utilisé par IBM Tivoli Monitoring 6.x Log File Agent
- Les informations de configuration et les chaînes de format utilisées par Tivoli Event Console Log File Adapter

Ces chaînes de format permettent à l'agent de filtrer les données de journal en fonction de masques dans le fichier de format et de soumettre uniquement les données appropriées à un consommateur d'événement. L'agent de système d'exploitation envoie des données au serveur Performance Management ou via EIF (Event Integration Facility) à un récepteur EIF, comme la sonde OMNIbus EIF.

Agent de surveillance des temps de réponse

Les tableaux de bord Transactions utilisateur final comprennent les informations d'utilisateur et de périphérique, qui étaient auparavant affichées dans les tableaux de bord Utilisateurs authentifiés et Utilisateurs de périphérique mobile dans le groupe Utilisateurs. Les informations relatives aux utilisateurs, aux sessions et aux périphériques sont triées par zone géographique (pays, état et ville) en fonction de l'adresse IP de l'utilisateur. Utilisez les tableaux de bord nouveaux et mis à jour pour comprendre les volumes d'utilisateurs et déterminer si des problèmes se limitent à des groupes d'utilisateurs spécifiques.

Personnalisez les localisations qui sont appliquées aux adresses IP ou aux plages d'adresses IP spécifiques dans les tableaux de bord Transaction utilisateur final pour votre environnement. Utilisez l'onglet **Geolocation** sous **Configuration d'agent** pour personnaliser les valeurs de localisation.

Suivi des transactions

La page Récapitulatif de transaction inclut une topologie Service Dependencies qui affiche le noeud de ressources sélectionné, comme IBM Integration Bus, et les services dont il dépend. La page Détails de transaction inclut une topologie Transaction Dependencies qui affiche un noeud de transaction pour chaque instance de composant et un noeud sans instrumentation pour chaque service dépendant au niveau d'une transaction ; par exemple, IBM Integration Bus et ses transactions de services. La page Détails de transaction présente également les utilisateurs de l'application sélectionnée qui enregistrent les temps de réponse les plus lents et les hôtes qui reçoivent le volume de transactions le plus élevé.

Améliorations générales apportées aux agents

Les améliorations suivantes ont été apportées à l'installation ou à la configuration des agents :

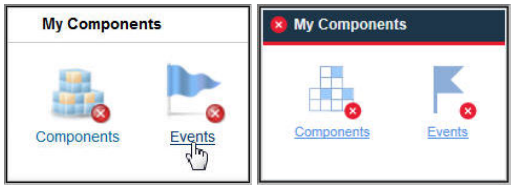
- Le script d'installation des agents effectue un contrôle des droits d'accès avant le démarrage de l'installation. Si vous n'avez pas les droits d'accès appropriés, un message s'affiche.
- La commande de statut des agents vérifie le statut entre l'agent et la console Performance Management.
- Les agents pris en charge sur les systèmes Windows incluent un utilitaire en mode graphique qui permet d'effectuer la configuration d'agent et de vérifier le statut de connexion.
- Vous pouvez utiliser une nouvelle commande pour supprimer une instance d'agent sans désinstaller l'agent.

Améliorations du serveur Performance Management

L'authentification utilisateur de Performance Management est gérée via un fournisseur IBMid OpenID Connect.

Améliorations de la console Performance Management

- L'aspect de la console Performance Management a été mis à jour pour ressembler à l'interface utilisateur d'IBM Bluemix. Par exemple, vous pouvez noter les différences entre une zone récapitulative du tableau de bord **Toutes mes applications** dans la version 8.1.2 et celle affichée dans la version actuelle :



- Une nouvelle option a été ajoutée à la page Configuration avancée afin que les utilisateurs avancés puissent facilement activer ou désactiver tous les seuils prédéfinis sur tous les groupes système. Voir «Informations de référence», à la page 1004 .
- Une nouvelle option a été ajoutée à la page de configuration avancée pour contrôler le taux de rafraîchissement automatique du Tableau de bord d'Application Performance. Pour plus d'informations, voir «Intégration de l'interface utilisateur», à la page 1104.
- Plusieurs améliorations ont été apportées aux interfaces d'installation et de configuration d'agent.
- Améliorations apportées à l'accessibilité de la console Performance Management. Pour plus d'informations sur les fonctions d'accessibilité de l'interface utilisateur, voir «Fonctions d'accessibilité», à la page 1553.

API

Vous pouvez utiliser les API pour créer des scripts afin d'automatiser l'intégration de votre environnement Performance Management. Pour plus d'informations, voir «Exploration des API», à la page 1103.

Amélioration d'Agent Builder

Agent Builder inclut le filtrage amélioré d'ensembles de données. Vous pouvez utiliser le filtrage pour créer des ensembles de données qui renvoient une seule ligne en fonction d'ensembles de données multilignes, y compris l'ensemble des données de disponibilité. Utilisez cette fonction pour fournir des informations dans les tableaux de bord de synthèse.

Chapitre 2. Documentation au format PDF

Les informations disponibles pour les rubriques contenues dans cet IBM Knowledge Center et pour les documents de référence d'agent sont disponibles au format PDF.

IBM Knowledge Center au format PDF

Outre ce Guide d'utilisation, vous pouvez télécharger le document IBM Agent Builder - Guide d'utilisation.

Documents de référence d'agent au format PDF

Pour télécharger le document de référence d'un agent, voir Agent metrics/Reference PDFs sur Application Performance Management Developer Center. Les références fournissent des informations sur les tableaux de bord, les seuils de génération d'événement et les ensembles de données. Les ensembles de données contiennent des attributs, qui sont les métriques signalées par l'agent et qui constituent les indicateurs clés de performance (KPI). La version de l'agent apparaît sur la page de titre du fichier PDF.

Chapitre 3. Présentation du produit

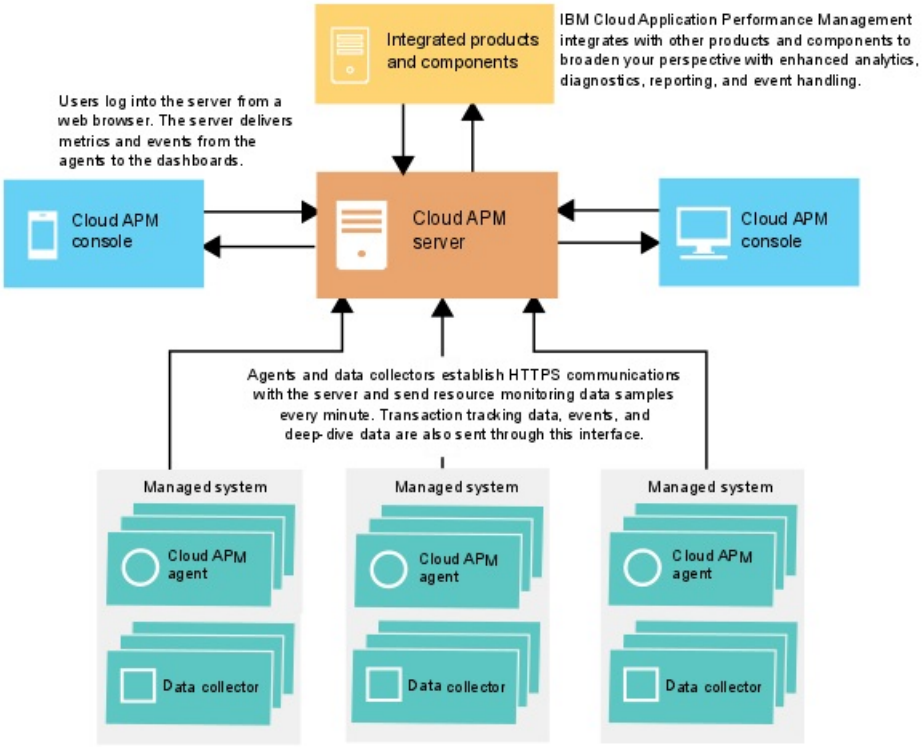
IBM Cloud Application Performance Management (Cloud APM) est une solution complète qui vous aide à gérer les performances et la disponibilité des applications déployées sur site(privées), dans un cloud public ou comme combinaison hybride. Cette solution fournit une visibilité sur les applications, et permet de les contrôler et de les automatiser, garantissant ainsi des performances et une utilisation des ressources optimales.

Cette solution permet de gérer le centre de données, l'infrastructure de cloud et les charges avec une intelligence cognitive. Vous pouvez réduire et empêcher les indisponibilités et les ralentissements dans un environnement d'applications hybrides car Cloud APM vous aide à passer de l'identification des problèmes de performances à l'isolement de l'endroit où le problème se produit et au diagnostic des problèmes avant qu'ils n'affectent votre activité.

Utilisez les fonctionnalités principales, qui varient selon l'offre, pour utiliser les données recueillies par les agents et les collecteurs de données Cloud APM. Plus de fonctionnalités sont disponibles grâce à l'intégration aux autres produits et composants.

Présentation de l'architecture

IBM Cloud Application Performance Management utilise des *agents* et les *collecteurs de données* pour collecter des données sur des hôtes surveillés. Les agents et les collecteurs de données transmettent les données au serveur Cloud APM, qui les assemble dans la console Cloud APM. Le serveur Cloud APM est hébergé dans le cloud IBM.



Collecte de données

Les agents et les collecteurs de données surveillent des systèmes, des sous-systèmes ou des applications et collectent des données. Un agent ou un collecteur de données interagit avec une seule ressource (par exemple, un système ou une application) et, dans la plupart des cas, se trouve sur l'ordinateur ou la machine virtuelle où s'exécute le système ou l'application. Par exemple, l'Linux OS

collecte des indicateurs de performance pour le système d'exploitation sur l'hôte Linux et l'Agent WebSphere Applications surveille les indicateurs de performance des serveurs d'applications WebSphere. Il existe également des agents qui suivent les transactions entre les différentes ressources.

Vous pouvez configurer des seuils pour les indicateurs clés de performance. Lorsqu'un indicateur passe au-dessus ou en-dessous du seuil, l'agent ou le collecteur de données génère une alerte que le serveur traite. Vous pouvez également configurer le transfert des événements vers une cible telle que la Netcool/OMNIbus Probe for Tivoli EIF ou un serveur SMTP et utiliser la fonction Alert Notification pour configurer les notifications par courrier électronique pour les événements.

Les agents et les collecteurs de données sont préconfigurés pour communiquer avec le serveur Cloud APM.

Communication entre le serveur et les agents ou les collecteurs de données

Les agents et les collecteurs de données de chaque hôte surveillé établissent des communications HTTPS avec le serveur Cloud APM qui se trouve dans le cloud IBM. L'agent ou le collecteur de données constitue le côté client de la connexion.

Les agents et les collecteurs de données ont besoin d'une connexion Internet pour envoyer les données au serveur. S'ils ne peuvent pas les envoyer directement sur Internet, l'utilisation d'un proxy direct peut s'avérer nécessaire. Pour plus d'informations, voir «Connectivité réseau», à la page 163.

Données stockées par le serveur

Les agents et les collecteurs de données envoient les données au serveur Cloud APM à des intervalles compris entre 1 minute et 8 minutes, en fonction de type des données. Le serveur stocke toutes les valeurs envoyées par les agents et les collecteurs de données pendant 8 jours par défaut. Des données de transaction résumées sont stockées pendant de plus longues périodes.

Les données de surveillance sauvegardées sont appelées *données d'historique*. Le serveur se sert des données d'historique pour afficher des tableaux et des graphiques qui vous permettent d'analyser les tendances de votre environnement.

Des rapports d'historique sont également disponibles pour certains agents. Pour plus d'informations, voir «Rapports», à la page 1156.

Evolutivité

Vous pouvez surveiller jusqu'à 10 000 systèmes gérés à partir de Cloud APM. Un système géré est un système d'exploitation, un sous-système ou une application unique de votre entreprise surveillé par un agent.

Cloud APM prend en charge entre 150 et 400 transactions utilisateur surveillées par seconde.

Intégration

IBM Cloud Application Performance Management est intégré avec d'autres produits et composants si ceux-ci sont configurés pour la communication avec le serveur Cloud APM.

Les produits qui peuvent être intégrés incluent IBM Control Desk, Netcool/OMNIbus, Tivoli Monitoring, OMEGAMON, Operations Analytics - Log Analysis, Operations Analytics - Predictive Insights, IBM Alert Notification et IBM Cloud.

Agent Builder est un composant qui peut être utilisé pour créer des agents personnalisés.

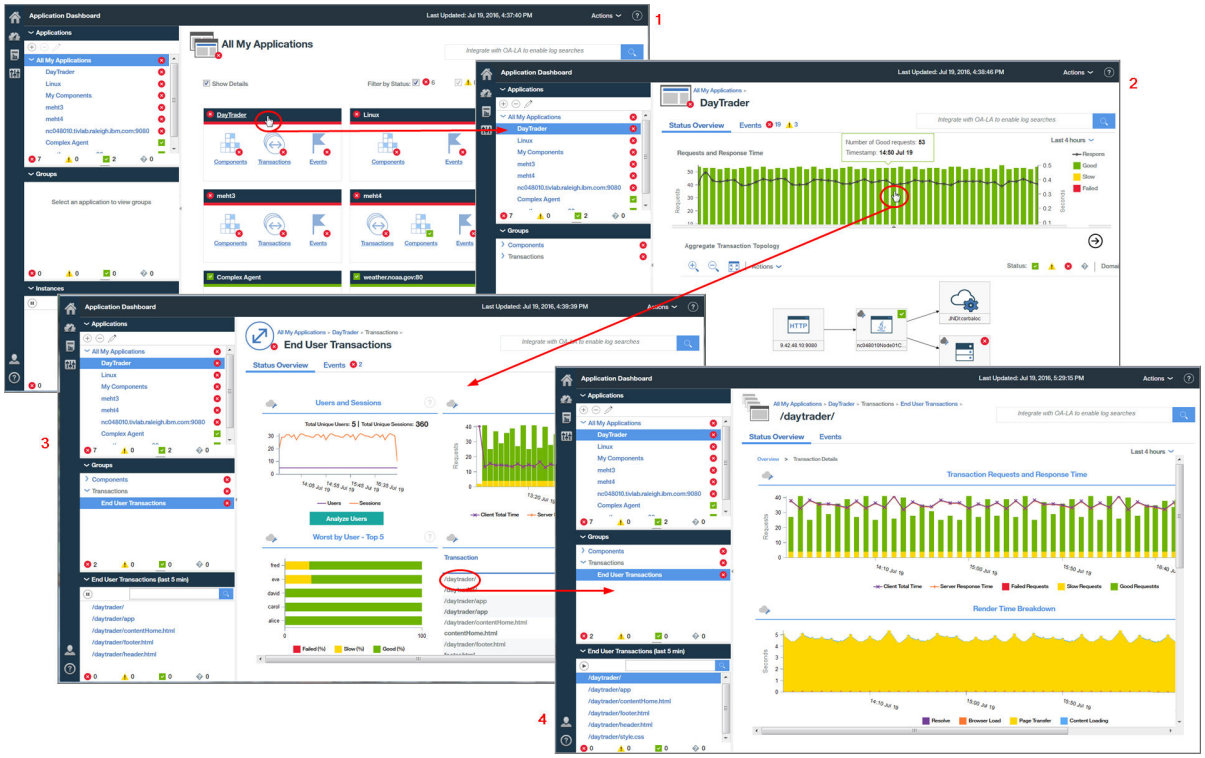
Interface utilisateur

La console Cloud APM est l'interface utilisateur de Cloud APM. Cette interface utilisateur unifiée fournit une vue unique au sein d'applications hybrides. Vous pouvez utiliser la console pour afficher le statut des applications et évaluer et résoudre rapidement les problèmes de performances et de disponibilité.

Les tableaux de bord de la console facilitent l'identification des problèmes pour vous permettre d'isoler les goulots d'étranglement qui affectent les performances des applications. A l'aide d'une simple navigation dans les tableaux de bord, vous pouvez passer d'une vue présentant le statut de l'application à des informations détaillées au niveau du code. Vous pouvez visualiser les problèmes du code source au moment exact de leur apparition. Vous pouvez rechercher et diagnostiquer des problèmes à l'aide des données d'analyse de recherche intégrées.

Le navigateur du Tableau de bord d'Application Performance dans la console est hiérarchique, ce qui vous permet d'avoir une vue globale du statut de vos applications, de la santé de leurs composants et de la qualité de l'expérience de leurs utilisateurs. Pour plus de détails sur la ressource surveillée, vous pouvez cliquer sur un élément de navigateur ou sur un lien dans les vues du tableau de bord. Imaginez, par exemple, que votre application présente un temps de réponse long. Le problème est signalé dans le tableau de bord. A partir du tableau de bord, vous pouvez remonter jusqu'à la source du problème en cliquant sur des liens pour en identifier la cause (par exemple, une utilisation élevée de l'unité centrale sur le système en raison d'un processus hors de contrôle).

Pour plus d'informations sur l'utilisation des tableaux de bord dans la console Cloud APM, voir Chapitre 10, «Utilisation des tableaux de bord», à la page 1109.



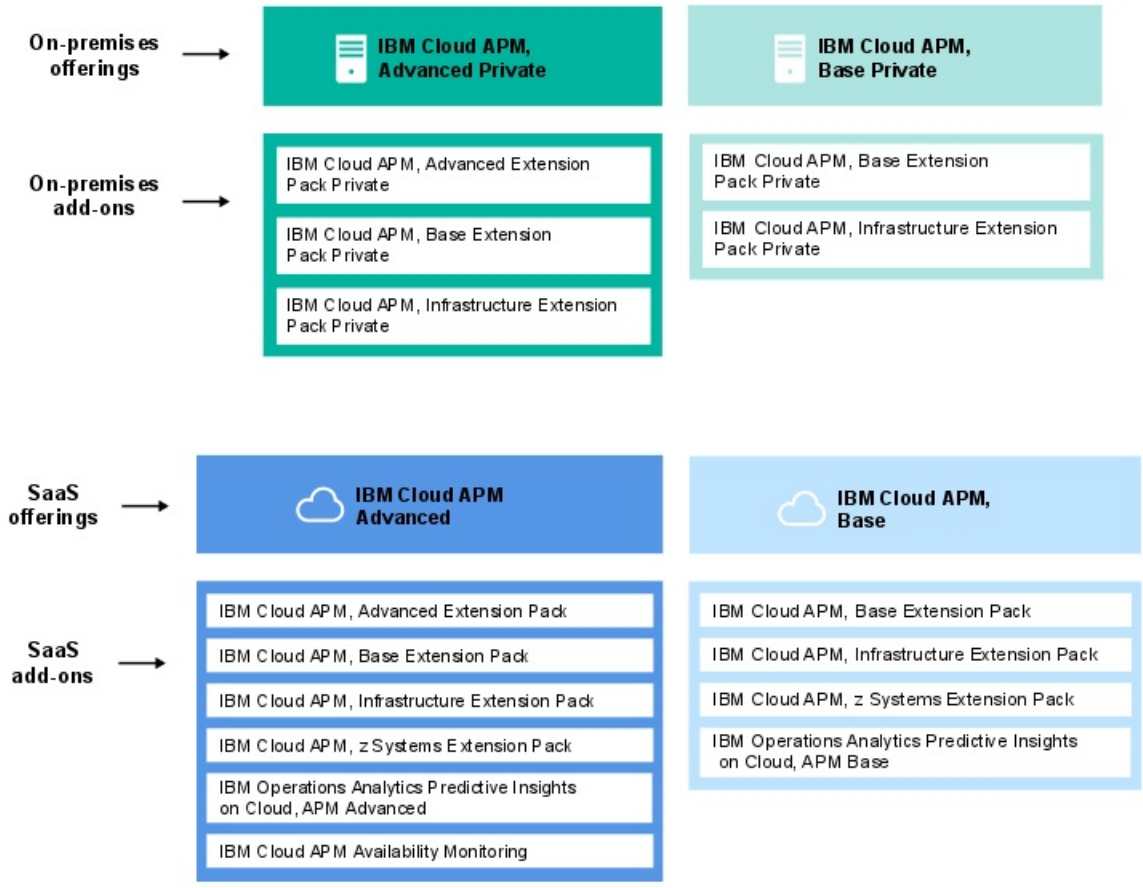
Offres et modules complémentaires

IBM Cloud Application Performance Management contient deux offres et plusieurs modules complémentaires. Les offres et modules complémentaires contiennent des agents et des collecteurs de données. Des modules complémentaires spécifiques peuvent être utilisés avec chaque offre.

Pour savoir quels agents sont inclus dans une offre ou un module complémentaire et découvrir les fonctionnalités d'agent et de collecteur de données, voir «Fonctions», à la page 55.

Pour chaque offre, des modules complémentaires sont disponibles dans IBM Marketplace. IBM Cloud Application Performance Management, Advanced est l'offre la plus complète, elle inclut tous les agents, tous les collecteurs de données et toutes les pages de tableau de bord. IBM Cloud Application Performance Management, Base est un sous-ensemble d'Cloud APM, Advanced. Vous pouvez remplacer Cloud APM, Base par Cloud APM, Advanced à tout moment. L'offre finale installée après ce remplacement est Cloud APM, Advanced. Le diagramme indique quels modules complémentaires sont disponibles pour chaque offre.

Les modules complémentaires sont les mêmes pour toutes les offres, sauf pour Availability Monitoring qui est un module complémentaire pour l'offre Cloud APM, Advanced.



Offres

IBM Cloud Application Performance Management, Advanced

Cette offre est conçue pour l'expérience utilisateur final, le suivi des transactions et la surveillance des ressources de tous vos composants d'application. Elle fournit une visibilité du niveau de code dans vos applications et la santé de vos serveurs d'applications. Utilisez les tableaux de bord de diagnostic pour rechercher les goulots d'étranglement des performances dans le code d'application et pour gérer vos applications vitales en production.

L'offre contient IBM Cloud Application Performance Management, Base ainsi que des agents et des collecteurs de données permettant de surveiller des applications, des transactions et d'autres ressources installées dans votre entreprise. Pour une liste des agents et collecteurs de données de cette offre, voir «Fonctions», à la page 55.

Cette offre permet à DevOps de disposer d'une solution complète capable d'offrir la pleine visibilité et le plein contrôle de vos applications et de votre infrastructure. Les propriétaires du secteur d'activité peuvent gérer les applications critiques et l'expérience utilisateur final en production. Les développeurs d'applications peuvent afficher les détails des transactions et diagnostiquer les problèmes des applications.

IBM Cloud Application Performance Management, Base

Cette offre est conçue pour la surveillance de ressources de charges de travail d'infrastructure, de composants d'application et du cloud. La surveillance des ressources vous aide à identifier et traiter les problèmes de transactions lentes, de capacité et d'indisponibilité. L'offre contient des agents et des collecteurs de données permettant de surveiller des applications et d'autres ressources installées dans votre entreprise. Pour une liste des agents et collecteurs de données de cette offre, voir «Fonctions», à la page 55.

Cette offre permet aux opérateurs informatiques de traiter les transactions lentes, les problèmes de capacité et les pannes.

Modules complémentaires

Advanced Extension Pack

Ce module d'extension contient Monitoring Agent for SAP HANA Database, l'Agent SAP NetWeaver Java Stack et Monitoring Agent for RabbitMQ.

Utilisez l'Agent SAP HANA Database pour surveiller la base de données SAP HANA. Utilisez l'Agent SAP NetWeaver Java Stack pour surveiller SAP NetWeaver Java Stack. Utilisez l'agent RabbitMQ pour surveiller la messagerie RabbitMQ. Ce module d'extension est disponible si vous disposez de l'offre IBM Cloud Application Performance Management, Advanced.

Base Extension Pack

Ce module d'extension contient les agents suivants :

- Monitoring Agent for Cassandra
- Monitoring Agent for InfoSphere DataStage
- Monitoring Agent for Hadoop
- Monitoring Agent for Microsoft Office 365
- Monitoring Agent for Sterling Connect Direct
- Monitoring Agent for Sterling File Gateway

Utilisez ces agents pour surveiller une base de données Cassandra, un cluster Hadoop, des ressources de serveur DataStage, des applications Microsoft Office 365, des serveurs Connect Direct et des applications Sterling File Gateway. Ce module d'extension est disponible si vous disposez de l'une des offres Cloud APM.

Infrastructure Extension Pack

Ce module d'extension contient les agents suivants :

- Monitoring Agent for Amazon EC2
- Monitoring Agent for AWS Elastic Load Balancer
- Monitoring Agent for Azure Compute
- Monitoring Agent for Citrix Virtual Desktop Infrastructure
- Monitoring Agent for IBM Cloud

Utilisez l'agent Amazon EC2 pour surveiller vos instances Amazon EC2. Utilisez l'agent Amazon ELB pour surveiller vos équilibreurs de charge élastiques AWS. Utilisez l'Agent Azure Compute pour surveiller vos machines virtuelles Azure Compute. Utilisez l'agent Citrix VDI pour surveiller votre infrastructure de bureau virtuel Citrix.

Ce module d'extension est disponible si vous disposez de l'une des offres Cloud APM.

z Systems Extension Pack

Vous pouvez utiliser z Systems Extension Pack pour visualiser les données de surveillance et les événements associés à vos composants d'application OMEGAMON dans la console Cloud APM. Ce module d'extension est disponible si vous disposez de l'une des offres Cloud APM.

Operations Analytics - Predictive Insights

Ce module complémentaire permet d'analyser les données de mesure qui sont collectées par Cloud APM et de générer des alarmes si des anomalies sont détectées. Le module complémentaire est disponible si vous disposez de l'une des offres Cloud APM.

Availability Monitoring
Ce module complémentaire permet de surveiller la disponibilité et les performances de vos applications Web à partir de plusieurs points de présence géographiquement répartis. Ce module complémentaire ne fonctionne pas comme une offre autonome, mais est disponible si vous disposez de l'offre IBM Cloud Application Performance Management, Advanced.

Pour avoir un aperçu des fonctions disponibles dans chaque offre, voir «Détails d'offre», à la page 50.

Pour obtenir une description de chaque agent et collecteur de données, ainsi que des liens vers les informations spécifiques à chacun, voir «Descriptions», à la page 59.

Détails d'offre

Certaines fonctions sont disponibles dans toutes les offres ; d'autres sont proposées uniquement dans une sélection d'offres.

Le Tableau 1, à la page 50 répertorie les principales fonctions disponibles avec chaque offre.

Tableau 1. Fonctions disponibles avec chaque offre

Fonction	Cloud APM, Advanced (Pour DevOps, les développeurs et le secteur d'activité)	Cloud APM, Base (Pour les opérations)
Surveillance des ressources d'application : Langues, middleware (le degré de couverture varie selon l'offre).	✓	✓
Surveillance du système d'exploitation : Systèmes Linux, UNIX et Windows	✓	✓
Surveillance des fichiers journaux : Utilisez les agents de système d'exploitation pour surveiller les fichiers journaux d'application.	✓	✓
Tableaux de bord : • Affichez les indicateurs clés de performance Tivoli Monitoring et Cloud APM dans les mêmes tableaux de bord • Mesures historiques • Tableaux de bords personnalisables	✓	✓
API : Gérez votre environnement à l'aide des API.	✓	✓
Contrôle d'accès basé sur les rôles : Gérez l'accès et les privilèges de vos utilisateurs IBM Cloud Application Performance Management.	✓	✓
Génération de rapports d'historique : Générez des rapports consignant les performances et les temps de réponse de vos applications par transaction, unité, navigateur, etc. (le niveau de couverture varie selon l'offre).	✓	✓
IBM Agent Builder: Créez des agents personnalisés pour surveiller vos différentes plateformes ou technologies.	✓	✓
Surveillance des ressources de base de données : (le degré de couverture varie selon l'offre).	✓	✓

Tableau 1. Fonctions disponibles avec chaque offre (suite)

Fonction	Cloud APM, Advanced (Pour DevOps, les développeurs et le secteur d'activité)	Cloud APM, Base (Pour les opérations)
Surveillance des ressources d'infrastructure : Hyperviseurs, stockage et réseau (le degré de couverture varie selon l'offre).	✓	✓
Surveillance des ressources d'applications commerciales : Applications métier et collaboratives (le degré de couverture varie selon l'offre).	✓	✓
Surveillance des temps de réponse : Identifiez en quoi les performances de l'application affectent vos utilisateurs.	✓	✓
Intégration avec l'analyse de recherche : Recherchez des informations approfondies pour isoler, diagnostiquer et résoudre les problèmes rapidement.	✓	✓
Operations Analytics - Predictive Insights (module complémentaire) : Identifiez les anomalies de performance des applications avant qu'elles n'affectent vos utilisateurs.	✓	✓
Surveillance de l'expérience réelle des utilisateurs : Identifiez les acquis de vos utilisateurs suite à l'utilisation de votre infrastructure sur leur unité.	✓	–
Suivi des transactions : Suivez les transactions de bout en bout au sein de votre environnement d'application. • Topologie d'application : Voyez comment tous les composants sont connectés dans votre environnement d'application. • Topologie des instances de transaction : Visualisez le chemin suivi par chaque instance d'une transaction au sein de votre environnement.	✓	–
Diagnostic approfondi : • Faites une exploration à partir des tableaux de bord récapitulatifs pour afficher des détails sur le niveau de code, les traces de pile et les requêtes SQL concernant des agents spécifiques. • Détectez, diagnostiquez et arrêtez les transactions lentes ou bloquées toujours en cours.	✓	–
Seuils : Détectez des conditions et des comportements d'application spécifiques en fonction de définitions activement surveillées.	✓	✓
Groupes de ressources : Classez les systèmes gérés de votre entreprise surveillée en fonction de leur objet.	✓	✓

Des fonctions supplémentaires, telles que celles décrites ci-dessous, sont disponibles pour toutes les offres par le biais de l'intégration avec d'autres produits et composants. Voir «Intégration », à la page 81 et, pour des informations détaillées, voir Chapitre 8, «Intégration à d'autres produits et composants», à la page 975.)

- Agents Tivoli Monitoring et OMEGAMON : Utilisez la passerelle hybride pour récupérer les données et événements de surveillance pour que ces informations s'affichent dans la console Cloud APM.
- Coexistence des agents : Installez les agents Cloud APM sur le même ordinateur que les agents Tivoli Monitoring.
- Netcool/OMNIbus et autres récepteurs EIF : Transférez les événements à l'IBM Tivoli Netcool/OMNIbus.
- Alert Notification : Recevez une notification lorsque les performances de l'application dépassent les seuils.
- IBM Control Desk : Ouvrez automatiquement des tickets dans Control Desk.
- IBM Cloud : Surveillez les applications IBM Cloud.

Agents et collecteurs de données

Les agents et les collecteurs de données IBM Cloud Application Performance Management sont disponibles à la fois dans les offres et les modules complémentaires.

Nombre de ressources de votre environnement peuvent être surveillées par des agents. Certaines ressources sur IBM Cloud et sur site peuvent être surveillées par des collecteurs de données. Des agents correspondants existent pour tous les collecteurs de données, exceptés les collecteurs de données J2SE et Python. Pour obtenir la liste des agents et des collecteurs de données ainsi que leur description, voir «Descriptions», à la page 59. Pour connaître les fonctions offertes par l'agent ou le collecteur de données pour chaque offre, voir «Fonctions», à la page 55. Pour connaître l'historique des modifications, voir «Historique des modifications», à la page 53.

Vous pouvez installer ces agents ou collecteurs de données, selon votre environnement et vos exigences. Les collecteurs de données envoient des données directement au serveur Cloud APM. Lorsqu'un agent est configuré, les collecteurs de données lui envoient des données et l'agent les transmet au serveur. Les collecteurs de données fonctionnent dans l'espace des processus d'application, tandis que les agents sont exécutés comme des processus distincts en dehors de l'espace des processus d'application.

Installez des collecteurs de données dans les cas suivants :

- Vous souhaitez une procédure d'installation plus simple.
- Vous utilisez des conteneurs.

Installez des agents dans les cas suivants :

- Vous souhaitez une plus grande évolutivité.
- Vous souhaitez limiter le nombre de sockets des noeuds finals au serveur.
- Lorsque vous ajoutez un seuil dans l'éditeur de seuil, vous souhaitez une liste claire, qui ne contient que les attributs de l'environnement à surveiller. Si vous utilisez un collecteur de données, vous devez sélectionner des attributs de plusieurs collecteurs de données.
- Vous souhaitez activer ou désactiver les fonctions de collecte de données dans l'interface utilisateur, telles que les diagnostics, le suivi des transactions ou la trace de méthode.
- Vous souhaitez afficher les données de diagnostic à la demande, telles que les demandes en cours et le cliché de tas à l'heure actuelle.

Historique des modifications

Recherchez des informations sur les versions et l'historique des changements pour chaque agent et collecteur de données.

Le tableau suivant répertorie le nom des agents et des collecteurs de données, ainsi que des liens vers des notes techniques relatives à l'historique des changements. Cliquez sur les liens pour afficher les détails de l'historique des changements.

Tableau 2. Historique des changements des agents et collecteurs de données

Agents et collecteurs de données	**Liens**
agent Amazon EC2	Historique des changements
agent Amazon ELB	Historique des changements
Agent Azure Compute	Historique des changements
agent Cassandra	Historique des changements
agent Cisco UCS	Historique des changements
agent Citrix VDI	Historique des changements
agent DataPower	Historique des changements
agent DataStage	Historique des changements
agent Db2	Historique des changements
agent Hadoop	Historique des changements
agent HMC Base	Historique des changements
agent HTTP Server	Historique des changements
agent IBM Cloud	Historique des changements
agent IBM Integration Bus	Historique des changements
Internet Service Monitoring	Historique des changements
collecteur de données J2SE	Historique des changements
agent JBoss	Historique des changements
collecteur de données Liberty	Historique des changements
agent Linux KVM	Historique des changements
Linux OS	Historique des changements
Agent MariaDB	Historique des changements
agent Microsoft Active Directory	Historique des changements
agent Microsoft Cluster Server	Historique des changements
agent Microsoft Exchange Server	Historique des changements
agent Microsoft Hyper-V Server	Historique des changements
agent Microsoft IIS	Historique des changements
agent Microsoft .NET	Historique des changements
agent Microsoft Office 365	Historique des changements
agent MicrosoftSharePoint Server	Historique des changements

Tableau 2. Historique des changements des agents et collecteurs de données (suite)	
Agents et collecteurs de données	**Liens**
agent Microsoft SQL Server	Historique des changements
Agent MongoDB	Historique des changements
Agent MQ Appliance	Historique des changements
Agent MySQL	Historique des changements
agent NetApp Storage	Historique des changements
Agent Node.js	Historique des changements
collecteur de données Node.js	Historique des changements
Agent OpenStack	Historique des changements
Agent Oracle Database	Historique des changements
Agent PHP	Historique des changements
Agent PostgreSQL	Historique des changements
collecteur de données Python	Historique des changements
agent RabbitMQ	Historique des changements
Agent de surveillance des temps de réponse	Historique des changements
Agent Ruby	Historique des changements
collecteur de données Ruby	Historique des changements
Agent SAP	Historique des changements
Agent SAP HANA Database	Historique des changements
Agent SAP NetWeaver Java Stack	Historique des changements
agent Siebel	Historique des changements
Agent Skype for Business Server	Historique des changements
Agent Sterling Connect Direct	Historique des changements
Agent Sterling File Gateway	Historique des changements
agent Sybase	Historique des changements
Agent Synthetic Playback	Historique des changements
Agent Tomcat	Historique des changements
Agent UNIX OS	Historique des changements
Agent VMware VI	Historique des changements
Agent WebLogic	Historique des changements
Agent WebSphere Applications	Historique des changements
agent WebSphere Infrastructure Manager	Historique des changements
agent WebSphere MQ	Historique des changements
agent Windows OS	Historique des changements

Fonctions

Les fonctionnalités d'agent et de collecteur de données varient en fonction de votre offre. Les principales fonctionnalités d'agent et de collecteur de données sont la surveillance des ressources, le suivi des transactions et le diagnostic. Vous pouvez vous abonner à toutes les offres et à tous les modules complémentaires proposés dans IBM Cloud Application Performance Management. Des offres spécifiques sont requises pour les modules complémentaires.

Chaque agent et collecteur de données surveille les ressources correspondant à son nom ; par exemple, Monitoring Agent for Cisco UCS surveille les ressources Cisco UCS.

Selon que vous êtes développeur, dans les opérations, ou propriétaire sectoriel, vous utilisez différentes fonctions d'Cloud APM.

- La fonction de surveillance des ressources inclut la surveillance des temps de réponse, la surveillance des ressources des applications et la surveillance des ressources d'infrastructure. Tous les agents et collecteurs de données peuvent offrir une fonction de surveillance des ressources.
- La fonction de suivi des transactions fournit des informations sur la topologie et l'instance de transaction.
- La fonction de diagnostic inclut le suivi et l'analyse de demandes spécifiques et, si nécessaire, d'appels de méthode.

A faire : La fonction de surveillance des ressources est commune à toutes les offres et tous les modules complémentaires. Les fonctions de diagnostic et de suivi des transactions sont uniquement disponibles dans l'offre Cloud APM, Advanced et ses modules complémentaires.

Les agents et les collecteurs de données pour les applications que vous souhaitez surveiller peuvent être téléchargés à partir de **Produits et services**. L'installation des agents prend plusieurs minutes. Les collecteurs de données ne nécessitent pas d'installation, vous devez simplement les configurer une fois le téléchargement terminé. Pour connaître les instructions d'installation des agents, voir Chapitre 6, «Installation des agents», à la page 123.

Le Tableau 3, à la page 55 fournit une liste complète des agents et des collecteurs de données, montre quelle offre ou quel module complémentaire contient l'agent ou le collecteur de données, et présente les fonctionnalités de l'agent ou du collecteur de données. Lorsque des modules complémentaires (tels que Infrastructure Extension Pack) sont répertoriés pour un agent ou un collecteur de données, ils sont alors obligatoires. Les agents et les collecteurs de données qui prennent en charge les fonctions de suivi des transactions et/ou de diagnostic sont également indiqués dans la colonne Cloud APM, Advanced.

✓ indique que l'agent ou le collecteur de données est disponible dans l'offre et qu'il peut offrir la fonction de surveillance des ressources.

— indique que les données ou la fonction n'est pas disponible dans cette offre, ou que le module complémentaire n'est pas requis pour l'agent ou le collecteur de données.

ST fait référence au suivi des transactions.

DD fait référence au diagnostic.

Tableau 3. Fonctions de l'agent et du collecteur de données dans chaque offre

Agents et collecteurs de données	Cloud APM, BaseCloud APM, Base Private	Cloud APM, Advanced	Module complémentaire (si requis)
agent Amazon EC2	✓	✓	Infrastructure Extension Pack
agent Amazon ELB	✓	✓	Infrastructure Extension Pack

Tableau 3. Fonctions de l'agent et du collecteur de données dans chaque offre (suite)

Agents et collecteurs de données	Cloud APM, BaseCloud APM, Base Private	Cloud APM, Advanced	Module complémentaire (si requis)
Agent Azure Compute	✓	✓	Infrastructure Extension Pack
agent Cassandra	✓	✓	Base Extension Pack
agent Cisco UCS	✓	✓	—
agent Citrix VDI	✓	✓	Infrastructure Extension Pack
agent Db2	✓	✓	—
agent DataPower	✓	✓ TT	—
agent DataStage	✓	✓	Base Extension Pack
agent Hadoop	✓	✓	Base Extension Pack
agent HMC Base	✓	✓	—
agent HTTP Server	✓	✓ TT	—
agent IBM Cloud	✓	✓	Infrastructure Extension Pack
agent IBM Integration Bus	—	✓ TT	—
Internet Service Monitoring	—	—	Base Extension Pack
collecteur de données J2SE pour les applications sur site	—	✓ ST DD	—
agent JBoss	✓	✓ ST DD	—
collecteur de données Liberty pour les applications IBM Cloud et sur site	—	✓ ST DD	—
agent Linux KVM	✓	✓	—
Linux OS	✓	✓	—
agent Microsoft Active Directory	✓	✓	—

Tableau 3. Fonctions de l'agent et du collecteur de données dans chaque offre (suite)

Agents et collecteurs de données	Cloud APM, BaseCloud APM, Base Private	Cloud APM, Advanced	Module complémentaire (si requis)
agent Microsoft Cluster Server	✓	✓	—
agent Microsoft Exchange Server	✓	✓	—
agent Microsoft Hyper-V Server	✓	✓	—
agent Microsoft IIS	✓	✓	—
agent Microsoft .NET	✓	✓ ST DD	—
agent Microsoft Office 365	✓	✓	Base Extension Pack
agent MicrosoftSharePoint Server	✓	✓	—
agent Microsoft SQL Server	✓	✓	—
Agent MongoDB	✓	✓	—
Agent MQ Appliance	—	✓	—
Agent MySQL	✓	✓	—
agent NetApp Storage	✓	✓	—
Agent Node.js	✓	✓ DD	—
collecteur de données Node.js pour les applications IBM Cloud et sur site	—	✓ ST DD	—
Agent OpenStack	✓	✓	—
Agent Oracle Database	✓	✓	—
Agent PHP	✓	✓	—
Agent PostgreSQL	✓	✓	—
collecteur de données Python pour les applications IBM Cloud et sur site	✓	✓ DD	—
agent RabbitMQ	—	✓	Advanced Extension Pack
Agent de surveillance des temps de réponse	✓	✓ TT	—
Agent Ruby	✓	✓ DD	—
collecteur de données Ruby pour les applications IBM Cloud	—	✓ DD	—

Tableau 3. Fonctions de l'agent et du collecteur de données dans chaque offre (suite)			
Agents et collecteurs de données	**Cloud APM, BaseCloud APM, Base Private**	**Cloud APM, Advanced**	**Module complémentaire (si requis)**
Agent SAP	—	✓	—
Agent SAP HANA Database	—	✓	Advanced Extension Pack
Agent SAP NetWeaver Java Stack	—	✓ ST DD	Advanced Extension Pack
agent Siebel	✓	✓	—
Agent Skype for Business Server (anciennement agent Microsoft Lync Server)	✓	✓	—
Agent Sterling Connect Direct	✓	✓	Base Extension Pack
Agent Sterling File Gateway	✓	✓	Base Extension Pack
agent Sybase	✓	✓	—
Agent Tomcat	✓	✓ TT	—
Agent UNIX OS	✓	✓	—
Agent VMware VI	✓	✓	—
Agent WebLogic	✓	✓ ST DD	—
Agent WebSphere Applications	✓	✓ ST DD	—
agent WebSphere Infrastructure Manager	✓	✓	—
agent WebSphere MQ	—	✓ TT	—
agent Windows OS	✓	✓	—

Pour savoir si la fonction de suivi des transactions ou de diagnostic est activée par défaut pour l'agent ou le collecteur de données, voir le tableau Activation du suivi des transactions pour les agents et les collecteurs de données. Pour plus d'informations sur les tableaux de bord de diagnostic des prédéfinis, voir Tableaux de bord de diagnostic des agents et collecteurs de données.

Descriptions

Les descriptions des agents et des collecteurs de données fournissent des informations sur ce que chacun de ces composants surveille et renvoient vers des informations supplémentaires sur chaque composant.

A chaque agent et collecteur de données est associé un numéro de version qui change chaque fois que l'agent ou le collecteur de données est mis à jour. Dans toute nouvelle édition, des agents et collecteurs de données peuvent être ajoutés et des agents et collecteurs de données existants mis à jour. Si vous ne disposez pas de la dernière version d'un agent ou collecteur de données, prévoyez de le mettre à jour. Pour plus d'informations sur la vérification de la version d'un agent ou d'un collecteur de données dans votre environnement, voir Commande de version d'agent.

Chaque description d'agent et de collecteur de données fournit des liens vers les types de détails suivants relatifs à ces composants :

- Configuration d'agent ou de collecteur de données et autres informations sur des fonctionnalités d'agents ou de collecteurs de données spécifiques
- Fichier PDF de référence qui contient des descriptions des tableaux de bord d'agent ou de collecteur de données, widgets de groupe, seuils, ensembles de données et attributs Cloud APM (mesures et indicateurs clés de performance)

Pour des liens vers la documentation des agents versions 6 et 7 d'IBM Tivoli Monitoring qui peuvent coexister avec des agents et collecteurs de données de Cloud APM version 8, voir Tableau 236, à la page 977.

Surveillance d'Amazon EC2

Monitoring Agent for Amazon EC2 permet de surveiller de manière centralisée la santé, la disponibilité et les performances des instances Amazon Elastic Compute Cloud (EC2). Il fournit un ensemble complet de mesures qui vous aident à prendre des décisions avisées concernant votre environnement EC2, y compris l'utilisation de l'UC, l'utilisation d'Elastic Block Store (EBS), l'utilisation du réseau, les mises à jour de maintenance d'Amazon Web Services (AWS) et la performance des disques.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance d'Amazon EC2», à la page 194.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Amazon EC2 Reference.

Surveillance d'AWS Elastic Load Balancer

L'agent Amazon ELB permet de surveiller de manière centralisée la santé, la disponibilité et les performances de vos équilibreurs de charge élastiques AWS. L'agent affiche un ensemble complet de mesures pour chaque type d'équilibreur de charge, application, réseau et classique, qui vous aident à prendre des décisions avisées concernant votre environnement AWS Elastic Load Balancer.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance d'AWS Elastic Load Balancer», à la page 202.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Amazon ELB Reference.

Surveillance Azure Compute

L'Agent Azure Compute permet de surveiller de manière centralisée la santé, la disponibilité et les performances de vos instances Azure Compute. L'agent affiche un ensemble complet de mesures qui vous aident à prendre des décisions avisées concernant votre environnement Azure Compute. Ces métriques incluent l'utilisation de l'UC, l'utilisation du réseau et les performances du disque.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance Azure Compute», à la page 207.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Azure Compute Reference.

Surveillance de Cassandra

L'agent Monitoring Agent for Cassandra vous offre la possibilité de surveiller le cluster Cassandra. Vous pouvez collecter et analyser les informations relatives aux noeuds, espaces de clé et familles de colonnes du cluster Cassandra.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Cassandra», à la page 217.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Cassandra Reference.

Surveillance de Cisco UCS

Monitoring Agent for Cisco UCS fournit un environnement permettant de surveiller la santé, le réseau et les performances de Cisco UCS. Il fournit une méthode complète de collecte et d'analyse des informations propres à Cisco UCS qui sont requises pour détecter les problèmes de manière précoce et les éviter.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Cisco UCS», à la page 220.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Cisco UCS Reference.

Surveillance de Citrix Virtual Desktop Infrastructure

Monitoring Agent for Citrix Virtual Desktop Infrastructure permet de surveiller de manière centralisée la santé, la disponibilité et les performances de votre infrastructure de postes de travail virtuels Citrix. L'agent affiche un ensemble complet de mesures qui vous aident à prendre des décisions avisées concernant vos ressources XenDesktop ou XenApp, y compris les sites, les machines, les applications, les bureaux, les sessions, les utilisateurs, etc.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Citrix Virtual Desktop Infrastructure», à la page 227.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Citrix VDI Reference.

Surveillance de DataPower

Monitoring Agent for DataPower permet de surveiller de manière centralisée les dispositifs DataPower dans votre environnement d'entreprise. Il permet d'identifier et de recevoir des notifications sur les problèmes courants liés aux dispositifs. L'agent fournit également des informations sur les performances, les ressources et la charge de travail des dispositifs.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de l'agent DataPower», à la page 246.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir DataPower agent Reference.
- Pour plus d'informations sur la surveillance des dispositifs DataPower dans la Pile d'intégration IBM, voir «Surveillance de la Pile d'intégration IBM», à la page 99.

Surveillance de la Db2

Monitoring Agent for Db2 offre un point central de surveillance de votre environnement Db2. Il permet de surveiller un grand nombre de serveurs à partir d'une console IBM Performance Management unique, chaque serveur étant surveillé par un agent Db2. Vous pouvez collecter et analyser des informations liées aux applications, bases de données et ressources système.

- Pour obtenir des informations préalablement à la mise à niveau vers une nouvelle version de l'agent, voir «Agents sous AIX : arrêt de l'agent et exécution de slibclean avant la mise à niveau», à la page 1174
- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Db2 », à la page 249.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Db2 Reference.

- Pour plus d'informations sur la surveillance des transactions de base de données dans la Liste d'applications Java IBM, voir «Surveillance de la Liste d'applications Java IBM», à la page 92.

Surveillance de Hadoop

Monitoring Agent for Hadoop fournit à votre organisation des fonctions de surveillance du cluster Hadoop. Il permet de collecter et d'analyser les informations relatives au cluster Hadoop telles que le statut des noeuds de données, les données concernant la machine virtuelle Java, les segments de mémoire et les segments de mémoire non dynamique, les informations sur les noeuds Hadoop, les systèmes de fichiers et les files d'attente.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Hadoop», à la page 261.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Hadoop Reference.

Surveillance de HMC Base

Monitoring Agent for HMC Base offre la possibilité de surveiller la console HMC (Hardware Management Console). Il surveille la disponibilité et la santé des ressources HMC : UC, mémoire, stockage et réseau. L'agent génère également des rapports sur l'inventaire et la configuration HMC des serveurs Power, des pools d'UC et des partitions logiques. Les utilisations de l'UC par les serveurs Power, les partitions logiques et les pools sont surveillées à l'aide des exemple de données de performances HMC.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de HMC Base», à la page 270.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent HMC Base Reference.

Surveillance de HTTP Server

Monitoring Agent for HTTP Server collecte les données relatives aux performances d'IBM HTTP Server. Par exemple, des informations sur le serveur s'affichent, comme l'état et le type du serveur, le nombre d'erreurs de serveur et de connexions au serveur réussies ou ayant échoué. Un collecteur de données rassemble les données qui sont envoyées à l'agent HTTP Server. Ce dernier s'exécute sur le même système que le serveur IBM HTTP Server qu'il surveille. Chaque serveur surveillé est enregistré en tant que sous-noeud. Le module Temps de réponse IBM HTTP Server est installé avec l'agent HTTP Server. Lorsque vous utilisez l'agent HTTP Server avec l'agent de surveillance Temps de réponse, l'agent WebSphere Application et un agent de base de données, les informations de surveillance des transactions s'affichent dans le navigateur pour la base de données de la pile d'applications IBM Java.

- Avant de commencer l'installation de l'agent, voir Préinstallation sur des systèmes AIX - agent HTTP Server et Préinstallation sur des systèmes Linux - agent HTTP Server.
- Pour savoir comment réviser les paramètres du collecteur de données et activer celui-ci après installation de l'agent, voir «Configuration de la surveillance de HTTP Server», à la page 275.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent HTTP Server Reference.
- Pour plus d'informations sur la surveillance des transactions du serveur HTTP dans la Liste d'applications Java IBM, voir «Surveillance de la Liste d'applications Java IBM», à la page 92.

IBM Cloud monitoring

Monitoring Agent for IBM Cloud collecte l'inventaire de machine virtuelle et les métriques auprès de votre compte IBM Cloud (Softlayer). L'agent IBM Cloud permet de suivre le nombre de périphériques virtuels que vous avez configurés et qui sont en cours d'exécution dans IBM Cloud. Vous pouvez visualiser les ressources allouées à chaque périphérique virtuel sur la page du tableau de bord détaillé, qui contient également certaines informations telles que le centre de données dans lequel se trouve un périphérique, le système d'exploitation et la bande passante de réseau public prévisionnelle pour le mois.

- Pour plus d'informations sur la configuration de l'agent après l'installation, voir Configuring IBM Cloud monitoring.

- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent IBM Cloud Reference.

Surveillance d'IBM Integration Bus

Monitoring Agent for IBM Integration Bus est un outil de surveillance et de gestion qui fournit la possibilité de vérifier, analyser et ajuster les topologies de courtier de messages qui sont associées aux produits IBM WebSphere Message Broker et IBM Integration Bus.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance d'IBM Integration Bus», à la page 283.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent IBM Integration Bus Reference.
- Pour plus d'informations sur la surveillance des courtiers IBM Integration Bus dans la Pile d'intégration IBM, voir «Surveillance de la Pile d'intégration IBM», à la page 99.

Surveillance d'InfoSphere DataStage

L'agent de surveillance d'InfoSphere DataStage surveille la disponibilité, l'utilisation des ressources et les performances du serveur DataStage. Il contrôle l'état de santé des noeuds et des tâches du moteur. Vous pouvez analyser les informations collectées par l'agent et prendre les mesures appropriées pour résoudre les problèmes du serveur DataStage.

- Pour plus d'informations sur la configuration de l'agent après l'installation, voir Configuring InfoSphere DataStage monitoring.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent DataStage Reference.

Internet Service Monitoring

Internet Service Monitoring permet de déterminer si un service particulier fonctionne de manière adéquate, d'identifier les zones problématiques et de générer un rapport sur les performances du service mesurées par rapport aux exigences des contrats de niveau de service (SLA). Internet Service Monitoring agent fonctionne par émulation des actions d'un utilisateur réel. Il interroge ou teste régulièrement les services Internet pour vérifier leur statut et leurs performances.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de l'agent sur des systèmes Windows», à la page 456.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir le document Internet Service Monitoring agent Reference

Surveillance du collecteur de données J2SE

Le collecteur de données J2SE collecte les données de surveillance des ressources et de diagnostics approfondis pour les applications Java. Les données de diagnostic approfondi sont affichées dans les tableaux de bord en fonction des demandes et des informations globales pour prendre en charge diverses vues d'exploration. La surveillance des ressources et le diagnostic approfondi sont pris en charge, ce qui permet de détecter, isoler et diagnostiquer les problèmes de vos applications Java. Vous pouvez configurer le collecteur de données pour diagnostiquer les demandes lentes.

- Pour plus d'informations sur la configuration du collecteur de données, voir Configuration du collecteur de données J2SE.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir J2SE data collector Reference.

Surveillance de JBoss

Monitoring Agent for JBoss surveille les ressources des serveurs d'applications JBoss et de la plateforme JBoss Enterprise Application. Utilisez les tableaux de bord fournis avec l'agent JBoss pour identifier les applications et les demandes les plus lentes, les goulots d'étranglement dans le pool d'unités d'exécution, les problèmes de segment de mémoire JVM et de récupération de place, les sessions les plus actives et les autres goulots d'étranglement sur le serveur d'applications JBoss.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de JBoss», à la page 467.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent JBoss Reference.

Surveillance de Linux KVM

Monitoring Agent for Linux KVM est un agent multi-instance et multiconnexion qui prend en charge des connexions d'hyperviseur KVM basé sur Enterprise Linux et des environnements RHEV-M (Red Hat Enterprise Virtualization Manager). Vous pouvez créer plusieurs instances de cet agent pour surveiller plusieurs hyperviseurs dans un environnement d'hyperviseur RHEV-M ou KVM. Vous pouvez surveiller les charges de travail virtualisées et analyser la capacité de ressources sur des machines virtuelles différentes. Pour connecter l'agent à une machine virtuelle dans l'environnement de l'hyperviseur KVM, vous devez installer les conditions préalables requises : `libvirt*.rpm` et interpréteur de commandes Korn (pdksh). L'agent collecte des indicateurs en se connectant à distance à un hyperviseur libvirt qui gère les machines virtuelles.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Linux KVM», à la page 482.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Linux KVM Reference.

Surveillance de Linux OS

Monitoring Agent for Linux OS fournit des fonctions de surveillance de la disponibilité, des performances et de l'utilisation des ressources de l'environnement de système d'exploitation Linux. Cet agent prend en charge la surveillance du conteneur de docker. Par exemple, des informations détaillées sur l'utilisation de l'UC, de la mémoire, du réseau et des E/S liées au conteneur de docker s'affichent. Des informations générales sur les conteneurs de docker exécutés sur le serveur, telles que l'ID et le nom d'instance du docker, s'affichent également. En outre, vous pouvez configurer la surveillance des fichiers journaux afin de surveiller les fichiers journaux d'application. Vous pouvez collecter et analyser des informations propres au serveur, comme les performances du système d'exploitation et de l'UC, l'analyse des informations et des performances du disque Linux, l'analyse de l'état des processus et les performances réseau.

- Pour des informations sur la configuration de la surveillance des fichiers journaux après l'installation, voir «Configuration de la surveillance des fichiers journaux de l'agent de système d'exploitation», à la page 649.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Linux OS Reference.

Surveillance de MariaDB

Monitoring Agent for MariaDB offre un point central de gestion pour votre environnement ou application MariaDB. Ce logiciel offre une solution complète permettant de rassembler les informations dont vous avez besoin pour détecter les incidents de manière précoce et vous en prémunir. Les informations sont standardisées à travers le système. Vous pouvez surveiller plusieurs serveurs à partir d'une seule console. En utilisant Monitoring Agent for MariaDB, vous pouvez aisément collecter et analyser des informations sur MariaDB.
Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de MariaDB», à la page 494

Surveillance de Microsoft Active Directory

Monitoring Agent for Microsoft Active Directory fournit à votre organisation des fonctions de surveillance d'Active Directory. Il permet de collecter et d'analyser les informations propres à Active Directory, comme l'état du réseau, la réplication Sysvol, les performances du carnet d'adresses et l'utilisation du système d'annuaire.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Microsoft Active Directory», à la page 497.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Microsoft Active Directory Reference.

Surveillance de Microsoft Cluster Server

Monitoring Agent for Microsoft Cluster Server fournit à votre organisation des fonctions de surveillance de Microsoft Cluster Server. Il permet de collecter les informations liées à la disponibilité des ressources de cluster, comme le niveau, les noeuds, les groupes de ressources, les ressources et les réseaux du cluster. Il fournit également des statistiques sur l'utilisation des ressources du cluster, comme l'utilisation du processeur, de la mémoire, du disque et du réseau.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Microsoft Cluster Server», à la page 505.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Microsoft Cluster Server Reference.

Surveillance de Microsoft Exchange Server

Monitoring Agent for Microsoft Exchange Server offre à votre organisation des fonctions de surveillance de la santé, de la disponibilité et des performances des serveurs Exchange Server. Vous pouvez utiliser l'agent Microsoft Exchange Server pour collecter des informations propres au serveur, comme le trafic via la messagerie, l'état des bases de données de boîte aux lettres et les activités des clients. Il fournit également des statistiques sur l'utilisation du cache, de la messagerie et de la base de données et sur les activités des clients pour vous aider à analyser les performances des serveurs Exchange Server.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Microsoft Exchange», à la page 507.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Microsoft Exchange Server Reference.

Surveillance de Microsoft Hyper-V Server

Monitoring Agent for Microsoft Hyper-V Server offre à votre organisation la possibilité de surveiller la disponibilité et les performances de tous les systèmes Hyper-V. L'agent Microsoft Hyper-V Server fournit des informations de configuration comme le nombre et l'état des machines virtuelles, le nombre de disques virtuels alloués, la mémoire virtuelle allouée et le nombre de processeurs virtuels alloués. Il fournit également des statistiques sur l'utilisation du processeur physique, de la mémoire, du réseau, du processeur logique et du processeur virtuel.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Microsoft Hyper-V», à la page 521.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Microsoft Hyper-V Server Reference.

Surveillance de Microsoft Internet Information Services

Monitoring Agent for Microsoft Internet Information Services vous offre la possibilité de surveiller la disponibilité et les performances de Microsoft Internet Information Server. Vous pouvez utiliser l'agent Microsoft Internet Information Server pour surveiller les détails d'un site Web, comme le taux des demandes, la vitesse de transfert des données et les statistiques sur les erreurs et les connexions.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Microsoft IIS», à la page 525.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Microsoft IIS Reference.

Surveillance de Microsoft .NET

Monitoring Agent for Microsoft .NET surveille les applications Microsoft .NET qui sont basées sur Internet Information Services (IIS) et les ressources Microsoft .NET Framework. Le composant de collecteur de données collecte les données des demandes HTTP entrantes. Il collecte les appels de méthode, construit une arborescence d'appels et collecte le contexte des demandes et les données de trace de pile. Utilisez les tableaux de bord fournis avec l'agent Microsoft .NET pour identifier les problèmes liés à Microsoft .NET Framework et les demandes HTTP les plus lentes à partir desquelles vous pouvez explorer les informations de trace de pile pour isoler les problèmes.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Enregistrement du collecteur de données», à la page 535.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Microsoft .NET Reference.

Surveillance de Microsoft Office 365

L'agent Monitoring Agent for Microsoft Office 365 vous offre la possibilité de surveiller Microsoft Office 365. Vous pouvez collecter et analyser les informations relatives à Microsoft Exchange Online, SharePoint Online, Skype for Business et OneDrive for Business.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Microsoft Office 365», à la page 544.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Microsoft Office 365 Reference.

Surveillance de Microsoft SharePoint Server

Monitoring Agent for Microsoft SharePoint Server vous offre l'environnement permettant de surveiller la disponibilité, les événements et les performances de Microsoft SharePoint Server. Utilisez cet agent pour collecter des données à partir de Microsoft SharePoint Server et pour gérer les opérations.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Microsoft SharePoint Server », à la page 550.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent MicrosoftSharePoint Server Reference.

Surveillance de Microsoft SQL Server

L'agent Monitoring Agent for Microsoft SQL Server vous offre la possibilité de surveiller Microsoft SQL Server. L'agent Microsoft SQL Server offre un point de gestion centralisé des bases de données réparties. Utilisez les tableaux de bord de l'agent Microsoft SQL Server pour surveiller la disponibilité, les performances, l'utilisation des ressources et l'état général de toutes les instances SQL Server surveillées.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Microsoft SQL Server », à la page 553.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Microsoft SQL Server Reference.

Surveillance de MongoDB

Monitoring Agent for MongoDB fournit des fonctions de surveillance de l'utilisation, de l'état et des performances du déploiement MongoDB. Vous pouvez collecter et analyser des informations comme l'utilisation de la capacité de la base de données, le pourcentage de connexions ouvertes, l'utilisation de la mémoire, l'état de l'instance et le temps de réponse dans des tableaux de bord visualisés.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de MongoDB», à la page 586.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent MongoDB Reference.

Surveillance de MQ Appliances

Monitoring Agent for MQ Appliance fournit des informations sur la surveillance axées sur le niveau de MQ Appliances, telles que des informations récapitulatives sur l'UC, la mémoire, le stockage, les capteurs et les gestionnaires de files d'attente.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance d'IBM MQ Appliances», à la page 298.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir le document MQ Appliance agent Reference.

Surveillance de MySQL

Monitoring Agent for MySQL fournit des fonctions de surveillance de l'état, de l'utilisation et des performances du déploiement MySQL. Vous pouvez collecter et analyser des informations comme Octets reçus / envoyés, Pages du pool de mémoire tampon InnoDB et Historique des performances.

- Avant de commencer l'installation de l'agent, voir Préinstallation sur des systèmes Linux - Agent MySQL ou Préinstallation sur des systèmes Windows - Agent MySQL.
- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de MySQL», à la page 591.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent MySQL Reference.

Surveillance de NetApp Storage

Monitoring Agent for NetApp Storage vous permet de surveiller les systèmes de stockage NetApp à l'aide de NetApp OnCommand Unified Manager (OCUM). Vous pouvez collecter et analyser les informations relatives aux agrégats, aux noeuds, aux disques et aux volumes des systèmes de stockage NetApp.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de NetApp Storage», à la page 594.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent NetApp Storage Reference.

Surveillance de Node.js

Monitoring Agent for Node.js ou le collecteur de données Node.js autonome peut être utilisé pour mesurer et collecter des données sur les performances des applications Node.js. Par exemple, la capacité de traitement et les temps de réponse pour les demandes HTTP, ainsi que d'autres mesures liées à l'utilisation des ressources, sont surveillés et stockés à des fins d'affichage et d'analyse. Pour choisir entre l'Agent Node.js et le collecteur de données Node.js, reportez-vous à la rubrique «Configuration de la surveillance de Node.js», à la page 601 pour des instructions.

Agent Node.js

- Avant de commencer l'installation, voir Préinstallation sur des systèmes Linux - Agent Node.js.
- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de l'Agent Node.js», à la page 602.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Node.js Reference.

collecteur de données Node.js (autonome)

Le collecteur de données Node.js surveille les applications IBM Cloud et sur site. La surveillance des ressources et le diagnostic approfondi sont pris en charge, ce qui permet de détecter, isoler et diagnostiquer les problèmes de vos applications. Vous pouvez configurer le collecteur de données pour le suivi individuel des performances des demandes et des appels de méthode, utiliser ces informations pour diagnostiquer les demandes lentes et agir en conséquence.

Applications IBM Cloud

- Pour plus d'informations sur la configuration du collecteur de données, voir «Configuration du collecteur de données Node.js autonome pour les applications IBM Cloud(anciennement Bluemix)», à la page 608.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Data collectors Reference.

Applications sur site

- Pour plus d'informations sur la configuration du collecteur de données, voir «Configuration du collecteur de données Node.js autonome pour les applications sur site», à la page 615.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Data collectors Reference.

Surveillance d'OpenStack

Monitoring Agent for OpenStack vous permet de surveiller vos applications OpenStack. Utilisez les tableaux de bord pour visualiser les performances de vos applications OpenStack, telles que les informations sur les noeuds finals d'API, la connexion au serveur SSH, les processus et les hyperviseurs.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de l'Agent OpenStack», à la page 626.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent OpenStack Reference.

Surveillance d'Oracle Database

Monitoring Agent for Oracle Database fournit des fonctions de surveillance de la disponibilité, des performances et de l'utilisation des ressources de la base de données Oracle. Vous pouvez configurer plusieurs instances d'Agent Oracle Database pour surveiller différentes bases de données Oracle. La fonction de surveillance à distance est également fournie par cet agent.

- Avant de commencer l'installation de l'agent, voir Préinstallation sur des systèmes AIX - Agent Oracle Database, Préinstallation sur des systèmes Linux - Agent Oracle Database ou Préinstallation sur des systèmes Windows - Agent Oracle Database (Windows).
- Pour savoir comment configurer l'agent après installation, voir «Configuration de la surveillance d'Oracle Database», à la page 631.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Oracle Database Reference.
- Pour plus d'informations sur la surveillance des transactions de base de données dans la Liste d'applications Java IBM, voir «Surveillance de la Liste d'applications Java IBM», à la page 92.

Surveillance de PHP

Monitoring Agent for PHP surveille les applications Web PHP en collectant les indicateurs d'accès au Web via un serveur Web Apache et des données de statistiques de performances à partir de MySQL. L'agent reconnaît toutes les applications WordPress sur un serveur Apache et fournit des informations statistiques sur l'application WordPress. Il permet de surveiller la disponibilité du serveur Web, l'état du serveur Apache et les demandes GET/POST. L'agent évalue uniquement les performances des requêtes PHP dans les applications WordPress. Le chargement CSS et JS n'est pas évalué. L'agent n'utilise pas les arguments d'URL pour identifier les URL.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de PHP», à la page 682.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent PHP Reference.

Surveillance de PostgreSQL

Monitoring Agent for PostgreSQL surveille la base de données PostgreSQL en collectant des indicateurs PostgreSQL via un pilote JDBC. Il fournit des données sur l'utilisation des ressources système, la capacité de la base de données, les connexions utilisées, l'état individuel des instances en cours d'exécution, les statistiques sur les opérations, le temps de réponse pour les instructions de requête SQL, les détails de taille de la base de données et les informations de verrou.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance PostgreSQL», à la page 685.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent PostgreSQL Reference.

Surveillance de Python

Le collecteur de données Python surveille à la fois les applications Python sur site et IBM Cloud. La surveillance des ressources et le diagnostic approfondi sont tous deux pris en charge, ce qui génère des données de surveillance, telles que la quantité d'UC et de mémoire utilisée, la récupération de place et les unités d'exécution. Vous pouvez configurer le collecteur de données pour le suivi individuel des performances des demandes et des appels de méthode, utiliser ces informations pour diagnostiquer les demandes lentes et agir en conséquence.

Applications IBM Cloud

- Pour plus d'informations sur la configuration du collecteur de données, voir «Configuration du collecteur de données Python pour les applications IBM Cloud», à la page 689.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir le Data collectors Reference.

Applications sur site

- Pour plus d'informations sur la configuration du collecteur de données, voir «Configuration du collecteur de données Python pour les applications sur site», à la page 695.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Data collector Reference.

Surveillance de RabbitMQ

L'agent Monitoring Agent for RabbitMQ vous offre la possibilité de surveiller le cluster RabbitMQ. Vous pouvez collecter et analyser les informations relatives aux noeuds, files d'attente et chaînes du cluster RabbitMQ.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de RabbitMQ », à la page 701.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent RabbitMQ Reference.

Surveillance des temps de réponse

L'Agent de surveillance des temps de réponse utilise la surveillance du réseau pour capturer les données de transaction HTTP et HTTPS, telles que les temps de réponse et les codes de statut. Il permet de surveiller les performances et la disponibilité des applications Web pour les utilisateurs, y compris les informations relatives aux demandes de transaction, à l'application et aux serveurs. Utilisez également cet agent pour surveiller les périphériques et les informations de session.

- Avant de commencer l'installation de l'Agent de surveillance des temps de réponse, voir Préinstallation sur des systèmes AIX - Agent de surveillance des temps de réponse, Préinstallation sur des systèmes Linux - Agent de surveillance des temps de réponse ou Préinstallation sur des systèmes Windows - Agent de surveillance des temps de réponse.
- Pour plus d'informations sur la configuration de l'agent après installation, voir «Injection JavaScript», à la page 709.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Transaction Monitoring Reference.
- Pour plus d'informations sur l'utilisation de la Surveillance des temps de réponse dans la Liste d'applications Java IBM, voir «Surveillance de la Liste d'applications Java IBM», à la page 92.

Surveillance de Ruby

Monitoring Agent for Ruby ou les collecteurs de données Ruby autonomes surveillent les performances de vos applications Ruby on Rails, comprenant le trafic des demandes et les statistiques sur la configuration. Vous pouvez également utiliser la fonction de diagnostic pour obtenir une vue plus précise de chaque application.

Le collecteur de données Ruby autonome surveille uniquement les applications IBM Cloud.

Agent Ruby

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Ruby», à la page 737.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Ruby Reference.

collecteur de données Ruby (autonome)

Vous pouvez utiliser le collecteur de données Ruby pour surveiller les applications IBM Cloud. La surveillance des ressources et le diagnostic approfondi sont tous deux pris en charge, ce qui permet de détecter, isoler et diagnostiquer les problèmes de vos applications. Vous pouvez

configurer le collecteur de données pour le suivi individuel des performances des demandes et des appels de méthode, utiliser ces informations pour diagnostiquer les demandes lentes et agir en conséquence.

Applications IBM Cloud

- Pour plus d'informations sur la configuration du collecteur de données, voir Configuration du collecteur de données Ruby.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir le Data collectors Reference.

Surveillance des applications SAP

Monitoring Agent for SAP Applications vous offre la possibilité de surveiller vos applications SAP qui fonctionnent sur la pile Advanced Business Application Programming (ABAP). L'agent surveille également SAP Solution Manager, qui est un outil de gestion du cycle de vie SAP, et SAP NetWeaver Process Integration (SAP PI), qui est un logiciel d'intégration d'entreprise pour SAP. Il offre un point central de gestion pour la collecte des informations dont vous avez besoin pour détecter les problèmes de manière précoce et suivre la procédure nécessaire pour les éviter à nouveau. Il permet une gestion efficace des systèmes, quels que soient les modules, les applications et les versions de SAP, ainsi que les bases de données, systèmes d'exploitation et interfaces externes utilisés.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de SAP», à la page 750.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent SAP Reference.

Surveillance de SAP HANA Database

Monitoring Agent for SAP HANA Database surveille la disponibilité, l'utilisation des ressources et la performance de la base de données HANA SAP. L'agent peut surveiller les scénarios de déploiement HANA tels que hôte unique - base données unique, hôte unique - bases de données titulaires multiples, hôtes multiples - base de données unique et hôtes multiples - bases de données titulaires multiples. Vous pouvez analyser les informations que l'agent collecte et prendre des mesures appropriées pour résoudre des problèmes dans la base de données HANA SAP.

- Avant de commencer l'installation de l'agent, voir Préinstallation sur les systèmes AIX - Agent SAP HANA Database ou Préinstallation sur les systèmes Linux - Agent SAP HANA Database ou Préinstallation sur les systèmes Windows - Agent SAP HANA Database.
- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de SAP HANA Database», à la page 784.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent SAP HANA Database Reference.

Surveillance de SAP NetWeaver Java Stack

Monitoring Agent for SAP NetWeaver Java Stack surveille la disponibilité, l'utilisation des ressources et les performances de SAP NetWeaver Java Stack. L'agent peut surveiller les scénarios de déploiement SAP NetWeaver Java Stack tels que hôte unique - instance unique, hôte unique - instances multiples, hôtes multiples - instances uniques et hôtes multiples - instances multiples. Vous pouvez analyser les informations collectées par l'agent et prendre des mesures appropriées pour résoudre des problèmes dans SAP NetWeaver Java Stack.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de SAP NetWeaver Java Stack», à la page 786.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent SAP NetWeaver Java Stack Reference.

Surveillance de Siebel

Monitoring Agent for Siebel permet de surveiller de manière centralisée vos ressources Siebel, notamment les statistiques Siebel, les sessions utilisateur, les composants, les tâches, le serveur d'application, le serveur de noms de passerelle Siebel, l'utilisation de la mémoire et de l'UC de processus et la surveillance des événements du journal.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Siebel», à la page 793.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Siebel Reference.

Surveillance Skype for Business Server (anciennement Microsoft Lync Server)
Monitoring Agent for Skype for Business Server vous permet de surveiller la santé, la disponibilité et les performances de Skype for Business Server. Vous pouvez utiliser l'agent Skype for Business Server pour collecter des informations spécifiques au serveur, telles que le temps d'attente, les transactions synthétiques, les opérations d'écriture de service d'enregistrement de détail d'appel (CDR), l'état des demandes régulées et les homologues SIP. De plus, l'agent fournit des statistiques d'utilisation historiques de la messagerie instantanée et du serveur de médiation pour vous aider à analyser les performances des serveurs Lync ou Skype for Business.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Skype for Business Server (anciennement Microsoft Lync Server)», à la page 528.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Skype for Business Server Reference.

Surveillance Sterling Connect Direct
Monitoring Agent for Sterling Connect Direct permet de surveiller la santé et les performances des serveurs Connect Direct. Il permet de surveiller la santé et les performances des serveurs Connect Direct. Il fournit également une analyse de l'activité de transfert de fichiers.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance Sterling Connect Direct», à la page 805.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Sterling Connect Direct Reference.

Surveillance Sterling File Gateway
Monitoring Agent for Sterling File Gateway surveille l'application Sterling File Gateway, utilisée pour transférer des fichiers entre les partenaires internes et externes à l'aide de différents protocoles, différentes conventions de dénomination de fichier et différents formats de fichier. Il prend également en charge la fonction de surveillance à distance.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance Sterling File Gateway», à la page 808.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Sterling File Gateway Reference.

Surveillance Sybase Server
Monitoring Agent for Sybase Server permet d'assurer la gestion des bases de données réparties de manière centralisée. Il collecte les informations requises pour que les administrateurs de base de données et système puissent examiner les performances du système Sybase Server, détecter rapidement les problèmes et les empêcher.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Sybase Server», à la page 815.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir le document agent Sybase Reference.

Surveillance de Tomcat
Monitoring Agent for Tomcat surveille les ressources des serveurs d'applications Tomcat. Utilisez les tableaux de bord fournis avec l'agent Tomcat pour identifier les applications et les demandes les plus lentes, les goulots d'étranglement dans le pool d'unités d'exécution, les problèmes de segment de mémoire JVM et de récupération de place, les sessions les plus actives et les autres goulots d'étranglement sur le serveur d'applications Tomcat.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de Tomcat», à la page 823.

- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent Tomcat Reference.

Surveillance d'UNIX OS

Monitoring Agent for UNIX OS fournit des fonctions de surveillance de la disponibilité, des performances et de l'utilisation des ressources de l'environnement de système d'exploitation UNIX. (Systèmes d'exploitation AIX et Solaris uniquement. Voir System requirements dans APM Developer Center.) En outre, vous pouvez configurer la surveillance des fichiers journaux afin de surveiller les fichiers journaux d'application. Vous pouvez collecter et analyser des informations propres au serveur, comme les performances du système d'exploitation et de l'UC, l'analyse des informations sur le disque UNIX et des performances, l'analyse de l'état des processus et les performances réseau.

- Pour des informations sur la configuration de la surveillance des fichiers journaux après l'installation, voir «Configuration de la surveillance des fichiers journaux de l'agent de système d'exploitation», à la page 649.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent UNIX OS Reference.

Surveillance de VMware VI

Monitoring Agent for VMware VI surveille l'infrastructure virtuelle VMware en se connectant au centre virtuel VMware. Il permet d'afficher le récapitulatif d'état des clusters et de surveiller plusieurs composants, tels que les clusters, les machines virtuelles, les magasins de données et les serveurs ESX à partir d'une console unique.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de VMware VI», à la page 831.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent VMware VI Reference.

Surveillance de WebLogic

Monitoring Agent for WebLogic permet de surveiller de manière centralisée la santé, la disponibilité et les performances de votre environnement de serveur WebLogic. L'agent affiche un ensemble complet de mesures qui vous aident à prendre des décisions avisées concernant vos ressources WebLogic, y compris les machines virtuelles Java, le service de messagerie Java et la connectivité Java Database Connectivity (JDBC).

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de WebLogic», à la page 840.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent WebLogic Reference.

Surveillance des applications WebSphere

Monitoring Agent for WebSphere Applications avec le collecteur de données imbriqué ou le collecteur de données Liberty autonome surveille les ressources des serveurs WebSphere Application Server. Ces composants de surveillance peuvent être configurés pour effectuer les opérations suivantes :

- Ils collectent les indicateurs PMI de surveillance des ressources via une interface JMX sur le serveur d'applications.
- Ils collectent les métriques de performances des demandes agrégées.
- Ils suivent les performances des appels de demande et de méthode individuels.

Les données de surveillance sont affichées dans les tableaux de bord. Vous pouvez utiliser les tableaux de bord fournis pour isoler les zones problématiques de votre serveur d'applications. Effectuez une exploration en aval pour déterminer si un problème est lié à une ressource sous-jacente ou au code de l'application.

Pour déterminer si l'agent ou l'un des collecteurs de données doit être utilisé, voir «Configuration de la surveillance des applications WebSphere», à la page 856.

Agent et collecteur de données imbriqué des applications WebSphere

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration du collecteur de données pour l'Agent WebSphere Applications», à la page 857.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir Agent WebSphere Applications Reference.
- Pour plus d'informations sur la surveillance des transactions du serveur WebSphere dans la Liste d'applications Java IBM, voir «Surveillance de la Liste d'applications Java IBM», à la page 92.

Collecteur de données Liberty (autonome)

Vous pouvez utiliser le collecteur de données Liberty pour surveiller le profil WebSphere Liberty sur IBM Cloud ou surveiller WebSphere Application Server Liberty on Linux for System x. La surveillance des ressources, les diagnostics et le suivi des transactions sont tous pris en charge, ce qui permet de détecter, d'isoler et de diagnostiquer les problèmes de vos applications. Vous pouvez configurer le collecteur de données autonome pour le suivi individuel des performances des demandes et des appels de méthode, utiliser ces informations pour diagnostiquer les demandes lentes et agir en conséquence.

Applications IBM Cloud

- Pour plus d'informations sur la configuration du collecteur de données, voir «Configuration du collecteur de données Liberty pour les applications IBM Cloud», à la page 910.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir le Data collectors Reference.

Applications sur site (Linux for System x uniquement)

- Pour plus d'informations sur la configuration du collecteur de données, voir «Configuration du collecteur de données Liberty pour les applications sur site», à la page 906.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir le Data collectors Reference.

Surveillance de WebSphere Infrastructure Manager

Monitoring Agent for WebSphere Infrastructure Manager fournit les fonctionnalités de surveillance de WebSphere Application Server Deployment Manager et de l'agent de noeud, avec notamment le statut du serveur, les ressources et les transactions. Vous pouvez utiliser les données collectées par l'agent WebSphere Infrastructure Manager pour analyser les performances de votre gestionnaire de déploiement et de l'agent de noeud et déterminer si un problème s'est produit.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de WebSphere Infrastructure Manager», à la page 956.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent WebSphere Infrastructure Manager Reference.

Surveillance de WebSphere MQ

Avec Monitoring Agent for WebSphere MQ, vous pouvez aisément collecter et analyser les données propres à WebSphere MQ pour vos gestionnaires de files d'attente à partir d'un point d'observation unique. Vous pouvez alors suivre les tendances dans les données collectées et traiter les problèmes système à l'aide des tableaux de bord prédéfinis.

- Pour plus d'informations sur la configuration de l'agent après installation, voir «Configuration de la surveillance de WebSphere MQ», à la page 957.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent WebSphere MQ Reference.
- Pour plus d'informations sur la surveillance des files d'attente de message dans la Pile d'intégration IBM, voir «Surveillance de la Pile d'intégration IBM», à la page 99.

Surveillance de Windows OS

Monitoring Agent for Windows OS fournit des fonctions de surveillance de la disponibilité, des performances et de l'utilisation des ressources de l'environnement de système d'exploitation

Windows. En outre, vous pouvez configurer la surveillance des fichiers journaux afin de surveiller les fichiers journaux d'application. Vous pouvez collecter et analyser des informations propres au serveur, comme les performances du système d'exploitation et de l'UC, l'analyse des informations sur le disque et des performances, l'analyse de l'état des processus, les données de session Internet, les informations des journaux surveillés, les statistiques sur le serveur Internet, les statistiques sur la mise en file d'attente des messages, les données d'état d'imprimante et de travail, les statistiques Remote Access Services et les informations relatives aux services. Le service KNTCMA_FCProvider est installé avec l'agent.

- Pour des informations sur la configuration de la surveillance des fichiers journaux après l'installation, voir «Configuration de la surveillance des fichiers journaux de l'agent de système d'exploitation», à la page 649.
- Pour plus d'informations sur les tableaux de bord, les seuils et les attributs, voir agent Windows OS Reference.

Fonctions

Les fonctions principales varient selon l'offre utilisée. Certaines fonctions sont disponibles dans une seule ou dans les deux offres, dans un module complémentaire ou encore par le biais de l'intégration à d'autres produits et composants.

Surveillance des ressources d'application
Utilisez les agents de surveillance des ressources pour surveiller les langues et les middleware. La couverture varie selon l'offre. Voir «Fonctions», à la page 55 .

Surveillance du système d'exploitation
Utilisez les agents de surveillance des ressources pour surveiller les systèmes d'exploitation Linux, UNIX et Windows. Voir «Fonctions», à la page 55 .

Surveillance des fichiers journaux
Les agents de système d'exploitation incluent une fonction pour surveiller les fichiers journaux d'application. Cette fonction permet de configurer la surveillance des fichiers journaux sur la base d'expressions régulières.

Pour des raisons de compatibilité, l'agent de système d'exploitation utilise les informations et les formats suivants :

- Les informations de configuration et le fichier de format utilisé par IBM Tivoli Monitoring Log File Agent V6.x
- Les informations de configuration et les chaînes de format utilisées par Tivoli Event Console Log File Adapter

Ces chaînes de format permettent à l'agent de filtrer les données de journal en fonction de masques dans le fichier de format et de soumettre uniquement les données appropriées à un consommateur d'événement. L'agent de système d'exploitation envoie des données au serveur Cloud APM ou via EIF (Event Integration Facility) à un récepteur EIF, comme Netcool/OMNIbus Probe for Tivoli EIF.

Tableaux de bord
Le **Tableau de bord d'Application Performance** fournit le statut général des applications dans votre environnement. Visualisez les domaines qui vous intéressent en les sélectionnant dans le navigateur ou en cliquant dans une zone récapitulative pour accéder au niveau suivant.

Pour en savoir plus sur les fonctionnalités disponibles à chaque niveau du tableau de bord, voir «Toutes mes applications - Tableau de bord d'Application Performance», à la page 1109, «Application - Tableau de bord d'Application Performance», à la page 1112 et «Groupe et Instance - Tableau de bord d'Application Performance», à la page 1117.

Affichez les indicateurs clés de performance des domaines Tivoli Monitoring et Cloud APM dans les mêmes tableaux de bord
Dans un environnement qui inclut les produits IBM Tivoli Monitoring et IBM Cloud Application Performance Management, vous pouvez installer la Passerelle hybride d'IBM Cloud Application

Performance Management afin d'offrir une vue consolidée des systèmes gérés provenant des deux domaines. Pour afficher votre environnement hybride dans la console Cloud APM, vous devez créer un groupe de systèmes gérés, installer la Passerelle hybride dans votre environnement Tivoli Monitoring et configurer les communications avec la Passerelle hybride.

Pour plus d'informations, voir «Intégration à IBM Tivoli Monitoring V6.3 », à la page 975.

Mesures historiques

Visualisez jusqu'à 24 heures de données historiques sur les Tableau de bord d'Application Performance. Si une barre de sélection de durée s'affiche dans l'onglet **Présentation des statuts** d'un tableau de bord, vous pouvez ajuster la période des graphiques et les tableaux dont les valeurs sont dérivées des échantillons de données historiques. Pour les graphiques à courbes, vous pouvez également comparer les données actuelles, jusqu'aux dernières 24 heures, avec jusqu'à 8 jours de données historiques pour déceler les anomalies.

Pour plus d'informations, voir «Ajustement et comparaison de mesures dans le temps», à la page 1121.

Vue universelle d'IBM Cloud Application Business Insights

Vous pouvez utiliser la Vue universelle pour créer des pages personnalisées pour les applications que vous surveillez. Vous avez le choix entre plusieurs options de graphique et de mesure pour créer des widgets permettant de surveiller les données en fonction de vos besoins. Avec la Vue universelle, vous pouvez personnaliser un tableau de bord pour afficher les données consolidées de plusieurs agents.

Lorsque vous affichez les données dans le tableau de bord, vous pouvez modifier dynamiquement le type du graphique. Dans le widget de grille, vous pouvez filtrer les données de manière dynamique.

Vous pouvez exporter les données de pages personnalisées dans un fichier de données brutes.

Pour plus d'informations, voir «Vues personnalisées», à la page 1144.

Détails d'application

Lorsque vous accédez à un tableau de bord détaillé d'une instance de système géré à partir du tableau de bord **Toutes mes applications**, l'onglet Détails d'attribut s'affiche pour vous permettre de créer et de gérer des graphiques à courbes d'historique et des tableaux personnalisés pouvant être sauvegardés. Vous pouvez sauvegarder des pages de graphiques ou de tableaux supplémentaires pour affichage uniquement ou à des fins de partage avec tous les utilisateurs du même environnement.

Pour plus d'informations, voir «Création d'une page de graphiques ou de tableaux personnalisés», à la page 1123.

API

Les API Cloud APM sont disponibles pour gérer votre environnement, par exemple pour affecter des rôles d'utilisateurs et créer des seuils. Pour plus d'informations, voir «Exploration des API», à la page 1103.

Contrôle d'accès basé sur les rôles

Dans Cloud APM, un rôle est un groupe de droits d'accès qui contrôlent les actions que vous pouvez effectuer. La fonction Contrôle d'accès basé sur les rôles permet de créer des rôles personnalisés. Les quatre rôles prédéfinis suivants sont disponibles : Administrateur de rôles, Administrateur de surveillance, Administrateur système et Utilisateur de surveillance. Vous pouvez affecter aux utilisateurs à la fois des rôles personnalisés et des rôles prédéfinis et les utilisateurs peuvent être affectés à plusieurs rôles. Vous pouvez affecter des droits à des rôles personnalisés ou davantage de droits aux rôles par défaut existants. Les droits d'accès sont cumulatifs. Un utilisateur dispose de tous les droits de tous les rôles auxquels ils sont affectés.

Vous pouvez affecter des droits d'affichage et de modification à des applications individuelles, des groupes de ressources système et des groupes de ressources personnalisées. Par exemple, si vous êtes membre d'un rôle doté du droit d'affichage pour une application, vous pouvez afficher tous les composants de prise en charge dans cette application.

Vous pouvez affecter des droits d'affichage et de modification à des tâches d'administration de système. Par exemple, si vous êtes membre d'un rôle doté du droit d'affichage de la configuration avancée, vous pouvez effectuer et sauvegarder des modifications dans la fenêtre **Configuration avancée**.

Pour plus d'informations, voir «Rôles et droits», à la page 1031.

Génération de rapports d'historique
Les rapports sont disponibles pour les données collectées par l'Agent WebSphere Applications, l'Agent de surveillance des temps de réponse et l'Agent Synthetic Playback. Le suivi des transactions est obligatoire pour les rapports de l'Agent de surveillance des temps de réponse (non disponible avec Cloud APM, Base) Pour des descriptions de rapport, voir «Rapports», à la page 1156.

Agent Builder
Créez des agents personnalisés pour surveiller vos différentes plateformes ou technologies. Voir https://www.ibm.com/support/knowledgecenter/SSMKFH/com.ibm.apmaas.doc/install/agent_builder_guide.htm .

Surveillance des ressources de base de données
La couverture varie selon l'offre. Voir «Fonctions», à la page 55 pour afficher les noms des bases de données pouvant être surveillées.

Surveillance des ressources d'infrastructure
Utilisez les agents de surveillance des ressources pour surveiller les hyperviseurs, le stockage et les réseaux. La couverture varie selon l'offre. Voir «Fonctions», à la page 55 .

Surveillance des ressources d'applications commerciales
Utilisez les agents de surveillance des ressources pour surveiller les applications métier et collaboratives. La couverture varie selon l'offre. Voir «Fonctions», à la page 55 .

Surveillance des temps de réponse et de l'expérience de l'utilisateur
Identifiez les acquis de vos utilisateurs suite à l'utilisation de votre infrastructure sur leur périphérique. Utilisez la surveillance des temps de réponse pour surveiller les performances et la disponibilité des sites et applications Web à partir du navigateur via la base de données, et pour surveiller des périphériques mobiles. Une fois que vous avez installé l'Agent de surveillance des temps de réponse sur les serveurs à surveiller, les données collectées par ces agents sont affichées dans le Tableau de bord d'Application Performance (aucune configuration n'est requise ou la configuration requise est limitée). Les données collectées par l'Agent de surveillance des temps de réponse sont utilisées pour les tableaux de bord **Transactions utilisateur final**. Dans Cloud APM, Advanced, vous pouvez mesurer le temps de réponse du navigateur, et les données de l'Agent de surveillance des temps de réponse sont également utilisées dans la **topologie de transaction d'agrégat**. Pour plus d'informations, voir «Scénario : Surveillance de la Liste d'applications Java IBM », à la page 91.

Suivi des transactions
Cette fonction est disponible avec Cloud APM, Advanced. La fonction de suivi des transactions active les vues de topologie et la surveillance des transactions au niveau de l'instance. Elle est installée en tant qu'élément du serveur Cloud APM. Le suivi des transactions est automatiquement activé pour certains agents mais doit être manuellement activé pour d'autres. Le Tableau 4, à la page 75 fournit des informations complémentaires sur les agents qui prennent en charge le suivi des transactions.

Tableau 4. Activation du suivi des transactions pour les agents et les collecteurs de données

Déploiement d'agents ou collecteur de données	Activé par défaut	Méthode d'activation
agent DataPower	✓	«Configuration du suivi des transactions pour l'agent DataPower», à la page 249
agent IBM Integration Bus	–	«Configuration du suivi des transactions pour l'agent IBM Integration Bus», à la page 296 **Remarque :** TT n'est pas pris en charge si vous déployez cet agent sous Solaris X86.

Tableau 4. Activation du suivi des transactions pour les agents et les collecteurs de données (suite)

Déploiement d'agents ou collecteur de données	Activé par défaut	Méthode d'activation
collecteur de données J2SE	✓	«Configuration de la surveillance de J2SE», à la page 461
agent JBoss	—	«Configuration du collecteur de données de suivi des transactions de l'agent agent JBoss», à la page 478
collecteur de données Liberty	✓	«Configuration du collecteur de données Liberty pour les applications sur site», à la page 906«Configuration du collecteur de données Liberty pour les applications IBM Cloud», à la page 910
agent Microsoft .NET	—	«Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 538
collecteur de données Node.js	—	«Personnalisation du collecteur de données Node.js autonome pour les applications IBM Cloud», à la page 610 «Personnalisation du collecteur de données Node.js pour les applications sur site», à la page 616
Agent de surveillance des temps de réponse + agent HTTP Server	—	«Planification de l'installation », à la page 706
Agent SAP NetWeaver Java Stack	—	«Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 791
Agent Tomcat	—	«Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 829
Agent WebLogic	—	«Configuration de la surveillance de WebLogic», à la page 840
Agent WebSphere Applications	—	«Configuration du collecteur de données en mode interactif», à la page 864 **Remarque :** TT n'est pas pris en charge si vous déployez cet agent sous Solaris X86.
agent WebSphere MQ	—	«Configuration du suivi des transactions pour l'agent WebSphere MQ», à la page 966 **Remarque :** TT n'est pas pris en charge si vous déployez cet agent sous Solaris X86.

Les données sont affichées dans les vues **Agréger une topologie de transaction** et **Topologie des instances de transaction** pour tous les agents prenant en charge le suivi des transactions.

Topologie d'application
Voyez comment tous les composants sont connectés dans votre environnement d'application. Pour plus d'informations, voir «Application - Tableau de bord d'Application Performance», à la page 1112.

Topologie des instances de transaction
Visualisez le chemin suivi par chaque instance d'une transaction au sein de votre environnement. Pour plus d'informations, voir «Topologie des instances de transaction », à la page 97.

Availability Monitoring

IBM Cloud Availability Monitoring offre une surveillance synthétique améliorée de vos applications Web à partir de plusieurs points de présence dans le monde. Créez des tests synthétiques qui imitent le comportement utilisateur à des intervalles réguliers. Exécutez vos tests à partir de points de présence publics, ou téléchargez et déployez vos propres points de présence sur des serveurs locaux ou privés. Utilisez le tableau de bord Availability Monitoring pour surveiller la disponibilité, les performances et les alertes des applications à l'aide de graphiques, de tables de répartition et de vues de carte. Utilisez l'analyse en cascade pour identifier les problèmes de performance et de disponibilité et savoir pour quelles raisons ils surviennent.

Pour plus d'informations sur l'utilisation des tests synthétiques, voir «Availability Monitoring», à la page 1076.

Diagnostics approfondis

Pour des agents spécifiques, vous pouvez explorer en aval les tableaux de bord récapitulatifs et les tableaux de bord de diagnostics approfondis de façon à afficher les informations relatives aux demandes individuelles. Explorez en aval les tableaux de bord récapitulatifs pour afficher les détails relatifs aux niveau de code, traces de pile et requêtes SQL. Utilisez les tableaux de bord de diagnostic pour identifier les demandes qui présentent des problèmes et déboguer les transactions problématiques. Vous pouvez également détecter, diagnostiquer ou arrêter les transactions lentes ou bloquées toujours en cours (voir Agent WebSphere Applications Reference). Le Tableau 5, à la page 77 fournit des informations complémentaires sur les agents de diagnostic.

Tableau 5. Tableaux de bord de diagnostic des agents et collecteurs de données

Agent ou collecteur de données	**Données de diagnostic configurées par défaut**	**Tableaux de bord de diagnostic disponibles**	**Comment accéder aux tableaux de bord de diagnostic**	**Comment configurer l'agent ou le collecteur de données pour la collecte des données de diagnostic**
collecteur de données J2SE	✓	Détail, Modules Web, Instances de demande, Récapitulatif des demandes et Traces des demandes	Cliquez sur **Diagnostiquer** dans le tableau de bord **Présentation** ou le tableau de bord **Modules Web**.	«Configuration de la surveillance de J2SE», à la page 461
agent JBoss	–	Tableau de bord de diagnostic, Récapitulatif des demandes en cours, tableau de bord Trace de pile des demandes en cours, Récupération de place par la machine virtuelle Java, Cliché de tas et Comparaison de cliché de tas	Cliquez sur **Diagnostiquer**, **Demandes Inflight**, **Détails** ou **Cliché de tas** dans le tableau de bord **Présentation**.	«Configuration du collecteur de données de suivi des transactions de l'agent agent JBoss», à la page 478

Tableau 5. Tableaux de bord de diagnostic des agents et collecteurs de données (suite)

Agent ou collecteur de données	Données de diagnostic configurées par défaut	Tableaux de bord de diagnostic disponibles	Comment accéder aux tableaux de bord de diagnostic	Comment configurer l'agent ou le collecteur de données pour la collecte des données de diagnostic
collecteur de données Liberty	✓	Détail, Cliché de tas, Comparaison de cliché de tas et Analyse de la mémoire	Cliquez sur **Diagnostiquer**, **Afficher le cliché de tas** ou **Afficher l'analyse de la mémoire** dans le tableau de bord **Présentation**.	• «Configuration du collecteur de données Liberty pour les applications IBM Cloud», à la page 910 • «Configuration du collecteur de données Liberty pour les applications sur site», à la page 906
agent Microsoft .NET	—	Instances de demande, Récapitulatif des demandes et Traces des demandes	Cliquez sur **Diagnostiquer** dans le tableau de bord **Présentation**.	«Activation de la collecte des données de diagnostic à l'aide de la commande configdc», à la page 539
Agent Node.js	✓	Détails de la récupération de place, Instances de demande, Récapitulatif des demandes et Traces des demandes	Cliquez sur **Diagnostiquer** dans le tableau de bord **Présentation**.	«Configuration de l'Agent Node.js», à la page 602
collecteur de données Node.js	✓	Détails de la récupération de place, Détails des demandes les plus lentes, Instances de demande et Traces des demandes	Cliquez sur **Diagnostiquer** ou **Détails de la récupération de place** dans le tableau de bord Présentation.	• «Configuration du collecteur de données Node.js autonome pour les applications IBM Cloud(anciennement Bluemix)», à la page 608 • «Configuration du collecteur de données Node.js autonome pour les applications sur site», à la page 615

Tableau 5. Tableaux de bord de diagnostic des agents et collecteurs de données (suite)

Agent ou collecteur de données	Données de diagnostic configurées par défaut	Tableaux de bord de diagnostic disponibles	Comment accéder aux tableaux de bord de diagnostic	Comment configurer l'agent ou le collecteur de données pour la collecte des données de diagnostic
collecteur de données Python	✓	Détails des demandes les plus lentes, Détails des traces de demandes, Détails des unités d'exécution Python, Récupération de place Python et Détails des segments de mémoire Python	Cliquez sur **Diagnostiquer**, **Détail des unités d'exécution**, ou **Détails de la mémoire** dans le tableau de bord **Présentation**.	• «Configuration du collecteur de données Python pour les applications IBM Cloud», à la page 689 • «Configuration du collecteur de données Python pour les applications sur site», à la page 695
Agent Ruby	–	Détail récapitulatif des demandes, Exemple d'instances de demande, Traces des demandes	Cliquez sur **Diagnostiquer** dans le tableau de bord **Présentation**.	«Configuration de la surveillance de Ruby», à la page 737
collecteur de données Ruby	✓	Instances de demande, Récapitulatif des demandes et Traces des demandes	Cliquez sur **Diagnostiquer** dans le tableau de bord **Présentation**.	«Configuration du collecteur de données Ruby pour les applications IBM Cloud», à la page 745
Agent SAP NetWeaver Java Stack	✓	Instances de demande, Récapitulatif des demandes et Traces des demandes	Cliquez sur **Diagnostiquer** dans le tableau de bord **Présentation**.	«Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 791
Agent Tomcat	–	Instances de demande, Récapitulatif des demandes et Traces des demandes	Cliquez sur **Diagnostiquer** dans le tableau de bord **Présentation**.	«Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 829

Tableau 5. Tableaux de bord de diagnostic des agents et collecteurs de données (suite)

Agent ou collecteur de données	Données de diagnostic configurées par défaut	Tableaux de bord de diagnostic disponibles	Comment accéder aux tableaux de bord de diagnostic	Comment configurer l'agent ou le collecteur de données pour la collecte des données de diagnostic
Agent WebLogic	—	Tableau de bord de diagnostic, Récapitulatif des demandes en cours, tableau de bord Trace de pile des demandes en cours, JVM GC Detail, Cliché de tas et Comparaison de cliché de tas	Cliquez sur **Diagnostiquer**, **View Requests**, **Détails** ou **Cliché de tas** dans le tableau de bord **Présentation**.	«Configuration de la surveillance de WebLogic», à la page 840
Agent WebSphere Applications	—	Diagnostics, Instances de demande, Séquence des demandes, Récapitulatif des demandes en cours, Trace de pile des demandes en cours, Cliché de tas, Comparaison de cliché de tas et Analyse de la mémoire	Cliquez sur **Diagnostiquer**, **View Requests**, **View Heap Dump**, ou **View Memory Analysis** dans le tableau de bord **Présentation**. Le bouton **View Memory Analysis** fonctionne uniquement lorsque la surveillance des fuites de mémoire a été activée.	• «Configuration du collecteur de données avec l'utilitaire de configuration simple», à la page 861 • «Activation de la surveillance des fuites de mémoire», à la page 902

Le bouton **Diagnostiquer** est activé uniquement si le diagnostic approfondi est configuré pour votre agent et que vous êtes membre du rôle Administrateur de rôles, Administrateur de surveillance, ou de tout autre rôle personnalisé disposant de droits sur la vue des tableaux de bord de diagnostic.

Seuils

Les seuils vous permettent de détecter des comportements d'application spécifiques et des conditions en fonction de définitions activement surveillées. Des seuils prédéfinis sont disponibles pour chaque agent et vous pouvez définir de nouveaux seuils pour la surveillance. Pour plus d'informations, voir «Gestionnaire de seuils», à la page 1014.

Lorsque la transmission d'événements est configurée, les événements sont envoyés au récepteur EIF. Vous pouvez utiliser le mappage par défaut entre les seuils et les événements transmis au serveur d'événements ou personnaliser la manière dont les seuils sont mappés. Pour plus d'informations, voir «Personnalisation d'un événement à transmettre à un récepteur EIF», à la page 1019.

Dans le **Tableau de bord d'Application Performance**, une fois que vous avez sélectionné une application, l'onglet **Événements** s'affiche. L'onglet **Événements** indique les événements ouverts pour l'application en cours. Vous pouvez accéder à des tableaux de bord détaillés contenant des mesures de performance pour vous aider à déterminer la cause de l'événement. Pour plus d'informations, voir «Statut de l'événement», à la page 1140.

Groupes de ressources

Les systèmes gérés de votre entreprise surveillée peuvent être classés en fonction de leur objet. Ces systèmes gérés possèdent souvent les mêmes exigences de seuil. Utilisez le Gestionnaire de groupes de ressources pour organiser les systèmes surveillés en groupes auxquels vous pouvez affecter des

seuils de génération d'événement. Pour plus d'informations, voir «Gestionnaire de groupes de ressources», à la page 1008.

Page Mise en route

Une fois que vous êtes connecté à la console Cloud APM, la page Mise en route s'affiche. Cliquez sur l'une des **Tâches utilisateur** ou des **Tâches administrateur** pour accéder à une présentation ou une vidéo par scénario. Les liens "Démarrer maintenant" vous permettent d'accéder directement à la fonctionnalité, telle que Gestionnaire de seuils. Les liens **Ressources communautaires** permettent d'accéder à la **Foire aux questions**, au forum Cloud APM et bien plus encore.

Des fonctionnalités supplémentaires sont disponibles par le biais de l'intégration avec d'autres produits et composants. Pour plus d'informations, voir «Intégration », à la page 81 et Chapitre 8, «Intégration à d'autres produits et composants», à la page 975.

Intégration

Des fonctions supplémentaires sont disponibles via l'intégration à d'autres produits et composants : Tivoli Monitoring, OMEGAMON, Netcool/OMNIbus, Operations Analytics - Log Analysis, Operations Analytics - Predictive Insights, Alert Notification, Control Desk, IBM Cloud et Agent Builder.

IBM Tivoli Monitoring

La coexistence des agents est prise en charge. Vous pouvez installer les agents IBM Cloud Application Performance Management sur le même ordinateur que les agents IBM Tivoli Monitoring. Cependant, les deux types d'agent ne peuvent pas être installés dans le même répertoire.Pour plus d'informations, voir «Coexistence de l'agent Cloud APM et de l'agent Tivoli Monitoring», à la page 976.

Si votre environnement dispose à la fois des produits IBM Tivoli Monitoring et Cloud APM (cloud et/ou sur site), vous pouvez installer la Passerelle hybride d'IBM Cloud Application Performance Management afin d'offrir une vue consolidée des systèmes gérés des deux environnements. Pour plus d'informations, voir «Passerelle hybride», à la page 979. Pour obtenir la liste actuelle des agents Tivoli Monitoring pris en charge, visitez le Hybrid Gateway supported agents (APM Developer Center).

IBM OMEGAMON

z Systems Extension Pack connecte un ou plusieurs agents OMEGAMON qui s'exécutent sur votre mainframez Systems à Cloud APM. En utilisant z Systems Extension Pack et la Passerelle hybride pour connecter vos agents OMEGAMON déployés à Cloud APM, vous pouvez visualiser les données de surveillance et les événements associés à vos composants d'application OMEGAMON dans la console Cloud APM.

Pour plus d'informations, voir «Intégration à OMEGAMON», à la page 991.

IBM Netcool/OMNIbus

Vous pouvez réacheminer vos événements de Cloud APM vers votre gestionnaire d'événements Netcool/OMNIbus sur site. Pour plus d'informations, voir «Intégration à Netcool/OMNIbus», à la page 992.

IBM Operations Analytics - Log Analysis

Si votre environnement inclut IBM Operations Analytics - Log Analysis, vous pouvez regrouper les données des journaux d'application et les données de performances pour faciliter la recherche de la cause première des problèmes rencontrés par vos applications. Vous pouvez effectuer des recherches dans les données du journal associées à vos applications pour identifier la cause d'un problème, comme la lenteur ou un échec. Pour plus d'informations, voir «Intégration à Operations Analytics - Log Analysis», à la page 996.

IBM Operations Analytics - Predictive Insights

Operations Analytics - Predictive Insights analyse les données et apprend le comportement normal d'un système. Il crée un modèle de performance et l'utilise pour détecter ou prévoir le comportement en dehors de la plage modélisée et génère des alarmes en cas de comportement anormal. Vous pouvez ajouter Operations Analytics - Predictive Insights à votre abonnement Cloud APM. Vous pouvez ensuite afficher les anomalies dans le Tableau de bord d'Application Performance et explorer l'interface utilisateur Operations Analytics - Predictive Insights pour plus de détails. Pour plus d'informations, voir «Intégration à Operations Analytics - Predictive Insights», à la page 997.

IBM Cloud
Vous pouvez afficher les informations de surveillance relatives à vos applications dans l'environnement IBM Cloud à l'aide des collecteurs de données autonomes. Les collecteurs de données permettent l'intégration des fonctionnalités de surveillance à IBM Cloud en transférant les données de surveillance et de diagnostic approfondi des ressources relatives à vos applications IBM Cloud au serveur Cloud APM. Le serveur Cloud APM reçoit et traite les informations de surveillance qui sont collectées par les collecteurs de données. Les types d'applications IBM Cloud suivants peuvent être surveillés :

- Applications Liberty
- Applications Node.js
- Applications Python
- Applications Ruby

Une fois que vous avez configuré un collecteur de données, vous pouvez afficher les données de surveillance sur la console Cloud APM. Pour plus d'informations, voir «Procédure générale de configuration des collecteurs de données», à la page 189.

IBM Alert Notification
Si vous utilisez IBM Cloud Application Performance Management, IBM Alert Notification est automatiquement intégré pour vous. Alert Notification est un système de notification simple et facile d'utilisation qui donne aux informaticiens une notification instantanée des alertes relatives aux problèmes de votre environnement informatique. Les données transmises par les agents fournissent la source des alertes. Une fois que vous avez activé Alert Notification, connectez-le à une instance Cloud APM. En package autonome, vous pouvez intégrer Alert Notification à tout outil de surveillance sur site qui peut implémenter et démarrer une API REST. Les outils pris en charge incluent IBM Tivoli Netcool/OMNIbus. Pour plus d'informations, voir Intégration à Alert Notification.

IBM Control Desk
Pour bénéficier de l'intégration avec IBM Control Desk, soumettez un ticket de demande de service au Support IBM. Vous pouvez configurer les événements Cloud APM pour que des tickets soient ouverts automatiquement dans IBM Control Desk. Pour cela, accédez au Support IBM et sélectionnez **Subscription**. Pour plus d'informations sur les éléments à fournir au support pour l'autoriser à configurer cette intégration, voir «Intégration à Control Desk», à la page 999.

IBM Agent Builder
Vous pouvez utiliser Agent Builder afin de générer des agents personnalisés pour n'importe quelle technologie. Pour plus d'informations, voir https://www.ibm.com/support/knowledgecenter/SSMKFH/com.ibm.apmaas.doc/install/agent_builder_guide.htm.

Documentation

Vous pouvez trouver des informations sur IBM Cloud Application Performance Management dans l'IBM Knowledge Center, dans la console Cloud APM et dans l'Application Performance Management Developer Center.

IBM Knowledge Center
Cloud APM dans l'IBM Knowledge Center représente la source officiel d'informations techniques pour le produit.

Aide de l'interface utilisateur
Lorsque vous êtes connecté à la console Cloud APM ou explorez la Démonstration guidée, vous pouvez accéder au système d'aide :

- Cliquez sur **Contenu de l'aide** dans la barre de navigation. Menu Aide.
- Cliquez sur dans la bannière du tableau d'Application Performance.
- Cliquez sur le lien **En savoir plus** dans les pages de configuration système.
- Cliquez sur dans un widget de tableau de bord.

IBM Application Performance Management Developer Center
Application Performance Management Developer Center est un emplacement central pour un grand choix de contenu APM applicable à un large éventail d'utilisateurs d'APM. Le contenu inclut la documentation, les blogues, les vidéos, et les liens vers des ressources additionnelles.

Forum IBM Cloud Application Performance Management et dwAnswers
Le forum Cloud Application Performance Management et dwAnswers contiennent des discussions techniques sur les problèmes relatifs au produit, y compris sur l'identification des incidents et leur résolution.

Des informations sont également disponibles sur les sites Web suivants :

Outil SPCR (Software Product Compatibility Reports)
Vous pouvez utiliser l'outil SPCR pour générer différents types de rapport liés aux offres et aux exigences de composant. Recherchez l'un des noms d'offre Cloud Application Performance Management ou IBM Cloud Application Performance Management - Agents.

IBM Marketplace
Des ressources telles que des démonstrations vidéo et des Foires aux questions sont disponibles dans IBM Marketplace.

IBM Explorateur d'API
Pour obtenir la documentation des API Cloud APM, voir «Exploration des API», à la page 1103.

Terminologie IBM
Le site Web IBM Terminology contient la terminologie relative aux produits IBM accessible depuis dans un emplacement unique.

IBM Redbooks
Les sites Web IBM Redbooks contiennent des publications Redbooks, des Redpapers et des notes techniques de Redbooks qui fournissent des informations sur les produits regroupées par plateformes et solutions.

Conventions utilisées dans la documentation

Plusieurs conventions sont utilisées dans cette documentation pour les termes spéciaux, actions, commandes et chemins en fonction de votre système d'exploitation et pour les informations spécifiques à la plateforme et au produit.

Conventions typographiques

Les conventions typographiques suivantes sont utilisées dans cette documentation :

Gras

- Commandes en minuscules, commandes en casse mixte, paramètres et variables d'environnement difficiles à distinguer du texte qui les entoure
- Contrôles d'interface (cases à cocher, boutons de commande, boutons d'option, toupies, zones, dossiers, icônes, zones de liste, éléments de zones de liste, listes à plusieurs colonnes, conteneurs, choix de menu, noms de menu, onglets, feuilles de propriétés), étiquettes (telles que **Astuce :**)
- Mots clés et paramètres figurant dans le texte

Italique

- Citations (par exemple, titres de publications, de disquettes et de CD)
- Mots et phrases définis dans le texte (exemple : une ligne spécialisée est appelée *ligne point-à-point*)
- Mise en évidence de mots et lettres (exemple : L'adresse du numéro d'unité logique (LUN) doit commencer par la lettre *L*.)
- Nouveaux termes dans le texte, sauf dans la liste des définitions (exemple : une *vue* est un cadre dans un espace de travail contenant des données.)
- Variables et valeurs à fournir (exemple : où *mon_nom* représente...)

`Espace fixe`

- Exemples et exemples de code.
- Noms de fichier, noms de répertoire, chemins, mots clé de programmation, propriétés et autres éléments difficiles à distinguer du texte qui les entoure
- Texte des messages et invites
- Texte que l'utilisateur doit saisir
- Valeurs d'arguments ou d'options de commande

`Espace fixe, gras`

- Noms de commandes et noms de macros et d'utilitaires pouvant être saisis comme des commandes
- Noms de variable d'environnement dans le texte
- Mots clé
- Noms de paramètres dans le texte : paramètres de structure d'API, paramètres et arguments de commande et paramètres de configuration
- Noms de processus
- Noms de variables du registre dans le texte
- Noms de scripts

Variables et chemins d'accès dépendants du système d'exploitation

Le sens de la barre oblique pour les chemins d'accès aux répertoires peut varier dans la documentation. Quel que soit le sens utilisé dans la documentation, observez les recommandations suivantes :

- Linux AIX Utilisez une barre oblique (**/**).
- Windows Utilisez une barre oblique inversée (****).

Les noms des variables d'environnement ne sont pas toujours identiques sous Windows et AIX. Par exemple, %TEMP% sous Windows correspond à $TMPDIR sous AIX ou Linux.

Pour les variables d'environnement, observez les recommandations suivantes :

- Linux AIX Utilisez **$***variable*.
- Windows Utilisez **%***variable***%**.

Windows Si vous utilisez l'interpréteur de commandes bash sur un système Windows, vous pouvez utiliser les conventions AIX.

Variable et chemins du répertoire d'installation des agents

rép_install correspond au répertoire d'installation des agents. L'emplacement par défaut dépend du système d'exploitation :

- Windows `C:\IBM\APM`
- Linux `/opt/ibm/apm/agent`
- AIX `/opt/ibm/apm/agent`

Chapitre 4. Planification du déploiement

Pour garantir la réussite du déploiement d'IBM Cloud Application Performance Management, il est indispensable d'effectuer une planification.

Configuration requise

Pour les agents et les collecteurs de données IBM Cloud Application Performance Management, divers systèmes d'exploitation sont pris en charge et chacun de ces composants a des exigences spécifiques.

Fuseau horaire

Utilisez NTP (Network Time Protocol) sur les systèmes gérés afin de garantir que l'heure en vigueur sur le système est correcte. Le réglage de l'heure pour correspondre à l'emplacement physique des serveurs (comme UTC-03:00 pour le Brésil et UTC+06:30 pour Yangon) contribue à assurer un horodatage précis des événements et des transactions. Les agents signalent les données dans l'interface utilisateur APM à l'heure locale de l'utilisateur.

Exigences des agents et collecteurs de données Cloud APM
Procurez-vous des informations sur les exigences de chaque agent de surveillance et collecteur de données autonome que vous prévoyez d'installer.

L'agent et le collecteur de données Cloud APM sont en général transparents vis-à-vis de l'hyperviseur, ce qui signifie qu'ils peuvent être installés et déployés sur n'importe quel système d'exploitation pris en charge, quels que soient les hyperviseurs sur lesquels les systèmes d'exploitation sont hébergés, tels que Hyper-V, IBM PowerVM, KVM, VMWare ESX, etc.

Pour les exigences des agents et des collecteurs de données, utilisez les liens de la section relative aux rapports sur les composants de la rubrique System requirements (APM Developer Center).

Pour obtenir des informations à jour sur les navigateurs pris en charge, reportez-vous au rapport détaillé sur la configuration système requise par IBM Cloud Application Performance Management.

Vous pouvez également rechercher IBM Cloud Application Performance Management dans l'outil Software Product Compatibility Reports.

Le système informatique local sur lequel l'agent est installé doit prendre en charge le codage UTF-8 si l'agent envoie des données internationalisées au serveur Cloud APM.

Ports par défaut utilisés par les agents et collecteurs de données

Divers ports sont utilisés pour les communications entre le composant Cloud APM et l'application ou le système (local ou distant) surveillé. Dans la plupart des cas, des ports par défaut sont fournis pour faciliter la configuration. La plupart des valeurs par défaut peuvent être personnalisées à l'aide des paramètres de configuration.

Le Tableau 6, à la page 86 répertorie les ports par défaut utilisés par les agents et les collecteurs de données Cloud APM pour communiquer avec les applications ou les systèmes qu'ils surveillent. La mention N/A dans le tableau indique l'un des cas suivants :

- L'agent ou le collecteur de données n'utilise pas de port pour communiquer avec l'application ou le système surveillé.
- Le port utilisé pour les communications est déterminé par la configuration de l'application surveillée.
- Les ports utilisés par l'agent ou le collecteur de données sont affectés de manière dynamique et aucune valeur par défaut statique n'est fournie.
- Tous les ports à utiliser doivent être spécifiés par l'utilisateur et aucune valeur par défaut n'est fournie.

Tableau 6. Ports par défaut utilisés par les agents et collecteurs de données

Agents et collecteurs de données	Ports par défaut	Configurable	Local	Distant
agent Amazon EC2	• Port TCP 80 (pour HTTP) • Port TCP 443 (pour HTTPS)	N/A	Oui	Non
agent Amazon ELB	• Port TCP 80 (pour HTTP) • Port TCP 443 (pour HTTPS)	N/A	Non	Non
Agent Azure Compute	• Port TCP 80 (pour HTTP) • Port TCP 443 (pour HTTPS)	Non	Non	Non
agent Cassandra	7199 (pour le JMX, local et distant)	Oui	Oui	Oui
agent Cisco UCS	• Port TCP 80 (pour HTTP) • Port TCP 443 (pour HTTPS)	Non	Oui	Non
agent Citrix VDI	Pour les appels PowerShell : • 5985 (pour HTTP) • 5986 (pour HTTPS)	Oui	Oui	Oui
agent Db2	• 50000 (port par défaut du serveur Db2) • Surveillance à distance prise en charge : utilise le numéro de port fourni par l'utilisateur lors du catalogage de l'instance de serveur distant.	Oui	Oui	Oui
agent DataPower	5550 (pour la connexion au dispositif DataPower distant)	Oui	Non	Oui
agent Hadoop	• Surveillance locale : valeur de la variable d'environnement **CP_PORT** • Surveillance à distance : – 50070 (Namenode de secours) – 50090 (Namenode secondaire) – 8088 (Gestionnaire de ressources) – 19888 (JobHistory Server) – 8080 (Ambari)	Oui	Oui	Oui
agent HMC Base	12443 (pour télécharger le SDK à partir de la console HMC)	Non	Oui	Non
agent HTTP Server	Il se peut que l'agent HTTP soit configuré sur un port différent, mais l'agent lui-même ne possède pas de port par défaut.	N/A	Oui	Non
agent IBM Cloud	Connexion sortante à api.softlayer.com port 443.	N/A	Non	Oui

Tableau 6. Ports par défaut utilisés par les agents et collecteurs de données (suite)

Agents et collecteurs de données	Ports par défaut	Configurable	Local	Distant
agent IBM Integration Bus	N/A	N/A	Oui	Non
Internet Service Monitoring	Pour databridge : • 9510 • 9520	Oui	Non	Oui
agent DataStage	• 9443 (port HTTPS WAS) • 50000 (port JDBC de la base de données) • 1433 (Microsoft SQL) • 1521 (Oracle)	Oui	Oui	Oui
collecteur de données J2SE	N/A	N/A	Non	Non
agent JBoss	Varie en fonction de la version du serveur JBoss : • 9990 • 9994 • 9999	Non	Oui	Non
collecteur de données Liberty	N/A	N/A	Non	Non
agent Linux KVM	• 8080 (pour HTTP) • 8443 (pour HTTPS)	Oui	Oui	Non
Linux OS	22 (pour la surveillance des journaux à distance avec SSH)	Oui	Oui	Non
Agent MariaDB	3306	Oui	Oui	Oui
agent Microsoft Active Directory	Le numéro de port dépend du réglage du programme d'écoute pour l'utilisation de la surveillance.	N/A	Oui	Oui
agent Microsoft Cluster Server	N/A	N/A	Non	Non
agent Microsoft Exchange Server	N/A	N/A	Non	Non
agent Microsoft Hyper-V Server	N/A	N/A	Non	Non
agent Microsoft IIS	N/A	N/A	Non	Non
agent Microsoft .NET	Pour envoyer les données de suivi des transactions, le port 5456 est utilisé par défaut.	Oui	Oui	Non
agent Microsoft Office 365	7799 (pour la transaction synthétique Skype)	Oui	Oui	Non
agent MicrosoftSharePoint Server	1433 (pour le serveur SQL)	Non	Oui	Oui

Tableau 6. Ports par défaut utilisés par les agents et collecteurs de données (suite)

Agents et collecteurs de données	Ports par défaut	Configurable	Local	Distant
agent Microsoft SQL Server	1433 (valeur par défaut du serveur SQL)	Oui (par **COLL_PORT**)	Oui	Non
Agent MQ Appliance	• 162 (pour la réception des événements SNMP) • 5554 (pour la connexion à MQ Appliances)	Oui	Oui	Oui
Agent MongoDB	• 27017 (pour une instance unique) • 27019 (pour le cluster)	Oui	Oui	Non
Agent MySQL	3306 (pour la connexion JDBC)	Oui	Oui	Oui
agent NetApp Storage	Pour la surveillance à distance : • 8088 • 8488 • 443 • 8443	Non	Non	Oui
Agent Node.js	63336	Oui	Oui	Non
collecteur de données Node.js	N/A	N/A	Non	Non
Agent OpenStack	5000 (pour se connecter au service d'identité d'OpenStack)	Oui	Non	Oui
Agent Oracle Database	1521 (pour la connexion SQL)	Oui	Oui	Non
Agent PHP	• Connexion Apache • Le numéro de port est basé sur la configuration Apache	Oui	Oui	Non
Agent PostgreSQL	5432 (pour la connexion JDBC)	Oui	Oui	Oui
collecteur de données Python	N/A	N/A	Non	Non
agent RabbitMQ	Numéro de port où le plug-in de gestion RabbitMQ est activé (local et distant) : 15672	Oui	Oui	Oui
Agent de surveillance des temps de réponse	• Le modèle d'analyseur de package surveille les transactions HTTP sur le port 80. • Le modèle de serveur HTTP surveille tous les ports.	Oui	Oui	Non
Agent Ruby	Généré de manière dynamique	N/A	Oui	Non
collecteur de données Ruby	N/A	N/A	Non	Non
Agent SAP	33*nn* (*nn* représentant le numéro d'instance SAP)	Non	Oui	Non

Tableau 6. Ports par défaut utilisés par les agents et collecteurs de données (suite)

Agents et collecteurs de données	Ports par défaut	Configurable	Local	Distant
Agent SAP HANA Database	Valeur par défaut : 30013. Plage : 30013 à 39913.	Oui	Oui	Non
Agent SAP NetWeaver Java Stack	Par défaut : 50004. Plage : 50004 à 59904.	Oui	Oui	Non
agent Siebel	N/A	N/A	Oui	Non
Agent Skype for Business Server (anciennement agent Microsoft Lync Server)	• Port par défaut du Business Server 5061 • Port 1433 du serveur SQL (local ou distant en fonction de l'environnement).	Non	Oui	Non
Agent Sterling Connect Direct	1363	Oui	Non	Oui
Agent Sterling File Gateway	50000 Le numéro de port de l'API REST IBM B2B Integrator et le numéro de port de la base de données sont tous les deux requis et configurables.	Oui	Oui	Oui
agent Sybase	5000	N/A	Oui	Non
Agent Synthetic Playback	• 4444 (pour se connecter au serveur selenium interne) • Les ports distants sont spécifiés dans l'URL http des sites Web surveillés, généralement HTTP 80 et HTTPS 443	Non	Oui	Non
Agent Tomcat	8686 (pour le serveur MBean Tomcat)	Oui (par port JMX)	Oui	Non
Agent UNIX OS	22 (pour la surveillance des journaux à distance avec SSH)	Oui	Oui	Non
Agent VMware VI	• 443 (pour la surveillance à distance) • 80 (pour la surveillance locale)	Non	Oui	Oui
Agent WebLogic	7003 (trafic HTTP JMX Management)	Oui	Oui	Non
Agent WebSphere Applications	• 63335 (pour l'agent de surveillance version 8) • 63336 (pour l'agent de surveillance version 6) • 63355 (pour la surveillance des ressources) • 5457 (pour Transaction Framework Extension)	Oui	Oui	Non

Tableau 6. Ports par défaut utilisés par les agents et collecteurs de données (suite)				
Agents et collecteurs de données	**Ports par défaut**	**Configurable**	**Local**	**Distant**
agent WebSphere Infrastructure Manager	N/A	N/A	Oui	Non
agent WebSphere MQ	Le numéro de port dépend du réglage du programme d'écoute pour l'utilisation de la surveillance.	N/A	Non	Oui
agent Windows OS	22 (pour la surveillance des journaux à distance avec SSH)	Oui	Oui	Non

Scénarios

Selon la complexité de votre environnement, vous devez installer différents agents pour surveiller différents composants. Appuyez-vous sur ces scénarios de déploiement pour comprendre quels éléments vous devez installer et où les installer afin d'obtenir les meilleurs résultats d'IBM Cloud Application Performance Management.

Scénario : Surveillance d'IBM API Connect

Vous pouvez surveiller votre environnement IBM API Connect, mais également en identifier et résoudre les problèmes, à l'aide des agents et collecteurs de données APM.

Le produit Cloud APM vous aide à gérer les performances et la disponibilité de votre environnement API Connect. A l'aide des agents et collecteurs de données Cloud APM, vous disposez d'une visibilité et d'un contrôle sur l'infrastructure API Connect et les API d'application, pour garantir des performances optimales et une utilisation efficace des ressources. Si vous rencontrez des problèmes de performance dans l'environnement API Connect, le produit Cloud APM peut vous aider à les détecter, diagnostiquer et isoler.

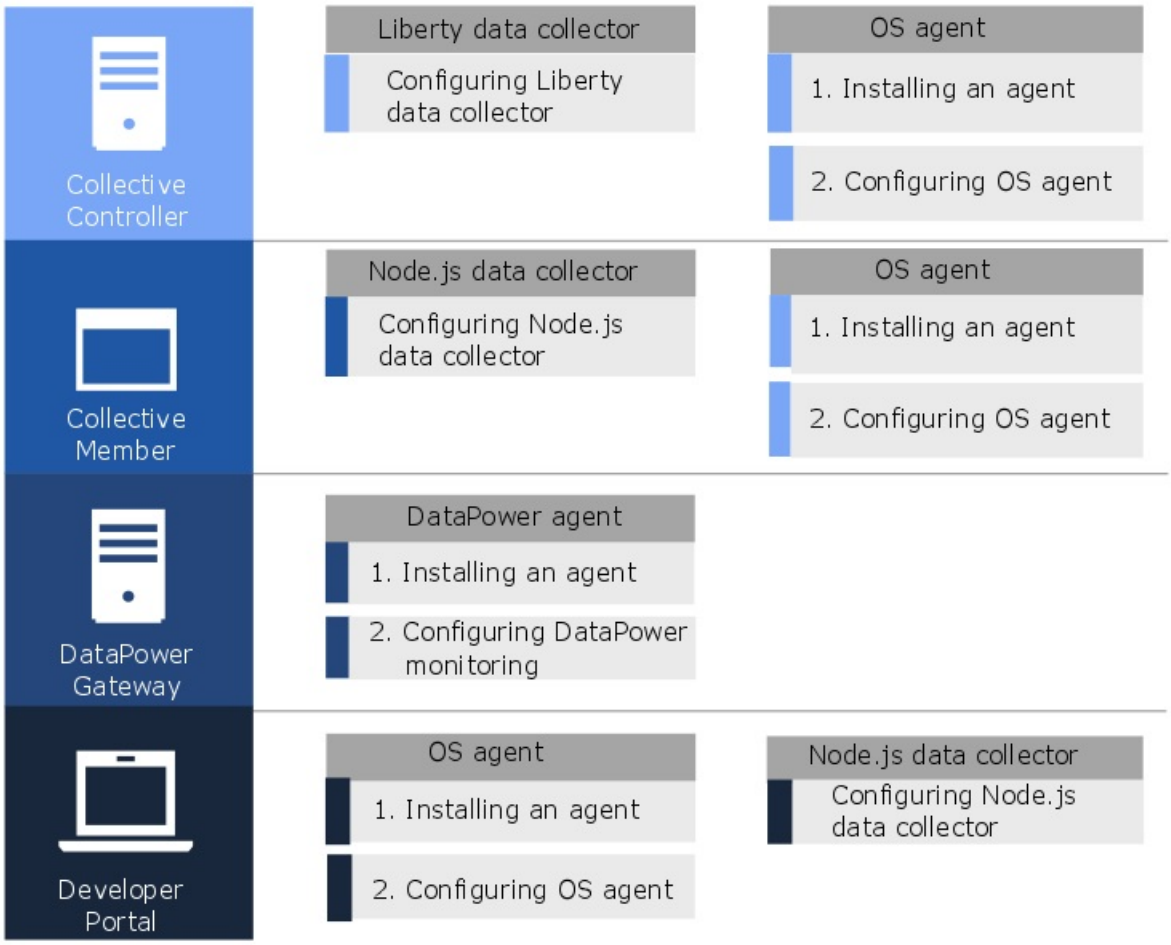
Par exemple, vous pouvez installer les agents de système d'exploitation sur tous les systèmes applicables. Ces agents permettent de collecter et d'analyser les performances du serveur, y compris les performances de l'UC, les E-S de disque et l'utilisation, la disponibilité et les performances des processus et les performances du réseau. Ils peuvent, de plus, être configurés pour surveiller les journaux clés et les journaux système d'API Connect.

Si d'autres produits middleware sont déployés, la fonction de suivi des transactions, installée comme faisant partie du serveur Cloud APM, fournit des vues de topologie permettant d'afficher les informations de suivi des transactions pour les produits middleware et les services qu'ils proposent et pour traiter les problèmes le cas échéant.

L'image ci-après illustre les composants API Connect et les agents et collecteurs de données Cloud APM correspondants qui peuvent les surveiller. Pour activer ces agents et collecteurs de données, effectuez les tâches d'installation et de configuration répertoriées sous le nom de l'agent et du collecteur de données. Cliquez sur les cases rectangulaires de l'image qui contient le nom de tâche pour accéder aux tâches d'installation ou de configuration.

Remarque :

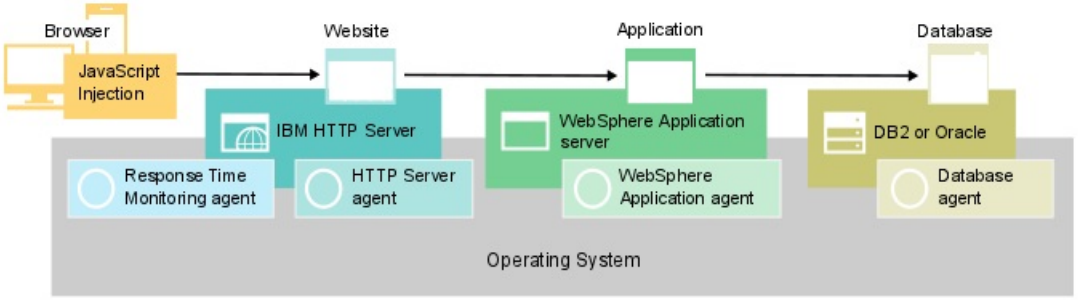
- Installez un collecteur de données Node.js sur chaque application IBM API Connect publiée dans le membre de collectivité.
- Lors de la surveillance de DataPower Gateway, l'agent DataPower s'exécute à distance à partir du dispositif DataPower.



1. «Configuration du collecteur de données Liberty pour les applications sur site», à la page 906
2. Chapitre 6, «Installation des agents», à la page 123
3. «Configuration de la surveillance du système d'exploitation», à la page 647
4. «Configuration du collecteur de données Node.js autonome pour les applications sur site», à la page 615
5. Chapitre 6, «Installation des agents», à la page 123
6. «Configuration de la surveillance du système d'exploitation», à la page 647
7. Chapitre 6, «Installation des agents», à la page 123
8. «Configuration de la surveillance DataPower», à la page 237
9. Chapitre 6, «Installation des agents», à la page 123
10. «Configuration de la surveillance du système d'exploitation», à la page 647
11. «Configuration du collecteur de données Node.js autonome pour les applications sur site», à la page 615

Scénario : Surveillance de la Liste d'applications Java IBM

Vous pouvez surveiller et traiter les incidents relatifs à la Liste d'applications Java IBM pour visualiser les informations de surveillance des transactions à partir du navigateur via la base de données, y compris la surveillance des ressources de composants individuels. La Liste d'applications Java IBM inclut IBM HTTP Server, WebSphere Application Server, et la base de données IBM Db2 ou Oracle.



Surveillance de la Liste d'applications Java IBM
Pour surveiller la Liste d'applications Java IBM, installez les agents répertoriés pour chaque composant dans l'ordre indiqué.

(Facultatif) Si vous souhaitez également surveiller le système, installez les agents de système d'exploitation sur tous les composants.

Pour le serveur Web, procédez comme suit :

1. Installez l'agent HTTP Server.

   Raccourci : Cette installation comprend l'installation du module IBM HTTP Server Response Time et configure automatiquement l'injection de JavaScript.
2. Configurez l'installation de l'agent HTTP Server..
3. Installez l'agent Response Time Monitoring.

Pour le serveur d'applications, installez l'Agent WebSphere Applications.

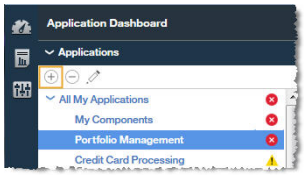
Pour la base de données, installez l'agent Oracle Database ou l'agent Db2, selon votre base de données.

Ajout d'applications Web au Tableau de bord d'Application Performance
Ajoutez les applications à surveiller au Tableau de bord d'Application Performance .

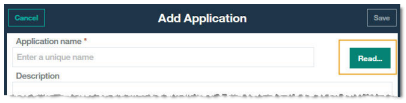
Procédure

Pour ajouter des applications Web, procédez comme suit :

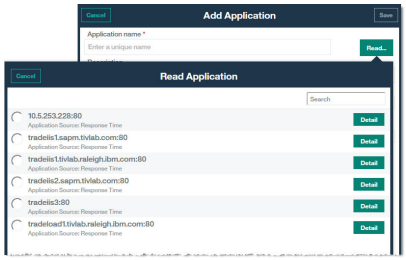
1. Dans le Tableau de bord d'Application Performance , cliquez sur **Ajouter une application**.



2. Cliquez sur **Lire** pour ouvrir la liste des applications reconnues.



3. Sélectionnez l'application Web à surveiller.



4. Cliquez sur **Sauvegarder**.

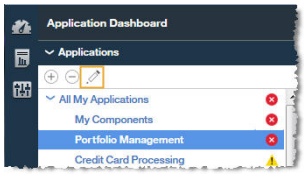
Association d'une Liste d'applications Java IBM à l'application Web

Editez l'application Web pour associer les composants WebSphere Application Server et de base de données à inclure dans la surveillance.

Procédure

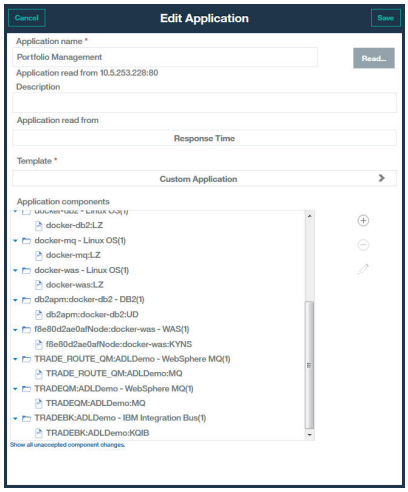
Pour afficher les composants de la Liste d'applications Java, procédez comme suit dans le Tableau de bord d'Application Performance :

1. Sélectionnez le serveur Web et cliquez sur **Modifier une application**.



2. Dans la fenêtre **Modification d'application**, cliquez sur **Ajouter des composants** +.
3. Dans la fenêtre **Sélectionner le composant**, sélectionnez WebSphere Application Server.
4. Dans l'**Editeur de composants**, sélectionnez les instances de composant requises et cliquez sur **Ajouter**.

   Toutes les instances WebSphere Application Server détectées sont ajoutées automatiquement à cette liste.
5. Cliquez sur **Précédent** et répétez les étapes «3», à la page 93 - «4», à la page 93 pour votre base de données. Ajoutez les autres instances de WebSphere Application Server et de base de données nécessaires à la Liste d'applications Java.



6. Cliquez sur **Fermer**, puis sur **Sauvegarder** pour revenir au Tableau de bord d'Application Performance .

Résultats

Conseil : Si le tableau de bord Agréger une topologie de transaction ne contient pas la topologie attendue, attendez que celui-ci s'actualise, puis vérifiez de nouveau quelques minutes plus tard. Si la topologie ne répond toujours pas à vos attentes, il est possible que votre application ne communique pas avec les composants prévus. Vérifiez votre environnement.

Affichage des résultats de la surveillance de la Liste d'applications Java IBM

Vous pouvez afficher les résultats de la surveillance de la Liste d'applications Java IBM dans les topologies.

Pourquoi et quand exécuter cette tâche

Les topologies contiennent des informations de surveillance des transactions transmises à partir du navigateur vers la base de données, y compris des informations de surveillance des ressources à partir des composants individuels. Les tableaux de bord Agréger une topologie de transaction et Topologie des instances de transaction contiennent les noeuds suivants :

- Navigateur, affiché uniquement lorsque l'injection de JavaScript est activée
- Serveur HTTP
- WebSphere Application Server
- Base de données

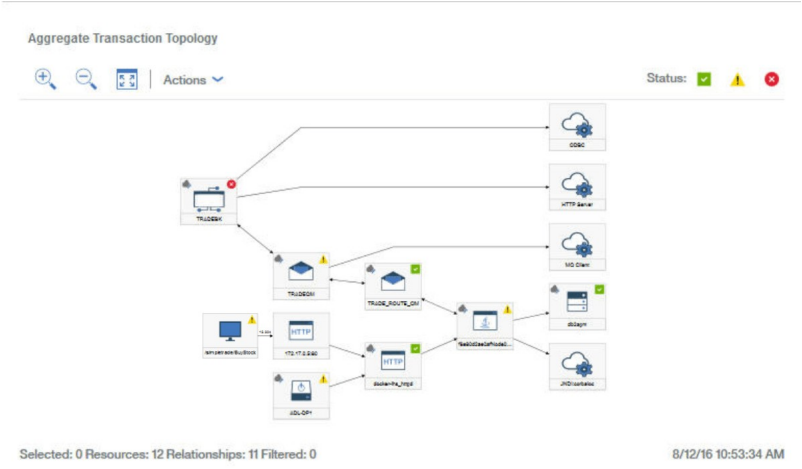
Procédure

Vous pouvez créer un lien entre les noeuds de la topologie et les détails supplémentaires sur ce noeud :

1. Survolez un noeud à l'aide de votre souris pour afficher une fenêtre contenant des informations supplémentaires.
2. Pour explorer un tableau de bord plus détaillé pour le noeud, cliquez avec le bouton droit de la souris sur le noeud et sélectionnez le lien.

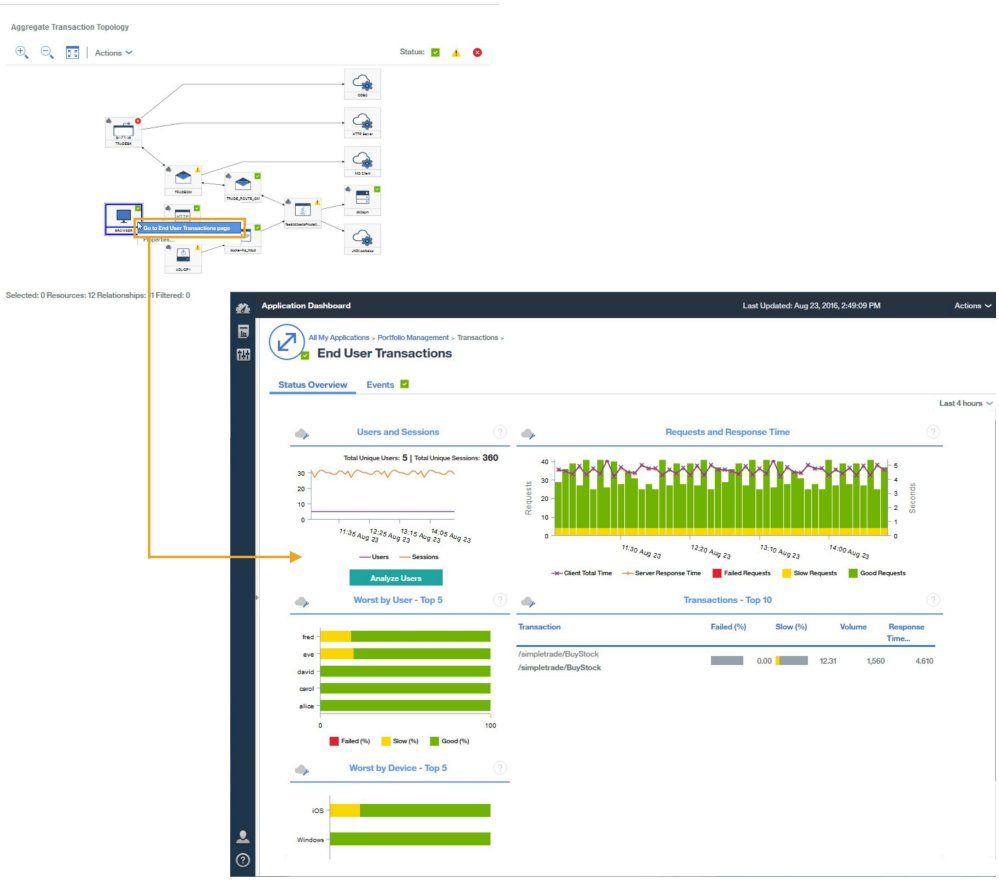
Agréger une topologie de transaction

Le widget Agréger une topologie de transaction est affiché dans le tableau de bord Récapitulatif de l'application.



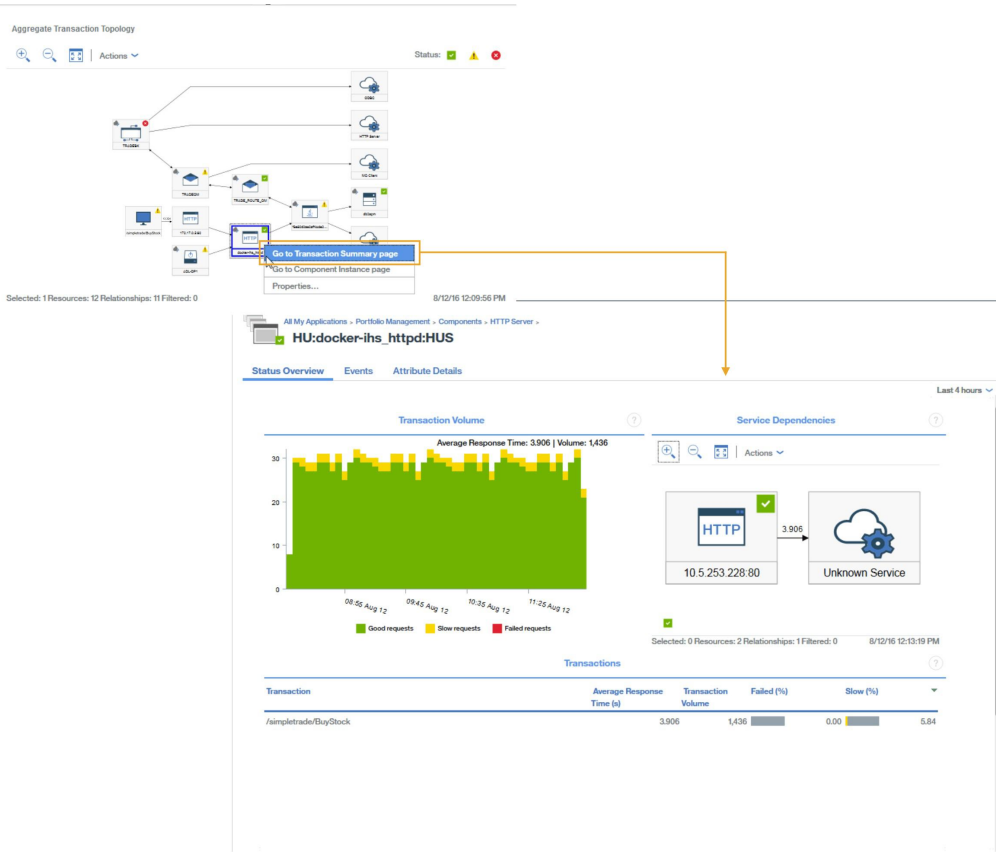
Le widget Agréger une topologie de transaction affiche les informations suivantes :

- Noeud pour les clients exécutables dans un navigateur, exploration détaillée de l'expérience d'utilisateur final



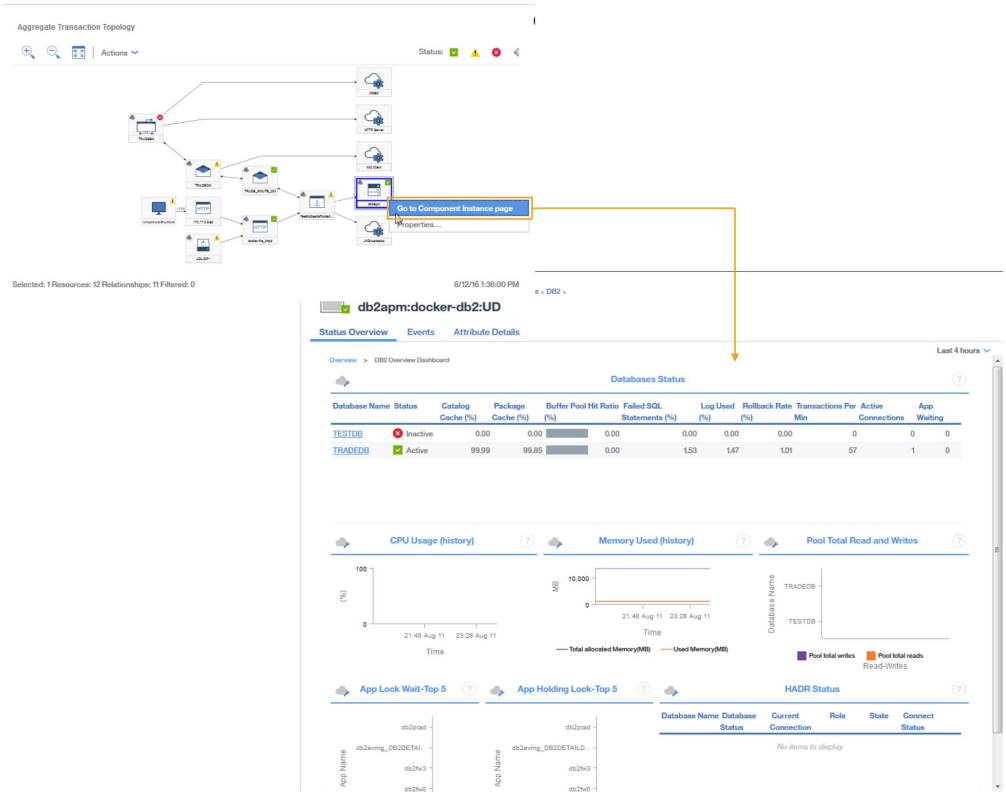
A faire : Ce noeud est affiché uniquement lorsque l'injection automatique de JavaScript mesure les données collectées par le navigateur.

- Noeuds pour les applications HTTP, exploration détaillée de la page des ressources du serveur Web ou de la page de récapitulatif des transactions



- Noeuds pour les applications basées sur WebSphere Application Server, exploration détaillée d'une page des ressources d'applications ou d'une page de récapitulatif des transactions

- Noeuds pour des serveurs de bases de données spécifiques, exploration détaillée de la page des ressources de base de données si disponible

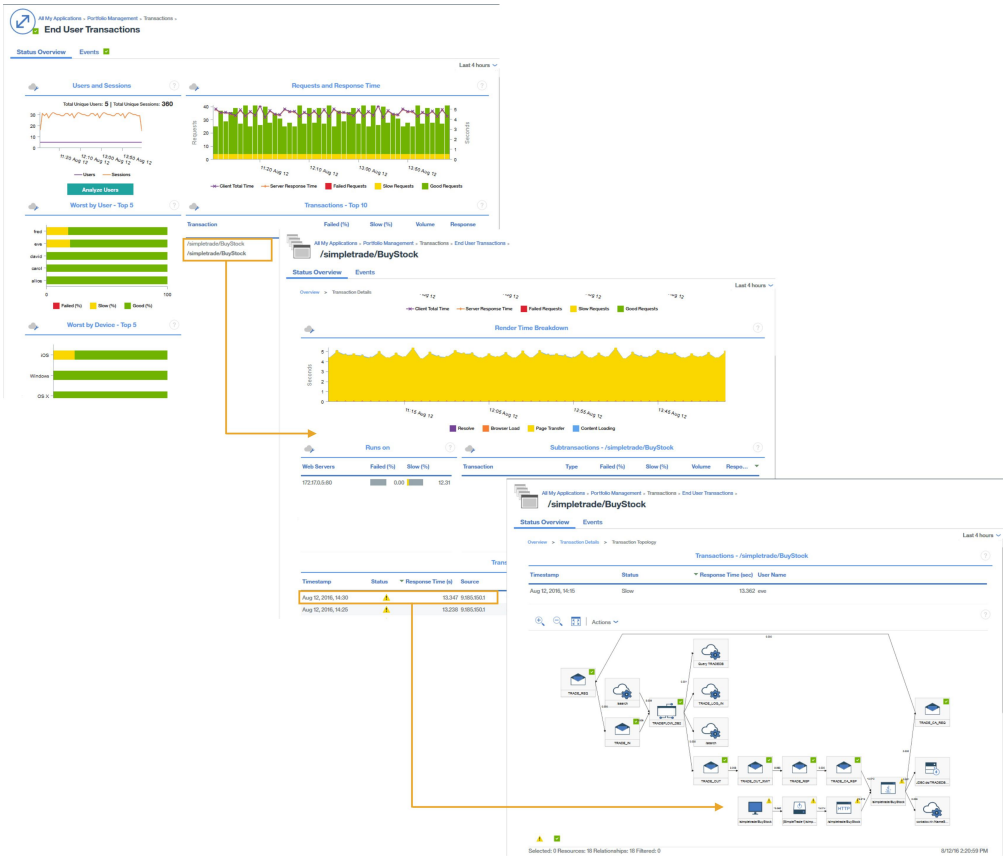


Topologie des instances de transaction

Les topologies des instances de transaction sont affichées pour les transactions d'utilisateur final réelles.

Accédez aux widgets suivants à partir du récapitulatif **Transactions utilisateur final** :

1. Sélectionner une transaction dans le tableau Transactions - 10 premières.
2. Sélectionner une instance dans le tableau Instances de transaction



Les topologies des instances de transaction pour la pile d'application Java affichent les noeuds suivants. Cliquez sur un noeud pour accéder à ses informations.

- Noeud pour les clients exécutables dans un navigateur

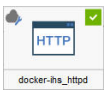
  A faire : Ce noeud est affiché uniquement lorsque l'injection automatique de JavaScript mesure les données collectées par le navigateur.
- Noeuds HTTP, y compris les temps de réponse du navigateur
- Noeuds DataPower, s'ils sont instrumentés
- Noeuds WebSphere Application Server incluant le détail d'une page des ressources d'application
- Noeuds de serveurs de base de données incluant le détail du statut d'une ressource de base de données et des informations de diagnostic d'instruction SQL pour les demandes JDBC

  Conseil : Lorsque la topologie indique que la plus grande partie du temps de réponse est utilisée dans la base de données, les informations d'instruction SQL sont directement ouvertes si vous cliquez sur **Diagnostiquer**.

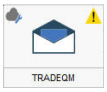
Les diagrammes de Gantt, qui récapitulent les temps des instances, sont également affichés.

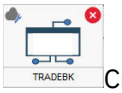
Diagnostic des incidents de votre environnement
Si les instances de transaction de l'un des composants de votre environnement sont lentes ou en échec alors le statut approprié est affecté au composant impacté.

Un noeud peut avoir l'un des statuts suivants :

- 

Satisfaisant : le noeud est caractérisé par une coche entourée d'un carré vert qui s'affiche dans l'angle supérieur droit

- 

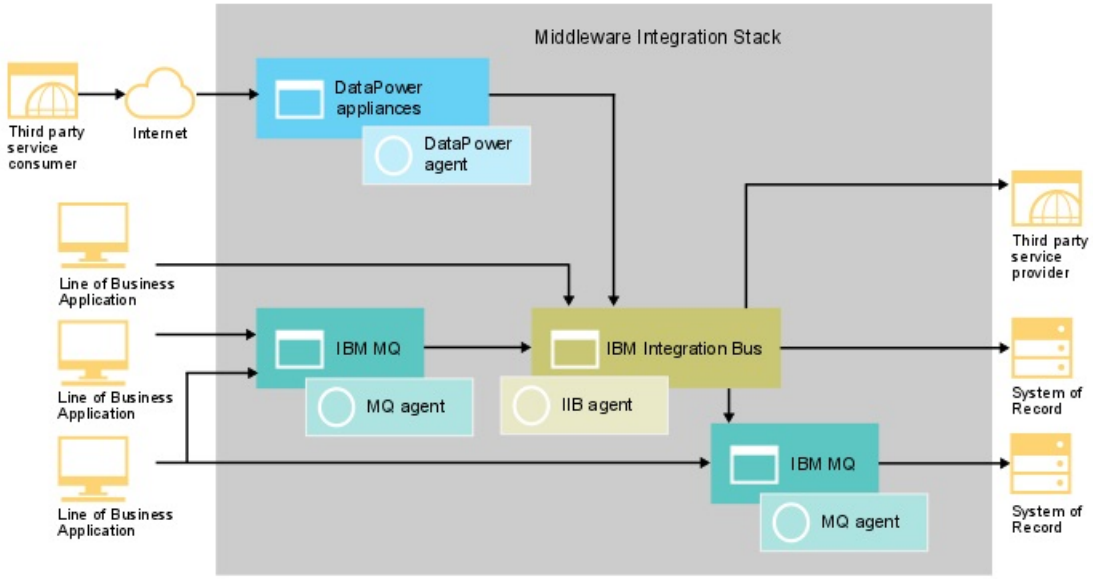
Avertissement : le noeud est caractérisé par un point d'exclamation entouré d'un triangle jaune qui s'affiche dans l'angle supérieur droit
- 

Critique : l'arrière-plan du noeud est rouge et une croix dans un cercle rouge s'affiche dans l'angle supérieur droit

Pour identifier la nature des problèmes liés aux composants dont le statut est avertissement ou critique, cliquez avec le bouton droit de la souris sur le noeud et examinez en détail les informations sur les causes probables des incidents.

Scénario : Surveillance de la Pile d'intégration IBM

Vous pouvez surveiller la Pile d'intégration IBM afin d'afficher des informations de suivi des transactions pour les produits middleware et les services qu'ils proposent et pour traiter les problèmes le cas échéant. La Pile d'intégration IBM contient IBM MQ, IBM Integration Bus et dispositif DataPower.



Surveillance de la Pile d'intégration IBM

Pour surveiller la Pile d'intégration IBM, installez les agents répertoriés pour chaque composant dans l'ordre indiqué.

(Facultatif) Si vous voulez également surveiller un système, installez les agents de système d'exploitation sur ce système.

Pour IBM MQ, procédez comme suit :

1. Installez Monitoring Agent for WebSphere MQ.
2. Configurez l'agent WebSphere MQ pour la connexion au gestionnaire de files d'attente.
3. Activez **Trace de l'activité de l'application MQ** dans le gestionnaire de files d'attente.

Pour IBM Integration Bus, procédez comme suit :

1. Installez Monitoring Agent for IBM Integration Bus.
2. Activez IBM Integration Bus pour le suivi des transactions.
3. Configurez le suivi des transactions pour les instances de l'agent IBM Integration Bus requises.

Pour dispositif DataPower, procédez comme suit :

1. Installez Monitoring Agent for DataPower.

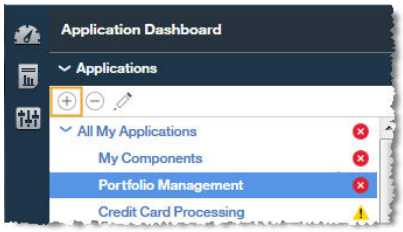
2. Configurez l'agent DataPower pour vous connecter au dispositif DataPower.
3. Vérifiez que le suivi des transactions est activé pour les instances de l'agent DataPower requises.
4. Configurez le dispositif DataPower.

Ajout d'applications middleware au Tableau de bord d'Application Performance
Créez une application Pile d'intégration IBM et ajoutez-y les instances IBM MQ, IBM Integration Bus et dispositif DataPower que vous souhaitez surveiller.

Procédure

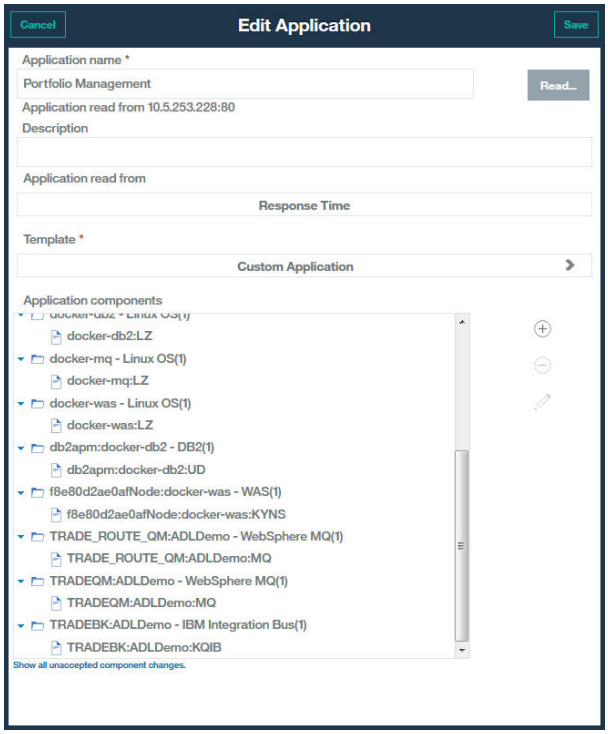
Pour afficher les composants de la Pile d'intégration IBM, procédez comme suit dans le Tableau de bord d'Application Performance :

1. Dans le Tableau de bord d'Application Performance , cliquez sur **Ajouter une application**.



2. Dans la fenêtre **Modification d'application**, ajoutez un nom d'application, puis cliquez sur **Ajouter des composants** +.
3. Dans la fenêtre **Sélectionner le composant**, sélectionnez **IBM Integration Bus**.
4. Dans l'**Editeur de composants**, sélectionnez les instances de composant requises et cliquez sur **Ajouter**.

   Toutes les instances IBM Integration Bus détectées sont ajoutées automatiquement à cette liste.
5. Cliquez sur **Précédent** et répétez les étapes 3 - 4 pour **WebSphere MQ** et **DataPower Appliance**. Ajoutez les autres instances IBM Integration Bus, IBM MQ et dispositif DataPower jusqu'à ce que la Pile d'intégration IBM soit terminée.



6. Cliquez sur **Fermer**, puis sur **Sauvegarder** pour revenir au Tableau de bord d'Application Performance .

Résultats

Conseil : Si le tableau de bord Agréger une topologie de transaction ne contient pas la topologie attendue, attendez que celui-ci s'actualise, puis vérifiez de nouveau quelques minutes plus tard. Si la topologie ne correspond toujours pas à vos attentes, votre application ne communique peut-être pas avec les composants attendus. Vérifiez votre environnement.

Affichage des résultats de la surveillance de la Pile d'intégration IBM

Vous pouvez afficher les résultats de la surveillance de la Pile d'intégration IBM dans les pages de topologies et de middleware. Vous pouvez également afficher les événements générés lorsqu'une transaction dépasse un seuil défini.

Pourquoi et quand exécuter cette tâche

Les topologies affichent les interactions entre les composants de middleware. Les noeuds middleware suivants s'affichent dans Agréger une topologie de transaction et Topologie des instances de transaction :

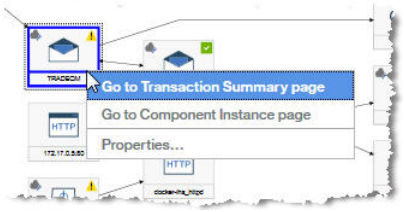
- IBM Integration Bus
- IBM MQ
- dispositif DataPower

Faites glisser le pointeur de la souris sur un noeud pour afficher une fenêtre de propriétés qui fournit des informations expliquant pourquoi un noeud a un statut particulier. Le statut est déterminé par des situations ; les situations dont le statut est incorrect sont affichées.

Procédure

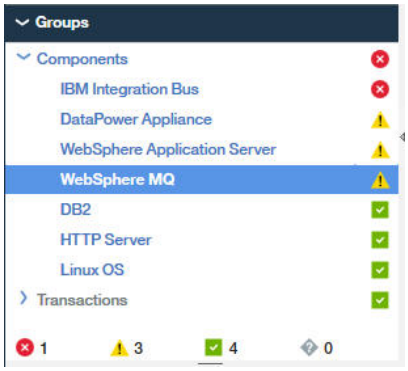
Vous pouvez créer un lien entre les noeuds de la topologie et les détails supplémentaires sur ce noeud :

1. Cliquez sur un noeud avec le bouton droit de la souris.



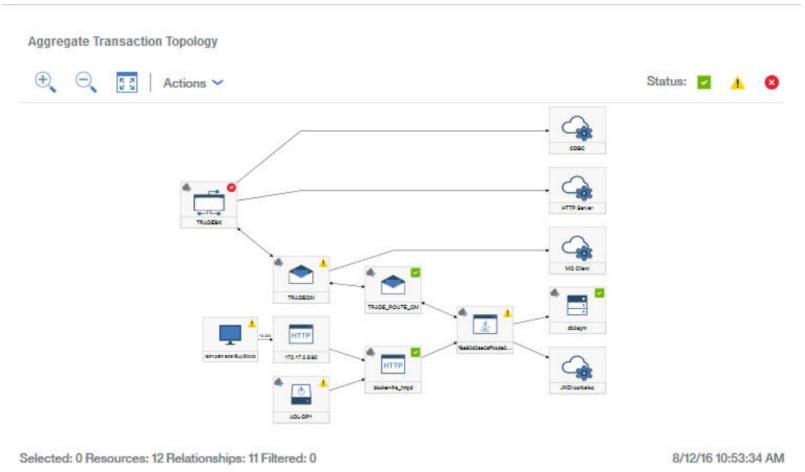
2. Sélectionnez **Accéder à la page Instance de composant** pour afficher des informations sur le composant.
3. Sélectionnez **Accéder à la page Récapitulatif des transactions** pour afficher des informations sur les transactions de middleware.

   Conseil : Sélectionnez **Groupes** > **Composants** > ***composant middleware*** dans le navigateur et sélectionnez une période de demande dans le widget de volume pour accéder au même tableau de bord.



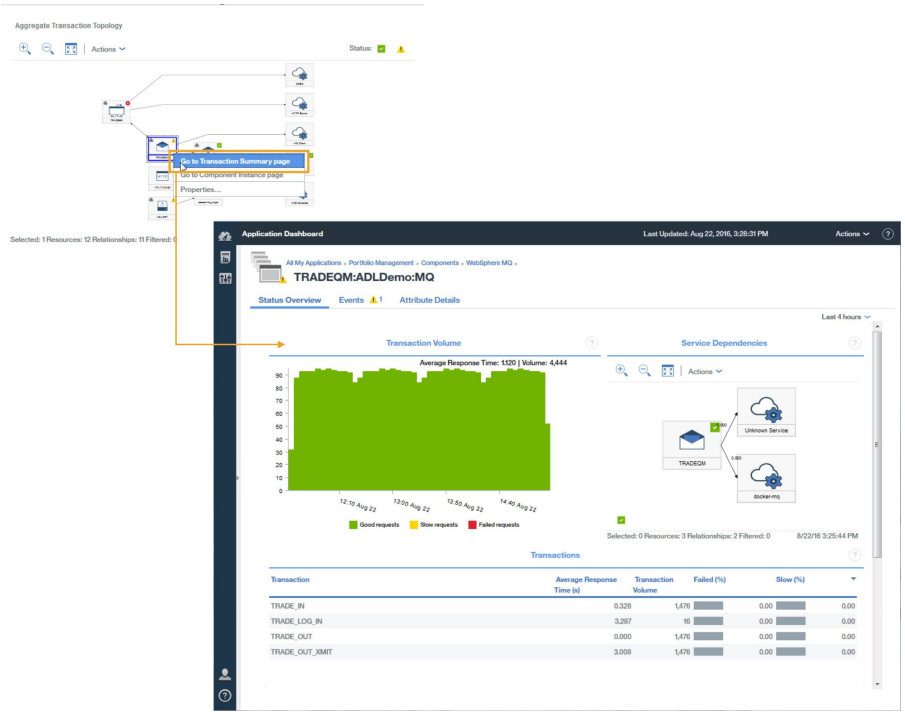
Agréger une topologie de transaction

Le widget Agréger une topologie de transaction est affiché dans le tableau de bord Récapitulatif de l'application.



Le widget Agréger une topologie de transaction peut afficher les noeuds IBM MQ, IBM Integration Bus et dispositif DataPower. Effectuez une exploration en aval à partir de ces noeuds pour obtenir plus d'informations sur la pile d'intégration du middleware.

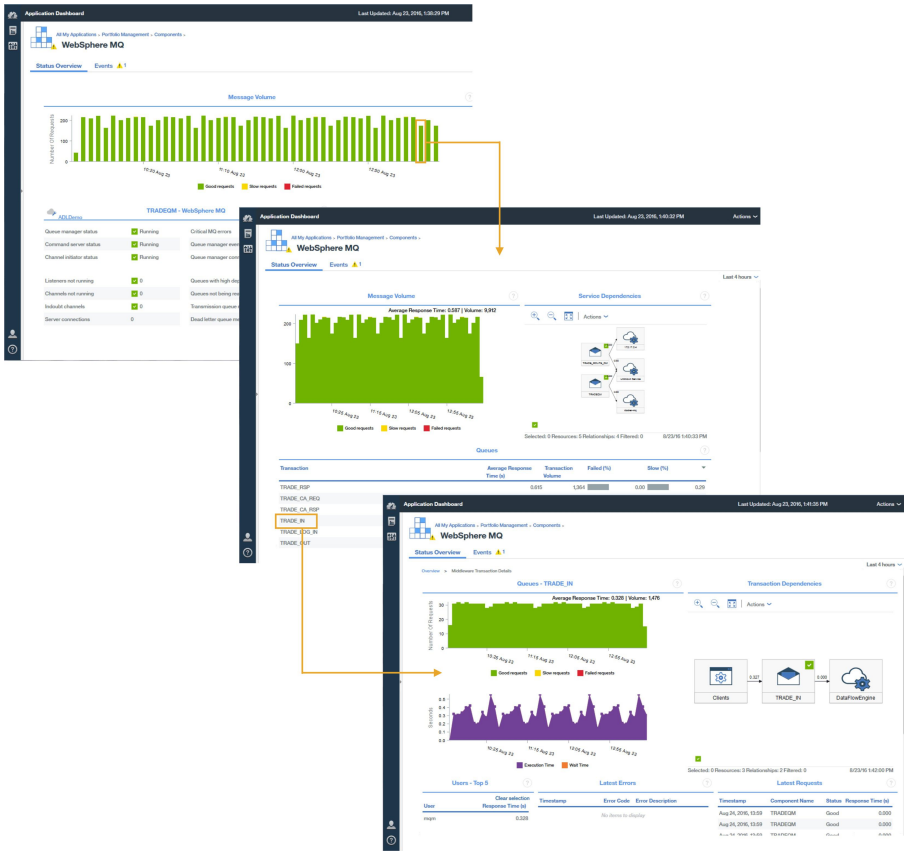
Pour explorer en aval, cliquez sur un noeud de middleware avec le bouton droit de la souris dans Agréger une topologie de transaction, puis sélectionnez **Accéder à la page Récapitulatif des transactions**. Vous pouvez également sélectionner **Groupes** > **Composants** > ***composant de middleware*** dans le navigateur et sélectionner une période de demande dans le widget de volume pour accéder aux mêmes informations.



Détails des transactions de middleware

A partir de la page Récapitulatif des transactions de middleware, vous pouvez explorer en aval jusqu'aux détails des transactions de middleware.

Pour explorer en aval les détails des transactions de middleware pour le composant, procédez comme suit :



1. Dans la page Récapitulatif des transactions de middleware pour le composant, sélectionnez un intervalle de surveillance dans le graphique **Message ou volume**.
2. Dans la page **Récapitulatif des transactions de middleware**, dans le widget **Files d'attente**, **Courtiers** ou **Dispositifs**, sélectionnez une file d'attente, un courtier ou un dispositif.

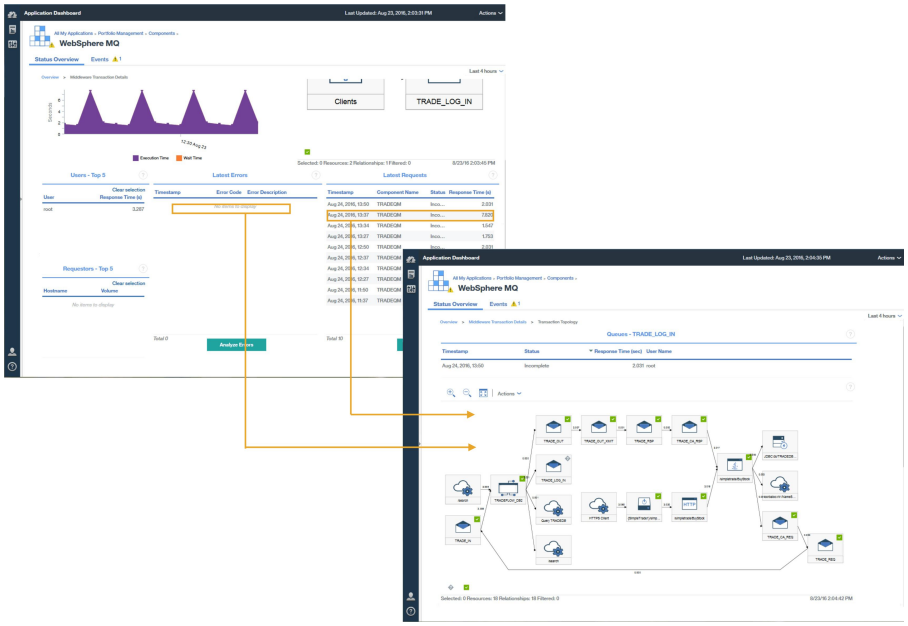
Analyse des erreurs et des instances

A partir de la page de détails des transactions du middleware, vous pouvez effectuer une exploration en aval jusqu'aux informations qui vous aident à analyser les erreurs et instances et accéder à la topologie des instances de transaction.

Pour explorer en aval jusqu'aux erreurs et instances des composants de middleware, puis accéder à la topologie des instances de transaction, dans la page **Détails des transactions**, effectuez l'une des étapes suivantes :

- Cliquez sur **Erreurs d'analyse** pour afficher la page **Analyse des erreurs**, puis sélectionnez une erreur.
- Cliquez sur **Demandes d'analyse** pour afficher la page **Analyse d'instance**, puis sélectionnez une instance.

Vous pouvez également, dans la page **Détails des transactions**, sélectionner une erreur ou une instance pour accéder directement à la topologie des instances de transaction.



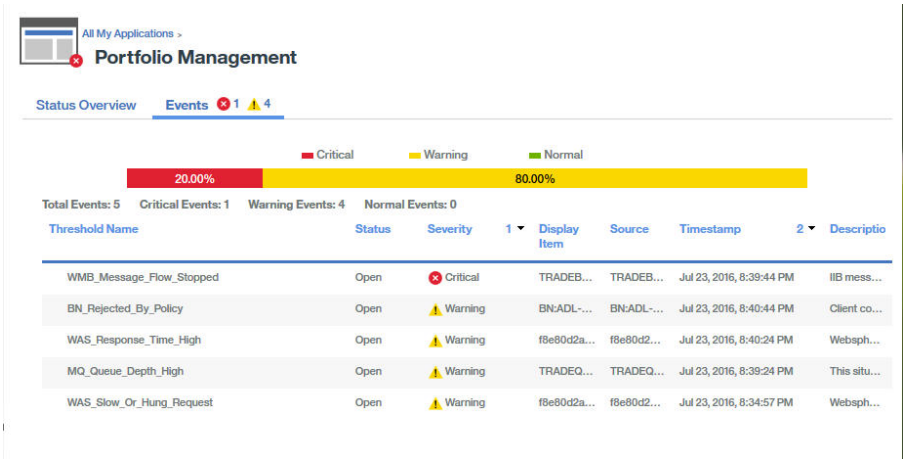
Les topologies des instances de transaction affichent les noeuds middleware suivants :

- Gestionnaires de files d'attente de messages
- Courtiers IBM Integration Bus
- Dispositifs DataPower

Sélectionnez un noeud pour afficher ses propriétés qui expliquent pourquoi un noeud a un statut particulier.

Un diagramme de Gantt des transactions s'affiche pour la file d'attente ou le courtier sélectionné. Le diagramme de Gantt vous aide à isoler les éléments les plus pertinents concernant le temps de réponse global de la transaction.

Evénements
Les seuils de suivi des transactions par défaut génèrent des événements pour la Pile d'intégration IBM, en plus des autres agents.



Pour plus d'informations sur les événements de suivi des transactions par défaut, voir «Seuils d'événement pour la surveillance des transactions », à la page 1043.

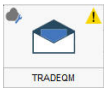
Vous pouvez ajouter des seuils pour créer plus d'événements, par exemple pour des débits de transaction qui sont lents ou qui passent au-dessous d'un certain seuil.

Pour plus d'informations sur l'ajout d'événements, voir «Création de seuils de génération d'événements pour la surveillance des transactions», à la page 1046.

Diagnostic des incidents de votre environnement
Si les instances de transaction de l'un des composants de votre environnement sont lentes ou en échec alors le statut approprié est affecté au composant impacté.

Un noeud peut avoir l'un des statuts suivants :

- 

Satisfaisant : le noeud est caractérisé par une coche entourée d'un carré vert qui s'affiche dans l'angle supérieur droit
- 

Avertissement : le noeud est caractérisé par un point d'exclamation entouré d'un triangle jaune qui s'affiche dans l'angle supérieur droit
- 

Critique : l'arrière-plan du noeud est rouge et une croix dans un cercle rouge s'affiche dans l'angle supérieur droit

Pour identifier la nature des problèmes liés aux composants dont le statut est avertissement ou critique, cliquez avec le bouton droit de la souris sur le noeud et examinez en détail les informations sur les causes probables des incidents.

Téléchargement de vos agents et de vos collecteurs de données

Vous pouvez accéder à votre abonnement Cloud APM à partir du site Web IBM Marketplace. Connectez-vous à votre compte et téléchargez les fichiers archive d'installation. Les fichiers archive d'installation incluent les fichiers d'installation et de configuration des agents et des collecteurs de données.

Pour en savoir plus sur le téléchargement des agents et des collecteurs de données, effectuez les étapes des tutoriels suivants :

- «Tutoriel : Téléchargement et installation d'un agent», à la page 106

- «Tutoriel : Téléchargement et configuration d'un collecteur de données», à la page 110

Vous pouvez vous inscrire pour un essai actif ou acheter un abonnement pour l'une des offres IBM Cloud Application Performance Management depuis IBM Marketplace.

IBM Marketplace

Inscrivez-vous pour un essai à l'adresse IBM Marketplace > Cloud APM > Essai gratuit. Achetez un abonnement à l'adresse IBM Marketplace > Cloud APM > Acheter . Connectez-vous à la page Produits et services pour télécharger vos agents et les collecteurs de données.

La page **Produits et services** est disponible pour les abonnés actifs. En cas de problème, accédez au Support Marketplace.

Tester la connectivité

Pour plus d'informations sur la vérification de la connectivité au serveur Cloud APM, qui est utilisé pour télécharger les packages, voir Connectivité réseau.

Tutoriel : Téléchargement et installation d'un agent

Ce tutoriel vous permet d'acquérir l'expérience du téléchargement et de l'installation d'un Cloud APM agent Windows OS à partir d'IBM Marketplace. Vous pouvez ensuite démarrer la console Cloud APM et vérifier la santé de votre ressource surveillée en affichant des indicateurs clés de performance dans les tableaux de bord.

Pourquoi et quand exécuter cette tâche

Ce tutoriel implique le téléchargement du package d'installation Windows depuis la page **Produits et services** sur IBM Marketplace, l'extraction des fichiers d'installation et l'installation de l'agent Windows OS. Retournez à la page **Produits et services** pour lancer la console Cloud APM et ouvrir le Tableau de bord d'Application Performance pour vérifier la santé de votre système Windows.

Procédure

1. Si vous n'êtes pas connecté à IBM Marketplace, connectez-vous avec vos ID utilisateur et mot de passe IBM, et accédez à **Produits et services**.

   La page **Produits et services** est disponible pour les abonnés actifs. En cas de problème, accédez au forum Cloud Application Performance Management ou au Support Marketplace.
2. Téléchargez le fichier archive d'installation de Windows :
   a) Dans la boîte de souscription de Cloud APM, cliquez sur **Gérer** > **Téléchargements**.
   b) Sélectionnez le système d'exploitation Windows.

      Sélectionnez le package d'agents IBM Cloud Application Performance Management 64 bits. Si vous utilisez la version 32 bits de Windows, sélectionnez le package d'agent 32 bits.
   c) Cliquez sur **Download** et enregistrez le fichier archive d'installation d'agent sur votre système. Exemple :

      ```
      C:\Users\MY_ADMIN\Downloads\IAPM_Agent_Install.zip
      ```
3. Sur votre système Windows local, accédez au répertoire dans lequel vous avez enregistré le fichier archive téléchargé et extrayez son contenu.
   Par exemple, dans l'Explorateur Windows, ouvrez le répertoire **Téléchargements**, cliquez avec le bouton droit de la souris sur `IAPM_Agent_Install.zip`, puis sélectionnez **Extraire tout**.
4. Ouvrez une invite de commandes en tant qu'administrateur :
   a) Dans le menu **Démarrer** de Windows, tapez `commande` dans la zone de recherche.
   b) Cliquez sur **Invite de commandes** avec le bouton droit de la souris dans la liste qui s'affiche, puis sélectionnez **Exécuter en tant qu'administrateur**.
5. Accédez au répertoire dans lequel vous avez extrait les fichiers d'installation.

Exemple :

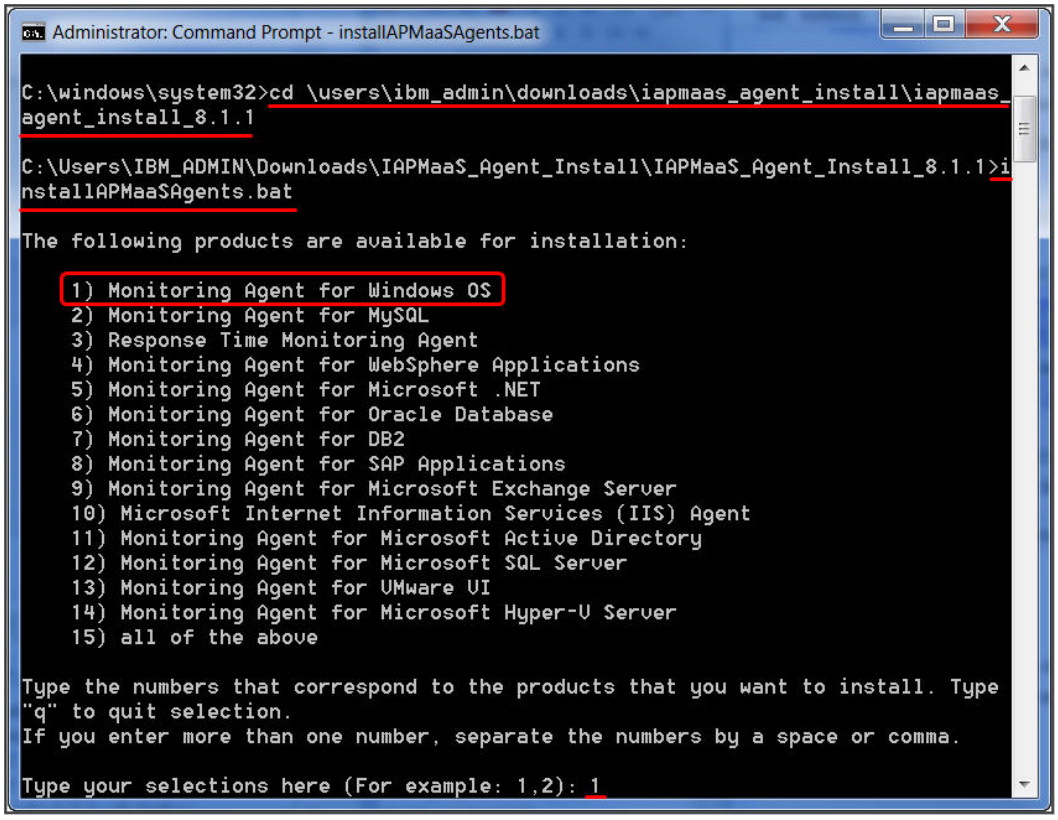
```
cd C:\Users\MY_ADMIN\Downloads\IAPM_Agent_Install\IAPM_Agent_Install_8.1.4
```

6. Exécutez le script d'installation pour installer l'agent Windows OS :
   a) Exécutez la commande suivante :

   ```
   installAPMAgents.bat
   ```

   b) Dans la liste des agents disponibles, entrez le numéro qui correspond à l'agent Windows OS.
   c) Répondez aux invites pour confirmer que vous voulez installer l'agent Windows OS et acceptez le contrat de licence.

   Une analyse des prérequis de votre environnement, qui prend un certain temps, commence. Si des exigences ne sont pas satisfaites, un message vous dirige vers un fichier journal indiquant la raison de l'échec. Un prérequis non satisfait tel un espace disque insuffisant entraîne l'arrêt du processus d'installation. Vous devez corriger le problème et relancer le script d'installation. En cas de problème, accédez au forum Cloud Application Performance Management ou envoyez un e-mail à `info@ibmserviceengage.com`.



Pour afficher le rapport sur les exigences du système d'exploitation Windows, voir System requirements (APM Developer Center).

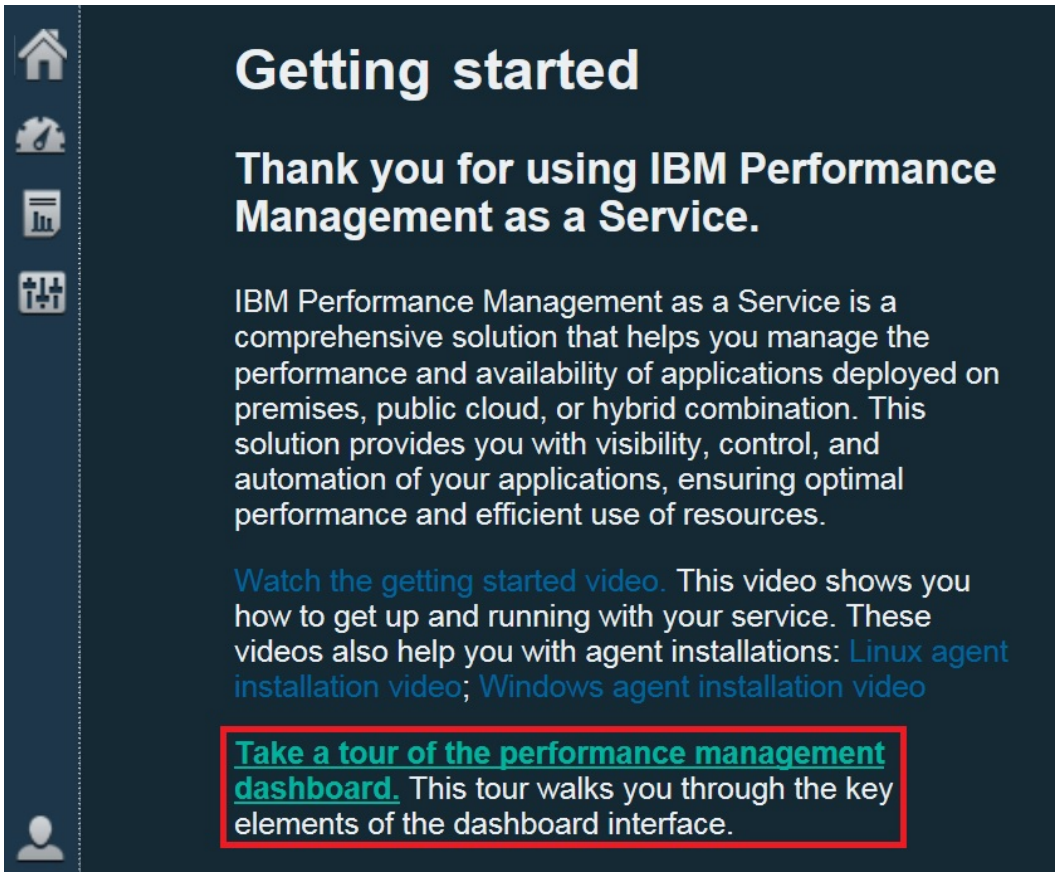
Une fois l'installation réussie, l'agent Windows OS démarre automatiquement et vous pouvez démarrer la console Cloud APM pour lancer la surveillance de votre système Windows.

Remarque : Si votre environnement inclut un pare-feu qui n'autorise pas les connexions HTTPS sortantes transparentes à un hôte externe, vous devez configurer un proxy direct pour les communications entre l'agent et le serveur Cloud APM. En configurant un proxy direct, vous pouvez acheminer l'intégralité du trafic vers un point spécifique du réseau et de n'autoriser qu'une seule connexion via le pare-feu. Pour plus d'informations, voir «Configuration des agents pour qu'ils communiquent via un proxy direct», à la page 163.

7. Retournez dans **Produits et services** sur IBM Marketplace et cliquez sur **Lancer** dans la boîte de souscription de Cloud APM.

La console Cloud APM s'ouvre sur la page **Mise en route** à partir de laquelle vous pouvez vous familiariser avec les fonctions, visionner des vidéos de différents scénarios d'utilisation et ouvrir les pages de console associées.

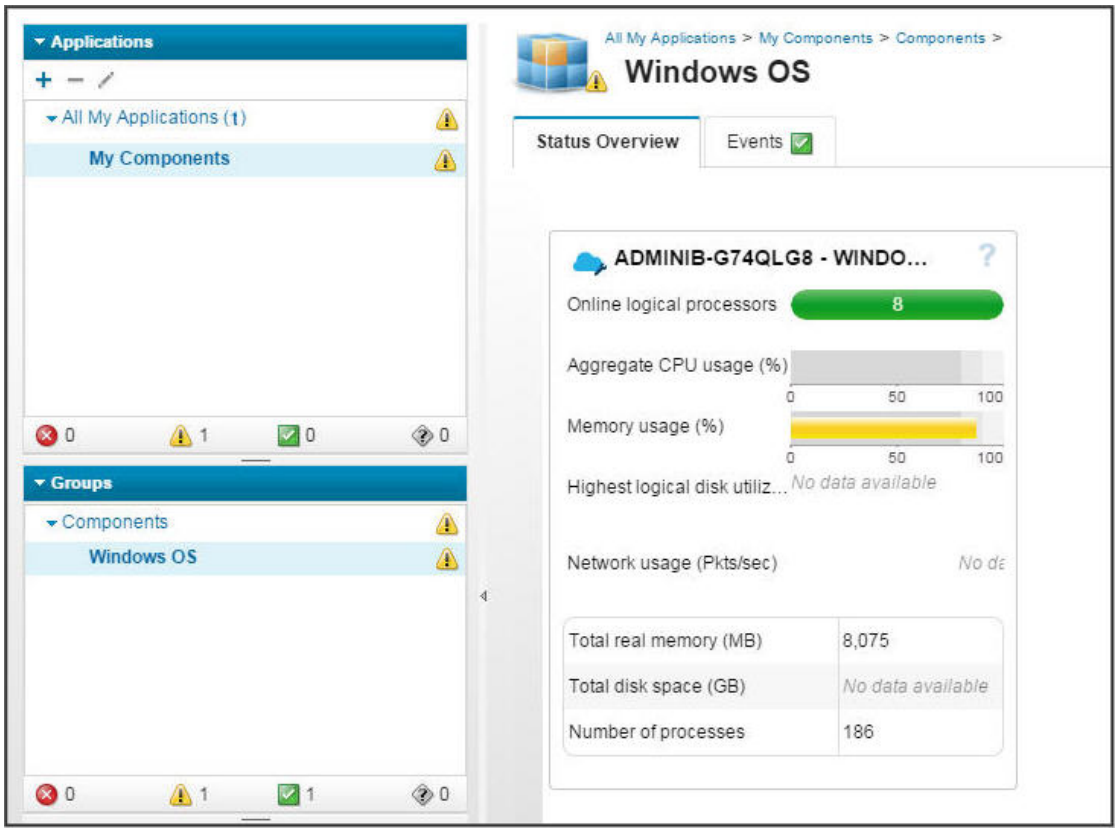
8. Dans la page **Mise en route**, cliquez sur "Visitez le tableau de bord de gestion des performances" pour un tour d'horizon des éléments de navigation.



9. Ouvrez le tableau de bord récapitulatif du système d'exploitation Windows :
   a) A partir de la barre de navigation, cliquez sur **Performance** > **Tableau de bord d'Application Performance**.
      - Le tableau de bord **Toutes mes applications** s'affiche avec une zone d'état récapitulative de chacune des applications définies dans votre environnement. Au départ, seule l'application prédéfinie **Mes composants** s'affiche.
      - Si une fenêtre **Ajouter une application** s'affiche au lieu de **Mes composants**, créez une application pour visualiser votre ressource surveillée :
        1) Entrez un nom pour l'application, par exemple, "Mon application".
        2) Cliquez sur +.
        3) Faites défiler la liste vers le bas jusqu'à **Sélectionner le composant**, puis cliquez sur **Système d'exploitation Windows**.
        4) Dans l'éditeur de composant, cliquez sur `Principal :`*`nom_hôte`*`:NT`, sur **Ajouter**, puis sur **Précédent** pour ajouter votre agent à l'application.
        5) Cliquez sur **Sauvegarder** pour fermer la fenêtre et afficher une zone d'état récapitulative de votre nouvelle application dans le tableau de bord.
   b) Dans la zone récapitulative, cliquez sur **Composants**.
      - Le tableau de bord récapitulatif de votre système géré de système d'exploitation Windows s'affiche. Dans ce tableau de bord, vous pouvez cliquer n'importe où dans le widget de groupe de

récapitulatif d'état pour défiler vers le bas jusqu'à des tableaux de bord détaillés contenant des indicateurs clés de performance renvoyés depuis votre agent Windows OS.

- Un agent qui vient d'être démarré peut nécessiter un peu de temps pour communiquer avec l'infrastructure de surveillance et envoyer des indicateurs clés de performance à la console.



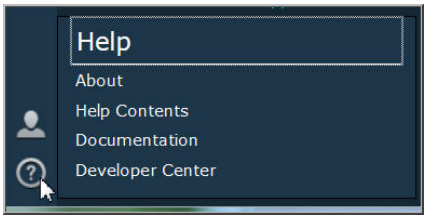
Si l'agent ne communique pas avec le serveur Cloud APM ou n'est pas démarré, le tableau de bord récapitulatif n'affiche aucun indicateur clé de performance et affiche l'état inconnu. Vous pouvez utiliser la commande **os-agent** pour vérifier l'état et démarrer l'agent si nécessaire. Ouvrez une invite de commande en tant qu'administrateur et entrez la commande **os-agent status** à partir du dossier `C:\\IBM\APM\bin`. Si l'agent n'est pas démarré, entrez la commande **os-agent start**.

Résultats

Vous avez installé un agent Cloud APM et observé les données de surveillance envoyées aux Tableau de bord d'Application Performance.

Que faire ensuite

- Explorez la console : Pendant que vous utilisez la console Cloud APM, explorez ses fonctionnalités. Vous pouvez en savoir plus sur le tableau de bord en cours en cliquant sur dans la bannière de la fenêtre. Vous pouvez ouvrir le système d'aide ou l'ensemble de rubriques relatives à Cloud APM sur IBM Knowledge Center à partir du menu **Aide** dans la barre de navigation.



- Installez d'autres agents : Vous disposez de tous les fichiers d'installation nécessaires pour installer d'autres types d'agent Windows pour la surveillance de votre environnement. Vous pouvez également installer des agents sur d'autres systèmes de votre environnement. Si vous disposez de systèmes AIX

ou Linux, téléchargez le fichier archive d'installation correspondant. Certains types d'agent ont des exigences à satisfaire avant de les installer et la plupart des types d'agent nécessitent quelques opérations de configuration après leur installation. Pour plus d'informations, voir «Préinstallation sur les systèmes AIX», à la page 125, «Préinstallation sur les systèmes Linux», à la page 132, «Préinstallation sur les systèmes Windows», à la page 140 et Chapitre 7, «Configuration de votre environnement», à la page 163.

Tutoriel : Téléchargement et configuration d'un collecteur de données

Ce tutoriel vous permet d'acquérir l'expérience du téléchargement et de la configuration d'un collecteur de données Cloud APM Bluemix Ruby à partir d'IBM Marketplace. Vous pouvez ensuite démarrer la console Cloud APM et vérifier la santé de votre ressource surveillée en affichant des indicateurs clés de performance dans les tableaux de bord.

Pourquoi et quand exécuter cette tâche

Ce tutoriel implique le téléchargement d'un package de collecteur de données pour applications Bluemix à partir de la page **Produits et services** sur IBM Marketplace, l'extraction des fichiers de configuration et la configuration du collecteur de données Bluemix Ruby sur un système Linux. Retournez à la page **Produits et services** pour lancer la console Cloud APM et ouvrir le Tableau de bord d'Application Performance pour vérifier la santé de votre application Bluemix Ruby.

Procédure

1. Si vous n'êtes pas connecté à IBM Marketplace, connectez-vous avec vos ID utilisateur et mot de passe IBM, et accédez à **Produits et services**.

   La page **Produits et services** est disponible pour les abonnés actifs. En cas de problème, accédez au forum Cloud Application Performance Management ou au Support Marketplace.
2. Téléchargez le package de collecteur de données pour applications Bluemix `IBM_Bluemix_Data_Collectors_Install.tgz`.
3. Sur votre système local, accédez au répertoire dans lequel vous avez enregistré le fichier archive téléchargé et extrayez son contenu en exécutant la commande suivante :

   ```
   tar -zxvf IBM_Bluemix_Data_Collectors_Install.tgz
   ```

   Vous obtenez quatre fichiers compressés, chacun représentant un collecteur de données pour un type d'application Bluemix. Le package de collecteur de données pour les applications Bluemix Ruby est `ruby_datacollector.tgz`.
4. Extrayez les fichiers de `ruby_datacollector.tgz` en exécutant la commande suivante, par exemple :

   ```
   tar -zxvf ruby_datacollector.tgz
   ```

   Vous obtenez un dossier `ibm_ruby_dc`.
5. Copiez l'intégralité du dossier `etc` qui se trouve dans `ibm_ruby_dc` vers le dossier principal de votre application Ruby en exécutant la commande suivante, par exemple :

   ```
   cp –r répertoire du dossier etc  répertoire de base de votre application Ruby
   ```

   Si vous extrayez le collecteur de données dans le répertoire `/opt/ibm/ccm/ibm_ruby_dc/etc` et si le répertoire de base de votre application Ruby est `/root/ruby_app/`, la commande est la suivante :

   ```
   cp –r /opt/ibm/ccm/ibm_ruby_dc/etc /root/ruby_app/
   ```
6. Ajoutez la section suivante au fichier `Gemfile` dans le dossier de base de votre application Bluemix Ruby :

   ```
   gem 'logger',  '>= 1.2.8'
   source 'https://managemserver.ng.bluemix.net' do
   ```

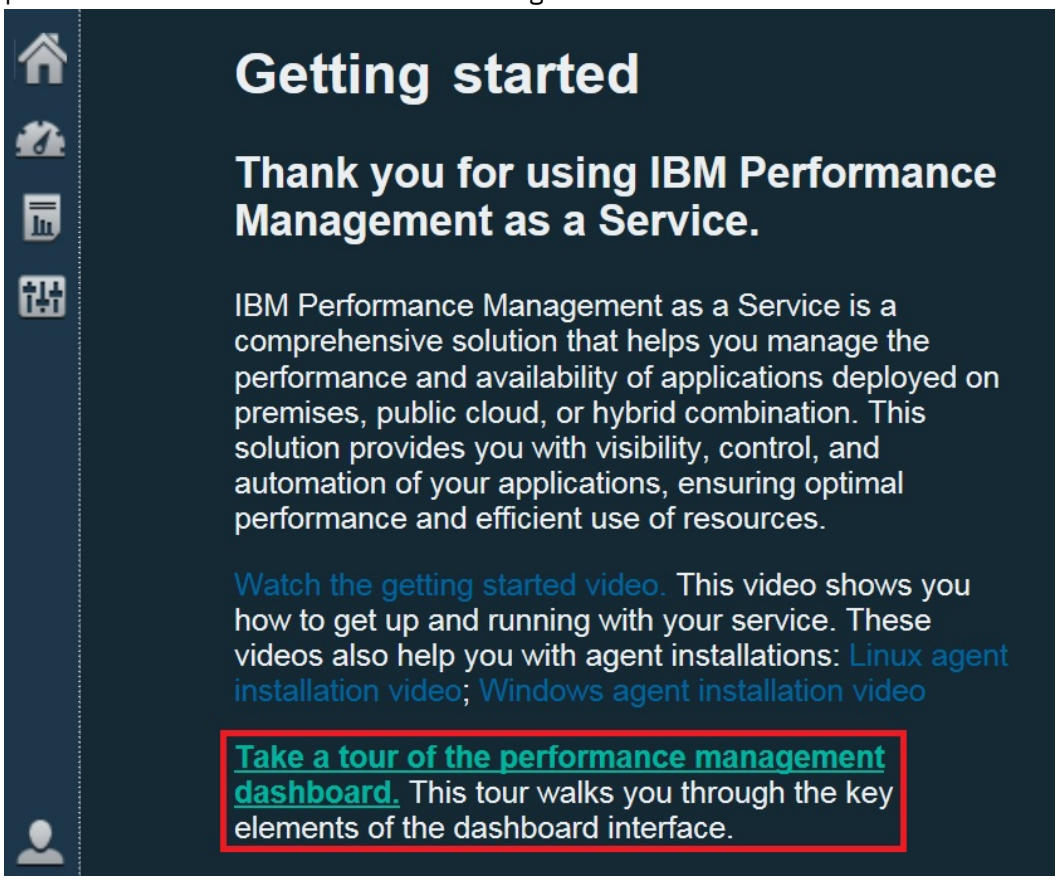
```
  gem 'ibm_resource_monitor'
  gem 'stacktracer'
end
```

7. Exécutez la commande `bundle lock` pour régénérer le fichier `Gemfile.lock`.
8. A partir du répertoire de base de votre application Ruby, exécutez la commande suivante :

```
cf push
```

9. Retournez dans **Produits et services** sur IBM Marketplace et cliquez sur **Lancer** dans la boîte de souscription de Cloud APM.

   La console Cloud APM s'ouvre sur la page **Mise en route** à partir de laquelle vous pouvez vous familiariser avec les fonctions, visionner des vidéos de différents scénarios d'utilisation et ouvrir les pages de console associées.
10. Dans la page **Mise en route**, cliquez sur "Visitez le tableau de bord de gestion des performances" pour un tour d'horizon des éléments de navigation.



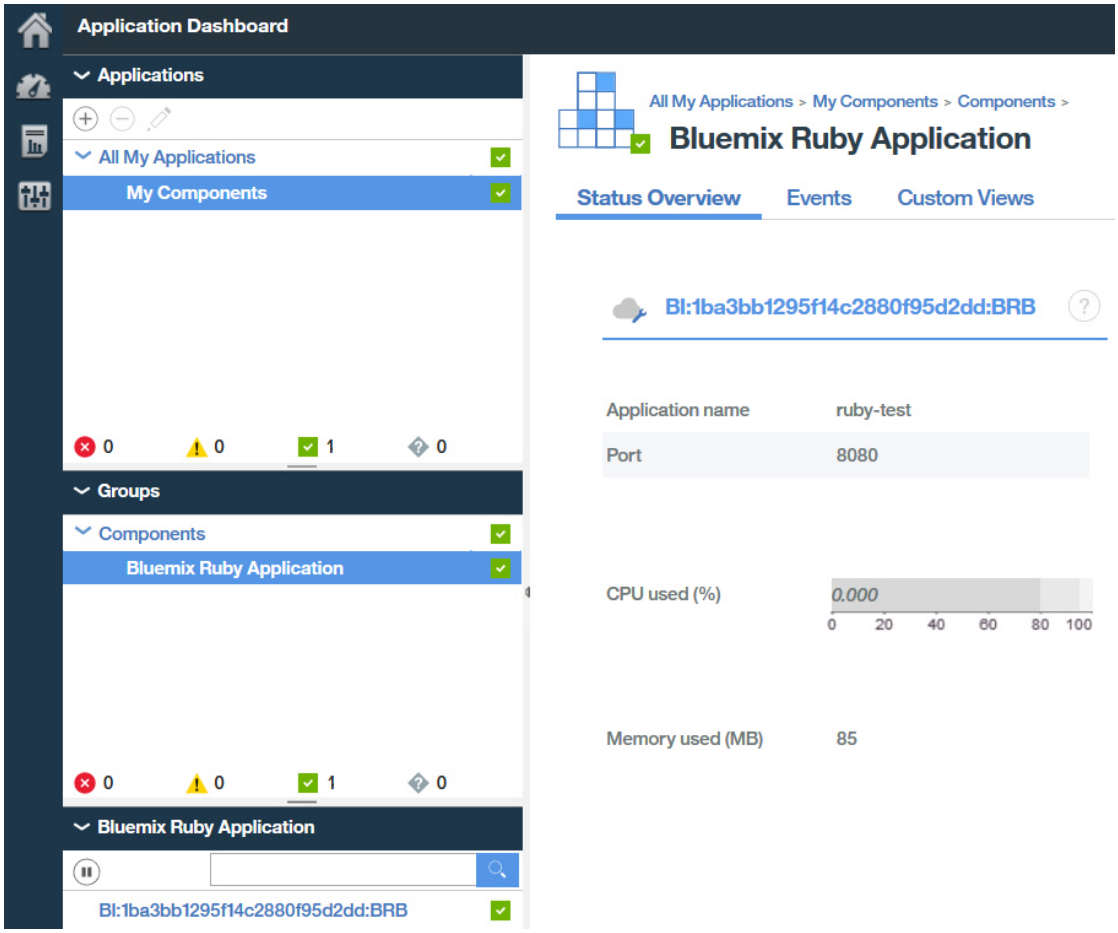
11. Ouvrez le tableau de bord récapitulatif des applications Bluemix Ruby :
    a) A partir de la barre de navigation, cliquez sur **Performance** > **Tableau de bord d'Application Performance**.
    - Le tableau de bord **Toutes mes applications** s'affiche avec une zone d'état récapitulative de chacune des applications définies dans votre environnement. Au départ, seule l'application prédéfinie **Mes composants** s'affiche.
    - Si une fenêtre **Ajouter une application** s'affiche au lieu de **Mes composants**, créez une application pour visualiser votre ressource surveillée :
      1) Entrez un nom pour l'application, par exemple, "Mon application".
      2) Cliquez sur +.
      3) Cliquez sur **Application Bluemix Ruby**.

4) Dans l'éditeur de composant, sélectionnez une instance, cliquez sur **Ajouter**, puis sur **Précédent** pour ajouter votre collecteur de données à l'application.

5) Cliquez sur **Sauvegarder** pour fermer la fenêtre et afficher une zone d'état récapitulative de votre nouvelle application dans le tableau de bord.

b) Dans la zone récapitulative, cliquez sur **Composants**.

- Le tableau de bord récapitulatif de votre application Bluemix Ruby s'affiche. Dans ce tableau de bord, vous pouvez cliquer n'importe où dans le widget de groupe de récapitulatif d'état pour défiler vers le bas jusqu'à des tableaux de bord détaillés contenant des indicateurs clés de performance renvoyés depuis votre collecteur de données Bluemix Ruby.
- Un collecteur de données qui vient d'être démarré peut nécessiter un peu de temps pour communiquer avec l'infrastructure de surveillance et envoyer des indicateurs clés de performance à la console.

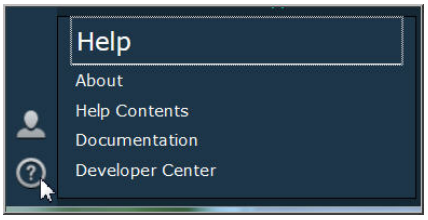


Résultats

Vous avez installé un collecteur de données Cloud APM et observé les données de surveillance envoyées au Tableau de bord d'Application Performance.

Que faire ensuite

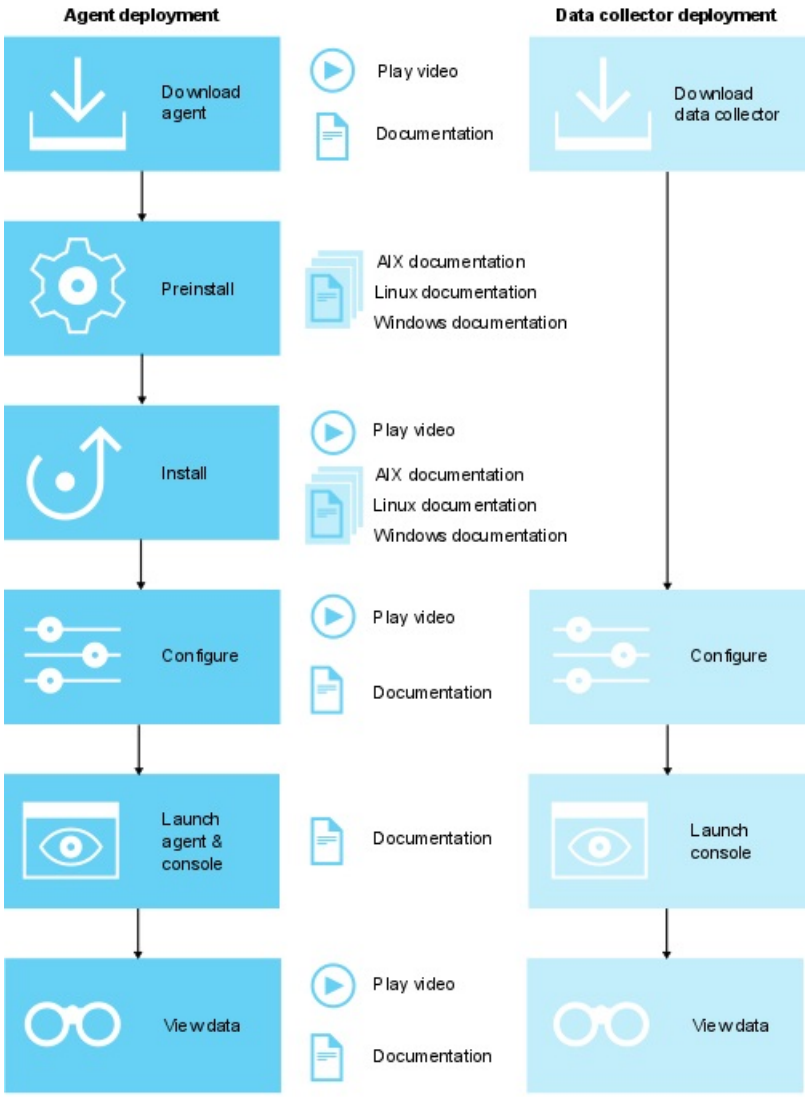
- Explorez la console : Pendant que vous utilisez la console Cloud APM, explorez ses fonctionnalités. Vous pouvez en savoir plus sur le tableau de bord en cours en cliquant sur dans la bannière de la fenêtre. Vous pouvez ouvrir le système d'aide ou l'ensemble de rubriques relatives à Cloud APM sur IBM Knowledge Center à partir du menu **Aide** dans la barre de navigation.



- Installez d'autres collecteurs de données : Vous disposez de tous les fichiers d'installation nécessaires pour installer d'autres types de collecteurs de données pour la surveillance de votre environnement. Vous pouvez également installer des collecteurs de données sur d'autres systèmes de votre environnement. Pour plus d'informations, voir Chapitre 7, «Configuration de votre environnement», à la page 163.

Chapitre 5. Déploiement d'agents et de collecteurs de données

Selon les agents, les tâches nécessaires entre l'installation et l'affichage des données qu'ils collectent varient. Certaines tâches sont automatiques, d'autres sont manuelles. Après avoir téléchargé vos collecteurs de données, vous devez configurer manuellement chaque collecteur de données.



1. Lire la vidéo de téléchargement
2. Télécharger la documentation
3. Documentation de préinstallation AIX
4. Documentation de préinstallation Linux
5. Documentation de préinstallation Windows
6. Lire la vidéo d'installation
7. Documentation d'installation AIX
8. Documentation d'installation Linux

9. Documentation d'installation Windows
10. Lire les vidéos de configuration
11. Documentation de configuration
12. Documentation de lancement
13. Lire la vidéo d'affichage des données
14. Documentation des fonctionnalités

1. Lire la vidéo de téléchargement
2. Télécharger la documentation
3. Documentation de préinstallation AIX
4. Documentation de préinstallation Linux
5. Documentation de préinstallation Windows
6. Lire la vidéo d'installation
7. Documentation d'installation AIX
8. Documentation d'installation Linux
9. Documentation d'installation Windows
10. Lire les vidéos de configuration
11. Documentation de configuration
12. Documentation de lancement
13. Lire la vidéo d'affichage des données
14. Documentation des fonctionnalités

Après l'installation, certains agents sont configurés et démarrés automatiquement
Tout agent démarré est configuré avec les paramètres par défaut. Pour déterminer quels agents sont configurés et démarrés manuellement, voir Tableau 7, à la page 117.

Après l'installation, certains agents nécessitent une configuration manuelle mais démarrent automatiquement
Pour plus d'informations sur la configuration de vos agents, voir Chapitre 7, «Configuration de votre environnement», à la page 163. Pour déterminer quels agents sont configurés manuellement et démarrés automatiquement, voir Tableau 7, à la page 117.

Après l'installation, certains agents doivent être configurés et démarrés manuellement
Tout agent qui n'est pas démarré automatiquement doit être configuré pour pouvoir être démarré. Pour déterminer quels agents sont configurés et démarrés manuellement, voir Tableau 7, à la page 117.

Les agents multi-instances nécessitent la création d'une première instance et un démarrage manuel
Vous devez créer la première instance et démarrer l'agent manuellement. Un agent multi-instance implique qu'une installation unique de l'agent instancie une instance de surveillance unique pour chaque instance d'application. Vous pouvez afficher ces instances depuis la console Cloud APM. Pour déterminer quels agents sont des agents multi-instances, voir Tableau 7, à la page 117.

Agents de système d'exploitation et surveillance des fichiers journaux
L'Linux OS, l'Agent UNIX OS et l'agent Windows OS sont configurés et démarrés automatiquement. Toutefois, vous pouvez configurer la surveillance des fichiers journaux pour les agents de système d'exploitation afin de pouvoir surveiller les fichiers journaux d'application. Pour plus d'informations, voir «Configuration de la surveillance des fichiers journaux de l'agent de système d'exploitation», à la page 649.

Déploiement d'agents d'agent et de collecteur de données

Tableau 7. Liste de contrôle post-installation

Déploiement d'agents ou collecteur de données	Configuré et démarré automatiquement	Configuré manuellement et démarré automatiquement	Configuré et démarré manuellement	Multi-instance (démarré manuellement)
agent Amazon EC2	—	—	—	✓
agent Amazon ELB	—	—	—	✓
Agent Azure Compute	—	—	—	✓
agent Cassandra	—	—	✓	✓
agent Cisco UCS	—	—	✓	✓
agent Citrix VDI	—	—	—	✓
agent DataPower	—	—	—	✓
agent DataStage	—	—	✓	✓
agent Db2	—	—	—	✓
agent Hadoop	—	—	✓	—
agent HMC Base	—	—	—	✓
agent HTTP Server	✓ Vous devez vérifier le fichier de configuration créé par l'agent pour le serveur HTTP. Vous devez ensuite ajouter manuellement la configuration du collecteur de données au fichier de configuration du serveur.	—	—	—
agent IBM Cloud	—	—	—	✓
agent IBM Integration Bus	—	—	—	✓
collecteur de données J2SE	—	✓	—	—
agent JBoss	—	—	—	✓
collecteur de données Liberty	—	✓	—	—
agent Linux KVM	—	—	✓	✓
Linux OS	✓	—	—	—

Tableau 7. Liste de contrôle post-installation (suite)

Déploiement d'agents ou collecteur de données	Configuré et démarré automatiquement	Configuré manuellement et démarré automatiquement	Configuré et démarré manuellement	Multi-instance (démarré manuellement)
agent Microsoft Active Directory	–	✓ Cet agent est démarré automatiquement. Vous devez cependant le configurer pour afficher les données de certains attributs.	–	–
agent Microsoft Cluster Server	–	–	✓	–
agent Microsoft Exchange Server	–	✓ Cet agent est démarré automatiquement. Vous devez cependant le configurer pour afficher les données de tous les attributs.	–	–
agent Microsoft Hyper-V Server	✓	–	–	–
agent Microsoft IIS	✓	–	–	–
Agent Skype for Business Server (anciennement agent Microsoft Lync Server)	✓	✓ Cet agent est démarré automatiquement. Vous devez cependant le configurer pour afficher les données de certains attributs.	–	–
agent Microsoft Office 365	–	–	✓	–

Tableau 7. Liste de contrôle post-installation (suite)

Déploiement d'agents ou collecteur de données	Configuré et démarré automatiquement	Configuré manuellement et démarré automatiquement	Configuré et démarré manuellement	Multi-instance (démarré manuellement)
agent Microsoft .NET	—	✓ Le collecteur de données doit être configuré avant le signalement des données.	—	—
agent MicrosoftSharePoint Server	✓	—	—	—
agent Microsoft SQL Server	—	—	—	✓ Chaque instance d'agent doit être configurée et démarrée manuellement.
Agent MQ Appliance	—	—	—	✓
Agent MongoDB	—	—	—	✓
Agent MySQL	—	—	—	✓
agent NetApp Storage	—	—	✓	✓
Agent Node.js	—	✓ L'agent doit être configuré avant le signalement des données. Vous devez ajouter un plug-in de surveillance à votre application Node.js.	—	—
collecteur de données Node.js	—	✓	—	—
Agent OpenStack	—	—	✓	✓
Agent Oracle Database	—	—	—	✓
Agent PHP	—	—	—	✓
Agent PostgreSQL	—	—	—	✓
collecteur de données Python	—	✓	—	—

Tableau 7. Liste de contrôle post-installation (suite)

Déploiement d'agents ou collecteur de données	Configuré et démarré automatiquement	Configuré manuellement et démarré automatiquement	Configuré et démarré manuellement	Multi-instance (démarré manuellement)
agent RabbitMQ	–	–	✓	✓
Agent de surveillance des temps de réponse	✓	–	–	–
Agent Ruby	–	–	–	✓ Pour des diagnostics approfondis, l'agent doit être configuré avant le signalement des données. Pour activer les tableaux de bord de diagnostic, vous devez installer et configurer le collecteur des données de diagnostic.
collecteur de données Ruby	–	✓	–	–
Agent SAP	–	–	✓	✓
Agent SAP HANA Database	–	–	✓	✓
Agent SAP NetWeaver Java Stack	–	–	✓	✓
agent Siebel	–	–	–	✓
Agent Sterling Connect Direct	–	–	–	✓
Agent Sterling File Gateway	–	–	✓	✓
agent Sybase	–	–	✓	✓

Tableau 7. Liste de contrôle post-installation (suite)

Déploiement d'agents ou collecteur de données	Configuré et démarré automatiquement	Configuré manuellement et démarré automatiquement	Configuré et démarré manuellement	Multi-instance (démarré manuellement)
Agent Synthetic Playback	✓ L'agent est configuré et démarré automatiquement pour les applications publiques externes mais les transactions doivent être créées dans Synthetic Script Manager avant la transmission des données.	✓ L'agent est démarré automatiquement mais l'agent doit être configuré pour des applications privées internes. Les transactions doivent être créées dans Synthetic Script Manager avant la transmission des données.	–	✓
Agent Tomcat	–	–	–	✓
Agent UNIX OS	✓	–	–	–
Agent VMware VI	–	–	✓	✓
Agent WebLogic	–	–	–	✓
Agent WebSphere Applications	–	✓ L'agent est démarré automatiquement mais le collecteur de données doit être configuré avant le signalement des données.	–	–
agent WebSphere Infrastructure Manager	–	–	–	✓
agent WebSphere MQ	–	–	–	✓
agent Windows OS	✓	–	–	–

Chapitre 6. Installation des agents

L'infrastructure IBM Cloud Application Performance Management est installée et gérée par IBM. Pour surveiller vos applications, sélectionnez et installez les agents de surveillance pour les applications que vous souhaitez surveiller. Vous pouvez installer les agents sur des systèmes d'exploitation Linux, AIX ou Windows. Les collecteurs de données autonomes ne requièrent pas d'installation.

Si vous choisissez des collecteurs de données autonomes pour surveiller vos applications, vous pouvez ignorer la procédure d'installation. Passez à la rubrique Chapitre 7, «Configuration de votre environnement», à la page 163 pour des instructions sur la manière de déployer les collecteurs de données pour la surveillance de vos applications.

Surveillance éloignée

Certains agents peuvent être installés à distance à partir de la ressource qu'ils surveillent. Les agents suivants prennent en charge la surveillance éloignée :

- Monitoring Agent for Amazon EC2
- Monitoring Agent for AWS Elastic Load Balancer
- Monitoring Agent for Azure Compute
- Monitoring Agent for Cassandra
- Monitoring Agent for Cisco UCS
- Monitoring Agent for Citrix Virtual Desktop Infrastructure
- Monitoring Agent for DataPower : cet agent ne peut être installé que sur un ordinateur distant.
- Monitoring Agent for Db2
- Monitoring Agent for Hadoop
- Monitoring Agent for HMC Base
- Monitoring Agent for IBM Cloud
- Monitoring Agent for InfoSphere DataStage
- Monitoring Agent for JBoss : si vous souhaitez utiliser cet agent pour la surveillance des ressources, installez-le à distance ou en local. Si vous souhaitez utiliser l'agent pour le suivi des transactions et les diagnostics Deep Dive, installez-le en local.
- Monitoring Agent for Linux KVM
- Monitoring Agent for MariaDB
- Monitoring Agent for Microsoft Cluster Server
- Monitoring Agent for Microsoft Exchange Server
- Monitoring Agent for Microsoft Office 365
- Monitoring Agent for Microsoft SharePoint Server
- Monitoring Agent for MongoDB
- Monitoring Agent for MySQL
- Monitoring Agent for NetApp Storage
- Monitoring Agent for OpenStack
- Monitoring Agent for Oracle Database
- Monitoring Agent for PostgreSQL
- Monitoring Agent for RabbitMQ
- Monitoring Agent for SAP Applications
- Monitoring Agent for SAP HANA Database

- Monitoring Agent for SAP NetWeaver Java Stack : si vous souhaitez utiliser cet agent pour la surveillance des ressources, installez-le à distance ou en local. Si vous souhaitez utiliser l'agent pour le suivi des transactions et les diagnostics Deep Dive, installez-le en local.
- Monitoring Agent for Sterling Connect Direct
- Monitoring Agent for Sterling File Gateway
- Monitoring Agent for VMware VI
- Monitoring Agent for WebLogic : si vous souhaitez utiliser cet agent pour la surveillance des ressources, installez-le à distance ou en local. Si vous souhaitez utiliser l'agent pour le suivi des transactions et les diagnostics Deep Dive, installez-le en local.
- Agent de surveillance des temps de réponse : si vous utilisez le composant Analyseur de paquet, installez l'agent à distance ou en local. Si vous utilisez le module Temps de réponse IBM HTTP Server, installez l'agent sur le même ordinateur que celui de HTTP Server.

Installation des agents sur les systèmes UNIX

Installez les agents de surveillance sur vos systèmes AIX ou Solaris pour les ressources que vous souhaitez gérer.

Liste des agents pouvant être installés sous AIX

- Monitoring Agent for DataPower
- Monitoring Agent for Cassandra
- Monitoring Agent for Db2
- Monitoring Agent for Hadoop
- Monitoring Agent for HMC Base
- Monitoring Agent for HTTP Server
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for MQ Appliance
- Monitoring Agent for Oracle Database
- Monitoring Agent for SAP Applications
- Monitoring Agent for SAP HANA Database
- Monitoring Agent for SAP NetWeaver Java Stack
- Monitoring Agent for Siebel
- Monitoring Agent for Sybase Server
- Monitoring Agent for UNIX OS
- Monitoring Agent for WebLogic
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ
- Agent de surveillance des temps de réponse

Liste des agents pouvant être installés sous SolariS Sparc

- Monitoring Agent for Db2
- Monitoring Agent for HTTP Server
- Monitoring Agent for JBoss
- Monitoring Agent for MySQL
- Monitoring Agent for Oracle Database
- Monitoring Agent for SAP Applications

- Monitoring Agent for Sybase Server
- Monitoring Agent for UNIX OS
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebLogic

Liste des agents pouvant être installés sous SolariS X86

- Monitoring Agent for Db2
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for SAP Applications
- Monitoring Agent for Sybase Server
- Monitoring Agent for UNIX OS
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ

Préinstallation sur les systèmes AIX

Vous devez effectuer les tâches de préinstallation requises avant d'installer les agents sur les systèmes AIX. Certaines tâches de préinstallation sont spécifiques à un agent et d'autres tâches s'appliquent à plusieurs agents.

Remarque : Ces exigences viennent s'ajouter aux exigences identifiées dans les rapports sur la compatibilité du produit logiciel.

Pour obtenir la configuration requise pour la version actuelle et les dépendances pour votre agent, voir System requirements (APM Developer Center) qui fournit un lien vers les rapports sur la compatibilité du produit logiciel.

Tous les agents

Les tâches de préinstallation suivantes s'appliquent à tous les agents :

Tester la connectivité
Avant d'installer les agents, vérifiez que votre système puisse communiquer avec le serveur Cloud APM. Pour plus d'informations sur la vérification de la connectivité au serveur Cloud APM, voir Communication sécurisée.

Installation en tant qu'utilisateur non superutilisateur
Vous devez disposer des droits d'écriture, de lecture et d'exécution sur le répertoire d'installation. Autrement, l'installation est annulée. Pour plus d'informations sur l'installation en tant qu'utilisateur non superutilisateur, voir «Installation des agents en tant qu'utilisateur non superutilisateur», à la page 145.

Limitation à 70 caractères pour le chemin d'installation
Le répertoire d'installation et son chemin d'accès ne doivent pas comporter plus de 70 caractères.

Limitation à 100 caractères des noms de fichier `.tar`
La commande par défaut **`tar`** sur des systèmes AIX ne peut pas traiter les noms de fichiers comportant plus de 100 caractères. Pour éviter les problèmes d'installation, procédez comme suit :

1. Téléchargez et installez la version GNU de la commande **`tar`** à partir du site Web AIX Toolbox for Linux Applications.
2. Faites de la version GNU votre commande **`tar`** par défaut. Effectuez l'une des étapes suivantes :
   - Ajoutez `/opt/freeware/bin` au début de la variable d'environnement *PATH* en cours. Exemple :

     ```
     export PATH=/opt/freeware/bin:$PATH
     ```

     où /opt/freeware/bin correspond au répertoire de GUN bin.

- Remplacez `/bin/tar` par un lien symbolique vers `/opt/freeware/bin/tar`, comme indiqué ci-dessous :

```
ln -s /opt/freeware/bin/tar /bin/tar
```

Sinon, effectuez une mise à niveau vers la dernière version d'AIX pour recevoir le correctif du code pour les noms de fichier comportant plus de 100 caractères. Pour plus de détails, voir la note technique relative à la commande TAR pour AIX V6.1 ou la note technique relative à la commande TAR pour AIX V7.1.

Définition de la variable d'environnement *CANDLEHOME*

Si vous avez utilisé ITM Agent Converter pour installer et configurer un agent sur le même système géré qu'auparavant, la variable d'environnement *CANDLEHOME* s'est vue affecter ce répertoire lorsque vous avez installé l'agent avec Agent Converter. Avant d'installer et de configurer un agent Cloud APM natif, vous devez affecter à la variable d'environnement *CANDLEHOME* un autre répertoire, faute de quoi l'agent Cloud APM natif ne peut pas démarrer.

Agents spécifiques

Les tâches de préinstallation suivantes s'appliquent aux agents spécifiés :

agent DataPower

Avant l'installation de l'agent, le programme de vérification des prérequis vérifie que le paramètre *ulimit* correspond à **unlimited** sous AIX. Vous devez exécuter la commande **ulimit -d unlimited** pour vous assurer que la variable d'environnement système *max data segment size* est définie sur **unlimited**. Cet agent ne peut pas être installé sur la même machine que le dispositif DataPower à surveiller.

agent HMC Base

Si vous prévoyez d'installer l'agent en tant que superutilisateur, vous devez vous assurer que le système TL07 est installé. Si vous prévoyez d'installer l'agent en tant qu'utilisateur non superutilisateur, vous devez vous assurer que le système TL08 est installé pour AIX version 6 uniquement.

agent HTTP Server

Installez et exécutez cet agent en tant que superutilisateur. Utilisez le même ID utilisateur pour installer et exécuter l'agent. Si vous installez et exécutez l'agent en tant qu'utilisateur non superutilisateur, ce dernier doit avoir le même ID utilisateur que l'utilisateur qui a démarré IBM HTTP Server. Sinon, l'agent a des difficultés à reconnaître IBM HTTP Server.

L'installation échoue sous AIX car la commande **.tar** par défaut tronque les chemins longs sur le système AIX. Pour plus d'informations, consultez la section "Limitation à 100 caractères pour les noms de fichier `.tar`" dans la présente rubrique.

AIX uniquement : installez l'utilitaire lynx ou l'application curl.

Agent Oracle Database

Sous Red Hat Enterprise Linux version 5 et version 6 et SUSE Linux Enterprise Server version 11 et version 12 x64, si l'Agent Oracle Database surveille la base de données Oracle à distance, vous devez commencer par installer les clients Oracle Instant. Installez les clients Oracle Instant à partir de la page Téléchargements Oracle Technology Network - Instant Client.

Les clients Instant v10.x ,v11.x et v12.x sont pris en charge par l'Agent Oracle Database.

Agent de surveillance des temps de réponse

Avant d'installer l'Agent de surveillance des temps de réponse, passez en revue la section relative à la planification de l'installation ici : «Planification de l'installation », à la page 706.

Agent SAP HANA Database

1. Installez le client de base de données SAP HANA HDBSQL version 1.00.102.06 ou ultérieure sur le système AIX.
2. Exécutez la commande suivante pour ajouter le chemin du répertoire d'installation à la variable d'environnement **LIBPATH**.

`export LIBPATH=$LIBPATH:`*`chemin_répertoire_install`*

Exemple : `export LIBPATH=$LIBPATH:/usr/sap/hdbclient`, où `/usr/sap/hdbclient` indique le chemin d'installation du client de base de données SAP HANA.

Important :

Si le chemin d'installation du client de base de données SAP HANA n'est pas ajouté à la variable d'environnement **LIBPATH** le scanner de prérequis renvoie le résultat `FAIL`.

La variable d'environnement que vous avez ajoutée à l'aide de la commande export est conservée uniquement pour une session donnée du terminal. Par conséquent, assurez-vous d'avoir exécuté le script d'installation de l'agent depuis le même terminal que celui utilisé pour ajouter la variable d'environnement.

Agent WebSphere Applications
Avant l'installation de l'agent, le programme de vérification des prérequis vérifie que le paramètre *ulimit* est défini sur **524000** sur le système AIX. Vous devez exécuter la commande **ulimit -d 524000** pour vous assurer que la variable d'environnement système *max data segment size* est définie sur **524000**.

Préinstallation sur les systèmes Solaris

Vous devez effectuer les tâches de préinstallation requises avant d'installer les agents sur les systèmes Solaris. Certaines tâches de préinstallation sont spécifiques à un agent et d'autres tâches s'appliquent à plusieurs agents.

Remarque : Ces exigences viennent s'ajouter aux exigences identifiées dans les rapports sur la compatibilité du produit logiciel.

Pour obtenir la configuration requise pour la version actuelle et les dépendances pour votre agent, voir System requirements (APM Developer Center) qui fournit un lien vers les rapports sur la compatibilité du produit logiciel.

Tous les agents

Les tâches de préinstallation suivantes s'appliquent à tous les agents :

Tester la connectivité
Avant d'installer les agents, vérifiez que votre système puisse communiquer avec le serveur Cloud APM. Pour plus d'informations sur la vérification de la connectivité au serveur Cloud APM, voir Communication sécurisée.

Installation en tant qu'utilisateur non superutilisateur
Vous devez disposer des droits d'écriture, de lecture et d'exécution sur le répertoire d'installation. Autrement, l'installation est annulée. Pour plus d'informations sur l'installation en tant qu'utilisateur non superutilisateur, voir «Installation des agents en tant qu'utilisateur non superutilisateur», à la page 145.

Limitation à 70 caractères pour le chemin d'installation
Le répertoire d'installation et son chemin d'accès ne doivent pas comporter plus de 70 caractères.

Limitation à 100 caractères des noms de fichier `.tar`
La commande par défaut **tar** sur les systèmes Solaris ne peut pas traiter les noms de fichiers comportant plus de 100 caractères. Pour éviter les erreurs @LongLink, procédez comme suit :

1. Téléchargez et installez la version GNU de la commande **tar** à partir du site Web http://www.gnu.org.
2. Faites de la version GNU votre commande **tar** par défaut. Effectuez l'une des étapes suivantes :
   - Dans la variable d'environnement *PATH*, insérez d'abord la variable suivante :

     ```
     export PATH=/opt/freeware/bin:$PATH
     ```

   - Remplacez `/bin/tar` par le lien symbolique vers `/opt/freeware/bin/tar`

Définition de la variable d'environnement *CANDLEHOME*

Si vous avez utilisé ITM Agent Converter pour installer et configurer un agent sur le même système géré qu'auparavant, la variable d'environnement *CANDLEHOME* s'est vue affecter ce répertoire lorsque vous avez installé l'agent avec Agent Converter. Avant d'installer et de configurer un agent Cloud APM natif, vous devez affecter à la variable d'environnement *CANDLEHOME* un autre répertoire, faute de quoi l'agent Cloud APM natif ne peut pas démarrer.

Agents spécifiques

Les tâches de préinstallation suivantes s'appliquent aux agents spécifiés :

agent HTTP Server

Installez et exécutez cet agent en tant que superutilisateur. Utilisez le même ID utilisateur pour installer et exécuter l'agent. Si vous installez et exécutez l'agent en tant qu'utilisateur non superutilisateur, ce dernier doit avoir le même ID utilisateur que l'utilisateur qui a démarré IBM HTTP Server. Sinon, l'agent a des difficultés à reconnaître IBM HTTP Server.

Installation d'agents

Vous pouvez installer toute combinaison des agents de surveillance sur un système géré. Par exemple, si vous installez l'Agent Ruby pour surveiller les applications Ruby On Rails, vous souhaiterez peut-être également installer l'Agent de surveillance des temps de réponse et/ou l'Linux OS. Grâce à l'Agent de surveillance des temps de réponse, vous pouvez regrouper davantage d'informations sur les temps de réponse pour vos applications Ruby. Grâce à l'Linux OS, vous pouvez surveiller d'autres aspects du système, tels que l'unité centrale, la mémoire et le disque.

L'offre détermine les agents de surveillance pouvant être installés. Pour obtenir la liste des agents compris dans chaque offre, voir «Fonctions», à la page 55.

Pour obtenir la liste des agents qui s'exécutent sur les systèmes AIX et Solaris, voir «Installation des agents sur les systèmes UNIX», à la page 124.

Avant de commencer

Téléchargez les agents. Voir «Téléchargement de vos agents et de vos collecteurs de données», à la page 105.

Lisez les informations de la section «Configuration requise», à la page 85 afin de vous assurer que vous répondez aux exigences liées aux agents que vous prévoyez d'installer.

Passez en revue les tâches de pré-installation des agents avant d'installer ces derniers.

- Pour les systèmes AIX, voir «Préinstallation sur les systèmes AIX», à la page 125.
- Pour les systèmes Solaris, voir «Préinstallation sur les systèmes Solaris», à la page 127.

Important : Java Runtime est installé uniquement lorsque l'agent le requiert et il n'est pas toujours disponible. En outre, ksh n'est plus requis pour l'installation des agents et SELinux en mode d'application est pris en charge.

Pourquoi et quand exécuter cette tâche

Vous pouvez installer des agents de surveillance en tant que superutilisateur ou utilisateur non superutilisateur. Si vous ne disposez pas des privilèges de superutilisateur et que vous souhaitez installer un agent de surveillance, vous pouvez installer l'agent en tant qu'utilisateur non superutilisateur (voir «Installation des agents en tant qu'utilisateur non superutilisateur», à la page 145). En outre, vous ne pouvez pas installer l'agent en tant qu'utilisateur non superutilisateur si vous êtes administrateur d'hôte et que vous ne souhaitez pas exécuter l'agent de surveillance comme superutilisateur. Le flux d'installation est le même que pour un superutilisateur.

La coexistence des agents est prise en charge. Vous pouvez installer les agents IBM Cloud Application Performance Management sur le même ordinateur que les agents IBM Tivoli Monitoring. Cependant, les deux types d'agent ne peuvent pas être installés dans le même répertoire. Pour plus d'informations sur la

coexistence des agents, voir «Coexistence de l'agent Cloud APM et de l'agent Tivoli Monitoring», à la page 976.

Procédure

1. Ouvrez une session shell de terminal sur le système AIX ou Solaris.
2. Sur votre système, accédez au répertoire dans lequel vous avez téléchargé le fichier .tar.

   Les agents doivent être installés sur le système sur lequel l'application que vous voulez surveiller est installée. Si nécessaire, transférez le fichier archive d'installation sur le système à surveiller. Le fichier archive contient les agents et le script d'installation.

   A faire : Vérifiez que le répertoire ne contient pas une ancienne version du fichier d'archive.
3. Procédez à l'extraction des fichiers d'installation à l'aide de la commande suivante :

   ```
   tar -xf ./fichiers d'installation
   ```

   où *fichiers d'installation* est le nom du fichier d'installation correspondant à votre offre.

   Le script d'installation est extrait dans un répertoire nommé en fonction du fichier archive et de la version. Par exemple : *offre*_Agent_Install_8.1.4.0. Les fichiers binaires de l'agent et les fichiers liés à la configuration sont extraits dans des sous-répertoires de ce répertoire.
4. Facultatif : Cette étape est obligatoire UNIQUEMENT pour Solaris 10. Vous devez créer un lien lointain à ksh avant d'exécuter le script d'installation sous Solaris 10.
   a) Sauvegardez la commande /bin/sh :

   ```
   mv /bin/sh /bin/sh.bkup_origin
   ```

   b) Créez un lien lointain à la commande ksh :

   ```
   ln -s /bin/ksh /bin/sh
   ```

   c) Confirmez que le résultat pointe vers ksh :

   ```
   ls -l /bin/sh
   ```
5. Exécutez le script d'installation à partir du répertoire nommé en fonction du fichier archive et de la version :

   ```
   ./installAPMAgents.sh
   ```

   Pour installer les agents en mode silencieux, voir «Installation des agents en mode silencieux», à la page 147.
6. Indiquez si vous souhaitez installer des agents individuels, une combinaison d'agents ou tous les agents.
7. Selon que vous installez ou mettez à niveau les agents, effectuez l'une des étapes suivantes :
   - Si vous installez les agents, spécifiez un autre répertoire de base d'installation d'agent ou utilisez le répertoire par défaut applicable :
     - /opt/ibm/apm/agent
   - Si vous mettez à niveau les agents, entrez le répertoire d'installation de la version précédente des agents à l'invite du répertoire de base d'installation des agents.
8. Lorsque vous êtes invité à accepter le contrat de licence, entrez 1 pour l'accepter et continuer ou 2 pour refuser.

   Après avoir saisi 1 (accepter), l'analyse des prérequis de votre environnement commence et prend un certain moment. Si des exigences ne sont pas satisfaites, un message vous dirige vers un fichier journal contenant la raison de l'échec. Si un prérequis est manquant (par exemple, bibliothèque manquante ou espace disque insuffisant), l'installation s'arrête. Vous devez corriger l'incident, et relancer le script d'installation.

9. Si vous avez installé les agents à l'aide d'un ID utilisateur non superutilisateur, vous devez mettre à jour les scripts de démarrage du système (voir «Installation des agents en tant qu'utilisateur non superutilisateur», à la page 145).
10. Une fois l'installation terminée et la ligne de commande disponible, vous pouvez répéter les étapes de cette procédure pour installer plus d'agents de surveillance sur le système géré.

Que faire ensuite

Configurez l'agent en fonction de vos besoins. Si votre agent de surveillance requiert des opérations de configuration comme indiqué dans Chapitre 5, «Déploiement d'agents et de collecteurs de données», à la page 115 ou si vous voulez consulter les paramètres par défaut, voir Chapitre 7, «Configuration de votre environnement», à la page 163.

- Si vous utilisez un proxy direct étant donné que votre pare-feu n'autorise pas les connexions HTTPS sortantes transparentes aux hôtes externes, vous devez éditer le fichier de configuration d'environnement de l'agent. Pour obtenir des instructions, voir «Configuration des agents pour qu'ils communiquent via un proxy direct», à la page 163.
- Si vous avez mis à niveau un agent d'une version précédente, identifiez les éventuelles tâches de reconfiguration ou de migration à effectuer avant de vous connecter à la console Cloud APM. Pour plus d'informations sur ces tâches, voir «Mise à niveau de vos agents», à la page 1171. Après une mise à niveau, vous devez redémarrer tous les agents qui ne sont pas automatiquement configurés et démarrés par le programme d'installation.

Pour démarrer un agent, exécutez la commande suivante :

```
./nom-agent.sh start
```

Pour plus d'informations sur les commandes de l'agent de surveillance, y compris le *nom* à utiliser, voir «Utilisation des commandes de l'agent», à la page 181. Pour plus d'informations concernant les agents démarrés automatiquement et manuellement, voir Chapitre 5, «Déploiement d'agents et de collecteurs de données», à la page 115.

Après une mise à niveau, vous devez redémarrer tous les agents qui ne sont pas automatiquement configurés et démarrés par le programme d'installation.

Après avoir configuré et démarré l'agent, affichez les données que l'agent collecte.

- Si vous n'êtes pas connecté, suivez les instructions figurant dans «Démarrage de la console Cloud APM», à la page 1003.
- Si vous voulez afficher les systèmes gérés de votre domaine IBM Tivoli Monitoring dans les Tableau de bord d'Application Performance, effectuez les tâches décrites dans «Intégration à IBM Tivoli Monitoring V6.3 », à la page 975.

Installation des agents sur les systèmes Linux

Installez les agents de surveillance sur vos systèmes Linux pour les ressources que vous souhaitez gérer.

- Monitoring Agent for Amazon EC2
- Monitoring Agent for AWS Elastic Load Balancer
- Monitoring Agent for Azure Compute
- Monitoring Agent for Cassandra
- Monitoring Agent for Cisco UCS
- Monitoring Agent for Citrix Virtual Desktop Infrastructure
- Monitoring Agent for DataPower
- Monitoring Agent for Db2
- Monitoring Agent for Hadoop

- Monitoring Agent for HTTP Server
- Monitoring Agent for IBM Cloud
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for Internet Services
- Monitoring Agent for MQ Appliance
- Monitoring Agent for InfoSphere DataStage
- Monitoring Agent for JBoss
- Monitoring Agent for Linux OS
- Monitoring Agent for Linux KVM
- Monitoring Agent for MariaDB
- Monitoring Agent for Microsoft SQL Server
- Monitoring Agent for MongoDB
- Monitoring Agent for MySQL
- Monitoring Agent for NetApp Storage
- Monitoring Agent for Node.js
- Monitoring Agent for OpenStack
- Monitoring Agent for Oracle Database
- Monitoring Agent for PHP
- Monitoring Agent for PostgreSQL
- Monitoring Agent for RabbitMQ
- Monitoring Agent for Ruby
- Monitoring Agent for SAP Applications
- Monitoring Agent for SAP HANA Database
- Monitoring Agent for SAP NetWeaver Java Stack
- Monitoring Agent for Siebel
- Monitoring Agent for Sterling Connect Direct
- Monitoring Agent for Sterling File Gateway
- Monitoring Agent for Sybase Server
- Monitoring Agent for Synthetic Playback
- Monitoring Agent for Tomcat
- Monitoring Agent for VMware VI
- Monitoring Agent for WebLogic
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere Infrastructure Manager
- Monitoring Agent for WebSphere MQ
- Agent de surveillance des temps de réponse

Les agents suivants sont pris en charge sous Linux sur les systèmes Power Little Endian (pLinux LE) :

- Monitoring Agent for Db2
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for Linux OS
- Monitoring Agent for Tomcat - La prise en charge est disponible pour la surveillance des ressources.
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ

Les agents suivants sont pris en charge sur les systèmes Linux for System z :

- Monitoring Agent for Db2
- Monitoring Agent for HTTP Server - Le suivi des transactions n'est pas pris en charge.
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for Linux OS
- Agent de surveillance des temps de réponse
- Monitoring Agent for Tomcat
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ

L'agent suivant est pris en charge sur les systèmes Linux for System x :

- Monitoring Agent for HTTP Server - Le suivi des transactions n'est pas pris en charge.

Préinstallation sur les systèmes Linux

Vous devez effectuer les tâches de préinstallation requises avant d'installer les agents sur les systèmes Linux. Certaines tâches de préinstallation sont spécifiques à un agent et d'autres tâches s'appliquent à plusieurs agents.

Remarque : Ces exigences viennent s'ajouter à celles identifiées dans les rapports sur la compatibilité du produit logiciel.

Pour obtenir la configuration requise pour la version actuelle et les dépendances pour votre agent, voir System requirements (APM Developer Center) qui fournit un lien vers les rapports sur la compatibilité du produit logiciel.

Tous les agents

Les tâches de préinstallation suivantes s'appliquent à tous les agents :

Tester la connectivité
Avant d'installer les agents, vérifiez que votre système puisse communiquer avec le serveur Cloud APM. Pour plus d'informations sur la vérification de la connectivité au serveur Cloud APM, voir Communication sécurisée.

Installation en tant qu'utilisateur non superutilisateur
Vous devez disposer des droits d'écriture, de lecture et d'exécution sur le répertoire d'installation. Autrement, l'installation est annulée. Pour plus d'informations sur l'installation en tant qu'utilisateur non superutilisateur, voir «Installation des agents en tant qu'utilisateur non superutilisateur», à la page 145.

Limitation à 70 caractères pour le chemin d'installation
Le répertoire d'installation et son chemin d'accès ne doivent pas comporter plus de 70 caractères.

Définition de la variable d'environnement *CANDLEHOME*
Si vous avez utilisé ITM Agent Converter pour installer et configurer un agent sur le même système géré qu'auparavant, la variable d'environnement *CANDLEHOME* s'est vue affecter ce répertoire lorsque vous avez installé l'agent avec Agent Converter. Avant d'installer et de configurer un agent Cloud APM natif, vous devez affecter à la variable d'environnement *CANDLEHOME* un autre répertoire, faute de quoi l'agent Cloud APM natif ne peut pas démarrer.

Systèmes d'exploitation spécifiques

Red Hat Enterprise Linux (RHEL) 8

Le package libnsl.so.1 est nécessaire sur RHEL 8

Par défaut, `libnsl.so.1` n'est pas installé sur Red Hat Enterprise Linux édition 8.0. Sans ce package, aucun agent ne peut être installé. Demandez à votre administrateur de configurer un référentiel YUM pour vous, puis exécutez cette commande :

```
yum install libnsl
```

Une fois l'installation terminée, vous pouvez voir `/usr/lib64/libnsl.so.1`.

Remarque : Le package `libnsl.so.1` est nécessaire uniquement pour les agents. Cette étape n'est pas nécessaire pour les collecteurs de données.

Contournement du scanner de prérequis pour certains agents

Vous pouvez ignorer le scanner de prérequis avant sa mise à jour en vue de sa compatibilité avec les dernières exigences. Pour en savoir plus sur les scénarios et les instructions appropriés, voir «Contournement de l'analyse des prérequis», à la page 149.

Remarque : Cette étape n'est pas nécessaire pour les collecteurs de données.

Agents spécifiques

Les tâches de préinstallation suivantes s'appliquent aux agents spécifiés :

agent DataPower
Vous devez exécuter la commande **`ulimit -d unlimited`** pour vous assurer que la variable d'environnement système *max data segment size* est définie sur **`unlimited`**. Cet agent ne peut pas être installé sur la même machine que le dispositif DataPower à surveiller.

agent DataStage

1. Activez les paramètres dans le fichier `DSODBConfig.cfg`. Effectuez les opérations suivantes :
   a. Ouvrez le fichier `DSODBConfig.cfg` dans un éditeur à la ligne suivante :

      ```
      infosphere_information_server_install_dir/Server/DSODB
      ```

   b. Supprimez la mise en commentaire des paramètres suivants en supprimant le symbole **#** :

      `MonitorLinks`=1
      `JobRunUsage`=1
      `ResourceMonitor`=1
      `DSODBON`=1

   c. Editez les valeurs des paramètres définis sur 1.
2. Copiez le pilote JDBC de la base de données utilisée pour la configuration du référentiel de métadonnées sur l'ordinateur agent.
   a. Entrez 4 pour le pilote JDBC 4 ou ultérieur. Exemple : `db2jcc4.jar`
   b. Entrez 4 pour le pilote JDBC pour Oracle. Exemple : `ojdbc6.jar`
   c. Pilote JDBC pour MS SQL :
      - `Sqljdbc41.jar` nécessite l'environnement d'exécution Java 7 et prend en charge l'API JDBC 4.1.
      - `Sqljdbc42.jar` nécessite l'environnement d'exécution Java 8 et prend en charge l'API JDBC 4.2.

agent HTTP Server
Si vous installez cet agent en tant que superutilisateur, vous devez utiliser le même ID utilisateur pour exécuter et configurer l'agent.

Si vous installez et exécutez l'agent en tant qu'utilisateur non root, ce dernier doit avoir le même ID utilisateur que l'utilisateur qui a démarré IBM HTTP Server. Sinon, l'agent a des difficultés à reconnaître IBM HTTP Server. Vous pouvez utiliser le même ID utilisateur pour exécuter et configurer l'agent.

agent Linux KVM

Monitoring Agent for Linux KVM est un agent multi-instance et multiconnexion qui prend en charge des connexions d'hyperviseur KVM basé sur Enterprise Linux et des environnements RHEV-M (Red Hat Enterprise Virtualization Manager). Vous pouvez créer plusieurs instances de cet agent pour surveiller plusieurs hyperviseurs dans un environnement d'hyperviseur RHEV-M ou KVM. Vous pouvez surveiller les charges de travail virtualisées et analyser la capacité de ressources sur des machines virtuelles différentes. Pour connecter l'agent à une machine virtuelle dans l'environnement de l'hyperviseur KVM, vous devez installer les conditions préalables requises : `libvirt*.rpm` et interpréteur de commandes Korn (pdksh). L'agent collecte des indicateurs en se connectant à distance à un hyperviseur libvirt qui gère les machines virtuelles.

agent Microsoft SQL Server

Pour surveiller un environnement Microsoft SQL, les pilotes Microsoft SQL Server et Microsoft SQL ODBC doivent être installés préalablement à l'installation de Monitoring Agent for Microsoft SQL Server. Par exemple, pour installer le pilote ODBC sur Red Hat Enterprise Linux, utilisez la commande suivante :

```
sudo yum install unixODBC
sudo yum install msodbcsql17
```

Pour exécuter le programme de vérification, l'agent doit être configuré sur Cloud Application Performance Management version 8.1.4.0 Server correctif provisoire 15 (8.1.4.0-IBM-APM-SERVER-IF0015.tar) ou version ultérieure.

Agent MongoDB

Vous devez installer et configurer l'Agent MongoDB sur le système sur lequel le serveur de base de données MongoDB est installé.

Agent MySQL

Pour surveiller un environnement MySQL, le serveur MySQL et le pilote MySQL JDBC doivent être installés avant d'installer Monitoring Agent for MySQL. Par exemple, pour installer le pilote JDBC sur Red Hat Enterprise Linux, utilisez la commande suivante :

```
yum install mysql-connector-java
```

Une fois que vous avez démarré l'installation de l'agent et au cours du contrôle des prérequis du nom de package MySQL, un avertissement peut être affiché si un fournisseur autre que Red Hat, tel qu'Oracle, est utilisé. Si MySQL Server et le pilote JDBC sont disponibles, cet avertissement n'entraîne pas l'échec de l'installation et vous pouvez ignorer le message. Exemple de sortie :

```
Scenario: Prerequisite Scan
KSE - Monitoring Agent for MySQL Prerequisite Checker [version 01000005]:
Property                              Result   Found
Expected
========                        ====== =====       ========
os.package.mysql-server         WARN  Unavailable  mysql-server-5.1.12+
os.package.mysql-connector-java WARN Unavailable mysql-connector-java-5.
1.12+
```

Agent Node.js

La version de Node.js que vous utilisez pour exécuter l'application surveillée doit être identique à la version installée par défaut.

Node.js v5 n'est actuellement pas pris en charge.

Agent OpenStack

Avant de pouvoir utiliser l'Agent OpenStack vous devez avoir les logiciels suivants sur le serveur où vous installez l'agent :

- Python 2.6.0, Python 2.7.0 ou une version ultérieure

- Clients OpenStack les plus récents :
  - OpenStack
  - Keystone
  - Neutron
  - Swift

  Pour installer les clients de ligne de commande OpenStack, voir Install the OpenStack command-line clients.
- Bibliothèque Paramiko pour l'accès à distance dans Python.

  Remarque : Si vous souhaitez installer l'Agent OpenStack sur un serveur RedHat Linux nettoyé, avant d'installer la bibliothèque Paramiko, exécutez la commande suivante pour installer le logiciel requis :

  ```
  wget https://ftp.dlitz.net/pub/dlitz/crypto/pycrypto/pycrypto-2.6.1.tar.gz
  yum install gcc/openssl-devel/libffi-devel
  ```
- Interpréteur de commandes Korn

Agent Oracle Database

Sous Red Hat Enterprise Linux version 5 et version 6 et SUSE Linux Enterprise Server version 11 et version 12 x64, si l'Agent Oracle Database surveille la base de données Oracle à distance, vous devez commencer par installer les clients Oracle Instant. Installez les clients Oracle Instant à partir de la page Téléchargements Oracle Technology Network - Instant Client.

Les clients Instant v10.x ,v11.x et v12.x sont pris en charge par l'Agent Oracle Database.

Agent PHP

Si l'application PHP est déployée à l'aide du superutilisateur, vous devez utiliser ce dernier pour installer, configurer, démarrer ou arrêter l'agent. Si l'application PHP est déployée à l'aide d'un utilisateur non superutilisateur, vous pouvez utiliser le superutilisateur ou le même utilisateur non superutilisateur pour installer, configurer, démarrer ou arrêter l'agent.

Une application WordPress existante doit être installée. L'Agent PHP surveille WordPress version 3.7.1 ou ultérieure.

L'agent évalue uniquement les performances des requêtes PHP dans les applications WordPress. Le chargement CSS et JS n'est pas évalué.

L'agent n'utilise pas les arguments d'URL pour identifier les URL.

collecteur de données Python

Le collecteur de données Python surveille les applications Django.

Agent de surveillance des temps de réponse

Avant d'installer l'Agent de surveillance des temps de réponse, passez en revue la section relative à la planification de l'installation ici : «Planification de l'installation », à la page 706.

Agent SAP HANA Database

1. Installez le client de base de données SAP HANA HDBSQL version 1.00.102.06 ou ultérieure sur le système Linux.

   Important : Pour le système d'exploitation 64 bits RHEL 5.x, installez Linux SUSE 9 sur le client de base de données SAP HANA x86_64 64 bits au lieu de Linux sur x86_64 64 bits. Pour RHEL 6.x ou les systèmes d'exploitation 64 bits ultérieurs, installez Linux sur le client de base de données SAP HANA x86_64 64 bits.
2. Exécutez la commande suivante pour ajouter le chemin du répertoire d'installation à la variable d'environnement **LD_LIBRARY_PATH** :

   `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:`*`chemin_répertoire_install`*

Exemple : `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/sap/hdbclient`, où `/usr/sap/hdbclient` indique le chemin d'installation du client de base de données SAP HANA.

Important :

Si le chemin d'installation du client de base de données SAP HANA n'est pas ajouté à la variable d'environnement **LD_LIBRARY_PATH**, le scanner de prérequis renvoie le résultat `FAIL`.

La variable d'environnement que vous avez ajoutée à l'aide de la commande export est conservée uniquement pour une session donnée du terminal. Par conséquent, assurez-vous d'avoir exécuté le script d'installation de l'agent depuis le même terminal que celui utilisé pour ajouter la variable d'environnement.

Agent Synthetic Playback

Pour installer l'Agent Synthetic Playback, l'utilisateur du système d'exploitation doit disposer des droits suivants :

- Activez le droit d'accès en lecture et exécution à l'image d'installation.
- Activez le droit d'accès en écriture à l'agent principal.

Pour exécuter l'Agent Synthetic Playback, l'utilisateur du système d'exploitation doit disposer des droits suivants :

- Activez le droit d'accès en lecture, écriture et exécution à l'emplacement d'installation de l'agent et à ses sous-répertoires et fichiers.
- Activez le droit d'exécution de Mozilla Firefox.
- Assurez-vous que les fichiers binaires d'exécution de Mozilla Firefox se trouvent dans la variable d'environnement PATH du profil de l'utilisateur.

Avant d'installer l'Agent Synthetic Playback, procédez comme suit :

1. Synchronisez les emplacements d'installation de l'agent avec la console Cloud APM.
2. Installez Mozilla Firefox et le serveur d'affichage Xvfb.
3. Vérifiez que le serveur d'affichage Xvfb fonctionne. Exécutez la commande suivante :

   ```
   # Xvfb -ac
   ```

   Aucune erreur ne devrait apparaître dans la sortie.
4. Vérifiez que le processus Xvfb est en cours. Exécutez la commande suivante :

   ```
   # ps -ef|grep Xvfb
   ```

   Exemple de sortie :

   ```
   root 7192 1 0 Jan14 ? 00:00:14 Xvfb -ac
   root 20393 17900 0 02:05 pts/0 00:00:00 grep -i xvfb
   ```
5. Arrêtez le processus Xvfb. Exécutez la commande suivante :

   ```
   # kill -9 7192
   ```
6. Accédez à *rép_install*`/etc/hosts` et éditez le début du fichier hosts de sorte à inclure les paramètres suivants :

   ```
   127.0.0.1 localhost
   ```

   Ensuite, sauvegardez et fermez le fichier hosts.

Agent WebSphere Applications

Avant l'installation de l'agent, le programme de vérification des prérequis vérifie que le paramètre *ulimit* est défini sur **524000** sur le système Linux. Vous devez exécuter la commande **ulimit -d**

524000 pour vous assurer que la variable d'environnement système *max data segment size* est définie sur **524000**.

Installation d'agents

Vous pouvez installer toute combinaison des agents de surveillance sur un système géré. Par exemple, si vous installez l'Agent Ruby pour surveiller les applications Ruby On Rails, vous souhaiterez peut-être également installer l'Agent de surveillance des temps de réponse et/ou l'Linux OS. Grâce à l'Agent de surveillance des temps de réponse, vous pouvez regrouper davantage d'informations sur les temps de réponse pour vos applications Ruby. Grâce à l'Linux OS, vous pouvez surveiller d'autres aspects du système, tels que l'unité centrale, la mémoire et le disque.

L'offre détermine les agents de surveillance pouvant être installés. Pour obtenir la liste des agents compris dans chaque offre, voir «Fonctions», à la page 55.

Pour obtenir la liste des agents qui s'exécutent sur les systèmes Linux, voir «Installation des agents sur les systèmes Linux», à la page 130.

Avant de commencer

Téléchargez les agents. Voir «Téléchargement de vos agents et de vos collecteurs de données», à la page 105.

Lisez les informations de la section «Configuration requise», à la page 85 afin de vous assurer que vous répondez aux exigences liées aux agents que vous prévoyez d'installer.

Passez en revue les tâches de pré-installation des agents avant d'installer ces derniers. Pour plus d'informations, voir «Préinstallation sur les systèmes Linux», à la page 132.

Remarque : Java Runtime est installé uniquement lorsque l'agent le requiert et il n'est pas toujours disponible. En outre, ksh n'est plus nécessaire dans le cadre de l'installation des agents, sauf en ce qui concerne l'Agent Summarization and Pruning, qui est installé lors de l'installation du serveur Cloud APM. SELinux en mode d'application n'est pas pris en charge.

Pourquoi et quand exécuter cette tâche

Vous pouvez installer des agents de surveillance en tant que superutilisateur ou utilisateur non superutilisateur. Si vous ne disposez pas des privilèges de superutilisateur et que vous souhaitez installer un agent de surveillance, vous pouvez installer l'agent en tant qu'utilisateur non superutilisateur (voir «Installation des agents en tant qu'utilisateur non superutilisateur», à la page 145). En outre, vous ne pouvez pas installer l'agent comme utilisateur non superutilisateur si vous êtes administrateur d'hôte et que vous ne souhaitez pas exécuter l'agent de surveillance comme superutilisateur. Le flux d'installation est le même que pour un superutilisateur.

La coexistence des agents est prise en charge. Vous pouvez installer les agents IBM Cloud Application Performance Management sur le même ordinateur que les agents IBM Tivoli Monitoring. Cependant, les deux types d'agent ne peuvent pas être installés dans le même répertoire. Pour plus d'informations sur la coexistence des agents, voir «Coexistence de l'agent Cloud APM et de l'agent Tivoli Monitoring», à la page 976.

Procédure

1. Ouvrez une session shell de terminal sur le système Red Hat Enterprise Linux.
2. Sur votre système, accédez au répertoire dans lequel vous avez téléchargé le fichier .tar

   Les agents doivent être installés sur le système sur lequel l'application que vous voulez surveiller est installée. Si nécessaire, transférez le fichier archive d'installation sur le système à surveiller. Le fichier archive contient les agents et le script d'installation.

   A faire : Vérifiez que le répertoire ne contient pas une ancienne version du fichier d'archive.
3. Extrayez les fichiers d'installation de l' en utilisant les commandes suivantes, qui dépendent de votre offre :

```
tar -xf ./fichiers d'installation.tar
```

où *fichiers d'installation* est le nom du fichier d'installation correspondant à votre offre.

Le script d'installation est extrait dans un répertoire nommé en fonction du fichier archive et de la version. Par exemple : *offre*_Agent_Install_8.1.4.0. Les fichiers binaires de l'agent et les fichiers liés à la configuration sont extraits dans des sous-répertoires de ce répertoire.

4. Exécutez le script d'installation à partir du répertoire nommé en fonction du fichier archive et de la version :

```
./installAPMAgents.sh
```

Pour installer les agents en mode silencieux, voir «Installation des agents en mode silencieux», à la page 147.

5. Indiquez si vous souhaitez installer des agents individuels, une combinaison d'agents ou tous les agents.
6. Selon que vous installez ou mettez à niveau les agents, effectuez l'une des étapes suivantes :
   - Si vous installez les agents, spécifiez un autre répertoire de base d'installation d'agent ou utilisez le répertoire par défaut applicable :
     – /opt/ibm/apm/agent
   - Si vous mettez à niveau les agents, entrez le répertoire d'installation de la version précédente des agents à l'invite du répertoire de base d'installation des agents.
     a. S'il existe une ancienne version des agents dans le répertoire /opt/ibm/apm/agent, vous devez spécifier un nouveau répertoire d'installation. A l'étape suivante, le système vous demande si vous souhaitez migrer la configuration d'agent à partir du répertoire /opt/ibm/apm/agent.
     b. Si vous confirmez vouloir migrer la configuration d'agent de l'ancien répertoire d'installation (/opt/ibm/ccm/agent) vers le nouveau répertoire d'installation (par exemple, /opt/ibm/apm/agent), vous devez démarrer l'agent dans le nouvel emplacement d'installation.

        Restriction : L'ancienne version de l'agent est arrêtée automatiquement dans l'ancien emplacement d'installation, mais elle n'est pas démarrée automatiquement dans le nouvel emplacement d'installation.
     c. Une fois que l'installation est terminée et que vous avez vérifié que l'agent fonctionne dans le nouveau répertoire d'installation, vous devez désinstaller l'ancienne version de l'agent du répertoire /opt/ibm/ccm/agent. Si vous souhaitez supprimer tous les agents, exécutez la commande **/opt/ibm/ccm/agent/bin/smai-agent.sh uninstall_all**.
7. Lorsque vous êtes invité à accepter le contrat de licence, entrez 1 pour l'accepter et continuer ou 2 pour refuser.

   Après avoir saisi 1 (accepter), l'analyse des prérequis de votre environnement commence et prend un certain moment. Si des exigences ne sont pas satisfaites, un message vous dirige vers un fichier journal contenant la raison de l'échec. Si un prérequis est manquant (par exemple, bibliothèque manquante ou espace disque insuffisant), l'installation s'arrête. Vous devez corriger l'incident, et relancer le script d'installation.

   Remarque : Si l'installation s'arrête avec le message ci-après, vérifiez si le service du serveur est démarré (Démarrer -> Outils d'administration -> Services). S'il ne l'est pas, démarrez-le, puis exécutez à nouveau installAPMAgents.bat.

```
This script [installAPMAgents.bat] must be run as Administrator.
```

8. Si vous avez installé les agents à l'aide d'un ID utilisateur non superutilisateur, vous devez mettre à jour les scripts de démarrage du système (voir «Installation des agents en tant qu'utilisateur non superutilisateur», à la page 145).

9. Une fois l'installation terminée et la ligne de commande disponible, vous pouvez répéter les étapes de cette procédure pour installer plus d'agents de surveillance sur le système géré.

Que faire ensuite

Configurez l'agent en fonction de vos besoins. Si votre agent de surveillance requiert des opérations de configuration comme indiqué dans Chapitre 5, «Déploiement d'agents et de collecteurs de données», à la page 115 ou si vous voulez consulter les paramètres par défaut, voir Chapitre 7, «Configuration de votre environnement», à la page 163.

- Si vous utilisez un proxy direct étant donné que votre pare-feu n'autorise pas les connexions HTTPS sortantes transparentes aux hôtes externes, vous devez éditer le fichier de configuration d'environnement de l'agent. Pour obtenir des instructions, voir «Configuration des agents pour qu'ils communiquent via un proxy direct», à la page 163.
- Si vous avez mis à niveau un agent d'une version précédente, identifiez les éventuelles tâches de reconfiguration ou de migration à effectuer avant de vous connecter à la console Cloud APM. Pour plus d'informations sur ces tâches, voir «Mise à niveau de vos agents», à la page 1171. Après une mise à niveau, vous devez redémarrer tous les agents qui ne sont pas automatiquement configurés et démarrés par le programme d'installation.

Pour démarrer un agent, exécutez la commande suivante :

```
./nom-agent.sh start
```

Pour plus d'informations sur les commandes relatives aux agents de surveillance, y compris le nom à utiliser, voir «Utilisation des commandes de l'agent», à la page 181. Pour plus d'informations concernant les agents démarrés automatiquement et manuellement, voir Chapitre 5, «Déploiement d'agents et de collecteurs de données», à la page 115.

Après une mise à niveau, vous devez redémarrer tous les agents qui ne sont pas automatiquement configurés et démarrés par le programme d'installation.

Après avoir configuré et démarré l'agent, affichez les données que l'agent collecte.

- Si vous n'êtes pas connecté, suivez les instructions figurant dans «Démarrage de la console Cloud APM», à la page 1003.
- Si vous voulez afficher les systèmes gérés de votre domaine IBM Tivoli Monitoring dans les Tableau de bord d'Application Performance, effectuez les tâches décrites dans «Intégration à IBM Tivoli Monitoring V6.3 », à la page 975.

Installation des agents sur les systèmes Windows

Vous pouvez installer des agents de surveillance Cloud APM sur des systèmes Windows.

Les agents de surveillance suivants sont pris en charge sur les systèmes Windows 64 bits. Lorsque cela est indiqué, les agents sont également pris en charge sur les systèmes Windows de 32 bits.

- Monitoring Agent for Amazon EC2
- Monitoring Agent for AWS Elastic Load Balancer
- Monitoring Agent for Azure Compute
- Monitoring Agent for Cassandra
- Monitoring Agent for Cisco UCS
- Monitoring Agent for Citrix Virtual Desktop Infrastructure
- Monitoring Agent for Db2
- Monitoring Agent for Hadoop
- Monitoring Agent for HTTP Server*
- Monitoring Agent for IBM Cloud

- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for Internet Services*
- Monitoring Agent for MQ Appliance
- Monitoring Agent for JBoss
- Monitoring Agent for MariaDB
- Monitoring Agent for Microsoft Active Directory*
- Monitoring Agent for Microsoft Cluster Server*
- Monitoring Agent for Microsoft Exchange Server
- Monitoring Agent for Microsoft Hyper-V Server
- Monitoring Agent for Microsoft Internet Information Services
- Monitoring Agent for Skype for Business Server (anciennement Microsoft Lync Server)*
- Monitoring Agent for Microsoft .NET
- Monitoring Agent for Microsoft Office 365
- Monitoring Agent for Microsoft SharePoint Server
- Monitoring Agent for Microsoft SQL Server*
- Monitoring Agent for MySQL
- Monitoring Agent for NetApp Storage
- Monitoring Agent for Oracle Database
- Monitoring Agent for PostgreSQL
- Monitoring Agent for RabbitMQ
- Monitoring Agent for SAP Applications
- Monitoring Agent for SAP HANA Database
- Monitoring Agent for SAP NetWeaver Java Stack
- Monitoring Agent for Siebel
- Monitoring Agent for Sterling Connect Direct
- Monitoring Agent for Sterling File Gateway
- Monitoring Agent for Sybase Server
- Monitoring Agent for Tomcat
- Monitoring Agent for VMware VI
- Monitoring Agent for WebLogic
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ
- Monitoring Agent for Windows OS*
- Agent de surveillance des temps de réponse*

* Pris en charge sur les systèmes Windows 64 et 32 bits.

Préinstallation sur les systèmes Windows

Vous devez effectuer les tâches de préinstallation requises avant d'installer les agents sur les systèmes Windows. Certaines tâches de préinstallation sont spécifiques à un agent et d'autres tâches s'appliquent à plusieurs agents.

Remarque : Ces exigences viennent s'ajouter aux exigences identifiées dans les rapports sur la compatibilité du produit logiciel.

Pour obtenir la configuration requise pour la version actuelle et les dépendances pour votre agent, voir System requirements (APM Developer Center) qui fournit un lien vers les rapports sur la compatibilité du produit logiciel.

Tous les agents

Les tâches de préinstallation suivantes s'appliquent à tous les agents :

Tester la connectivité
Avant d'installer les agents, vérifiez que votre système puisse communiquer avec le serveur Cloud APM. Pour plus d'informations sur la vérification de la connectivité au serveur Cloud APM, voir Communication sécurisée.

Installation à partir de l'invite de commande sur une unité locale
Utilisez l'invite de commande Windows pour lancer le script d'installation. N'utilisez pas Windows PowerShell pour lancer le script d'installation.

Copiez les fichiers d'installation sur un disque local ou une unité réseau mappée et lancez ensuite le script d'installation. Ne lancez pas ce dernier à partir d'un emplacement réseau.

Lancez le script d'installation à partir d'une nouvelle invite de commande. Ne lancez pas le script d'installation à partir d'une invite de commande existante car cette dernière peut comporter des variables d'environnement périmées.

Définition de la variable d'environnement *CANDLEHOME*
Si vous avez utilisé ITM Agent Converter pour installer et configurer un agent sur le même système géré qu'auparavant, la variable d'environnement *CANDLEHOME* s'est vue affecter ce répertoire lorsque vous avez installé l'agent avec Agent Converter. Avant d'installer et de configurer un agent Cloud APM natif, vous devez affecter à la variable d'environnement *CANDLEHOME* un autre répertoire, faute de quoi l'agent Cloud APM natif ne peut pas démarrer.

Agents spécifiques

Les tâches de préinstallation suivantes s'appliquent aux agents spécifiés :

agent DataStage

1. Activez les paramètres dans le fichier `DSODBConfig.cfg`. Effectuez les opérations suivantes :
   a. Ouvrez le fichier `DSODBConfig.cfg` dans un éditeur à la ligne suivante :

      ```
      infosphere_information_server_install_dir\Server\DSODB
      ```

   b. Supprimez la mise en commentaire des paramètres suivants en supprimant le symbole *#* :

      ```
      MonitorLinks=1
      JobRunUsage=1
      ResourceMonitor=1
      DSODBON=1
      ```

   c. Editez les valeurs des paramètres définis sur 1.
2. Copiez le pilote JDBC de la base de données utilisée pour la configuration du référentiel de métadonnées sur l'ordinateur agent.
   a. Entrez 4 pour le pilote JDBC 4 ou ultérieur. Exemple : `db2jcc4.jar`
   b. Entrez 4 pour le pilote JDBC pour Oracle. Exemple : `ojdbc6.jar`
   c. Pilote JDBC pour MS SQL :
      - `Sqljdbc41.jar` nécessite l'environnement d'exécution Java 7 et prend en charge l'API JDBC 4.1.
      - `Sqljdbc42.jar` nécessite l'environnement d'exécution Java 8 et prend en charge l'API JDBC 4.2.

agent IBM Integration Bus
Assurez-vous que l'ID utilisateur employé pour installer l'agent IBM Integration Bus se trouve dans le groupe d'utilisateurs `mqbrkrs`.

Internet Service Monitoring
Pour Internet Service Monitoring, vous devez appliquer IBM Cloud Application Performance Management 8.1.4.0 Core Framework Interim Fix 3 sur APM Server à partir d'ici, puis préconfigurer

l'agent. L'agent et le module de pont utilisent les ports 9510 et 9520. Au cas où ces ports sont déjà utilisés, l'installation est suspendue.

Remarque :

- Pour les utilisateurs existants, il est recommandé d'installer l'agent Internet Service Monitoring sur les plateformes 64 bits (Windows ou Linux) plutôt que de mettre à niveau l'agent sur une plateforme Windows 32 bits vers une version plus récente.
- L'agent Internet Service Monitoring ne prend pas en charge Windows 2008 R2 sur la plateforme Windows 64 bits.

Agent MySQL

Pour Monitoring Agent for MySQL, vous devez installer le serveur MySQL et le pilote JDBC MySQL avant d'installer l'Agent MySQL sur ce système. Pour installer le pilote JDBC, voir Pilote MySQL Connector/J JDBC.

Agent Oracle Database

Si l'Agent Oracle Database surveille la base de données Oracle à distance, vous devez au préalable installer les clients Oracle Instant depuis Téléchargements Oracle Technology Network - Instant Client sur les systèmes suivants :

- Windows Server 2012 64 bits
- Windows Server 2012 R2 64 bits
- Windows Server 2008 R2 Datacenter 64 bits
- Windows Server 2008 R2 Enterprise 64-bits
- Windows Server 2008 R2 Standard 64 bits

Les clients Instant v10.x ,v11.x et v12.x sont pris en charge par l'Agent Oracle Database.

Agent de surveillance des temps de réponse

Avant d'installer l'Agent de surveillance des temps de réponse, passez en revue la section relative à la planification de l'installation ici : «Planification de l'installation », à la page 706.

Agent SAP HANA Database

1. Installez le client de base de données SAP HANA HDBSQL version 1.00.102.06 ou ultérieure sur le système Windows.
2. Ajoutez le chemin d'accès du client SAP HANA à la variable d'environnement **PATH**.

   Exemple : Ajoutez `C:\Program Files\sap\hdbclient` à la variable d'environnement **PATH**, où `C:\Program Files\sap\hdbclient` indique le chemin d'accès du client de base de données SAP HANA.

Agent Tomcat

1. Le kit SDK Java est installé sur le serveur Tomcat sur lequel l'agent est installé.
2. Le chemin d'accès au kit SDK est ajouté à la variable *PATH* directement, ou à l'aide de la commande **`set path`** avant d'installer l'agent.
3. La commande **JAR** fonctionne.

Installation d'agents

Vous pouvez installer toute combinaison des agents de surveillance sur un système géré. Par exemple, si vous installez Monitoring Agent for MySQL pour surveiller des serveurs MySQL, vous pouvez également installer l'Agent de surveillance des temps de réponse afin de collecter plus d'informations sur les temps de réponse de vos applications Ruby. Vous pouvez également installer l' Monitoring Agent for Windows OS pour surveiller d'autres aspects du système, tels que l'unité centrale globale, la mémoire et le disque.

Votre offre détermine les agents de surveillance disponibles pour l'installation. Pour obtenir la liste des agents compris dans chaque offre, voir «Fonctions», à la page 55.

Pour obtenir la liste des agents qui s'exécutent sur un système Windows, voir «Préinstallation sur les systèmes Windows», à la page 140.

Avant de commencer

Téléchargez les agents. Voir «Téléchargement de vos agents et de vos collecteurs de données», à la page 105.

Lisez les informations de la section «Configuration requise», à la page 85 afin de vous assurer que vous répondez aux exigences liées aux agents que vous prévoyez d'installer.

Revoyez les tâches prérequises des agents avant d'installer ces derniers. Pour plus d'informations, voir «Préinstallation sur les systèmes Windows», à la page 140.

Pourquoi et quand exécuter cette tâche

Vérifiez que vous disposez des droits appropriés pour exécuter le script d'installation de l'agent et les commandes d'agent. Vous devez être connecté à l'aide de l'un des types de compte utilisateur suivants :

- Compte utilisateur administrateur Windows par défaut
- Compte utilisateur administrateur
- Compte utilisateur membre du groupe Administrateurs
- Compte utilisateur enregistré en tant qu'administrateur dans les services Active Directory

La coexistence des agents est prise en charge. Vous pouvez installer les agents IBM Cloud Application Performance Management sur le même ordinateur que les agents IBM Tivoli Monitoring. Cependant, les deux types d'agent ne peuvent pas être installés dans le même répertoire. Pour plus d'informations sur la coexistence des agents, voir «Coexistence de l'agent Cloud APM et de l'agent Tivoli Monitoring», à la page 976.

Procédure

Pour installer des agents de surveillance sur des machines virtuelles et des systèmes sur lesquels le système d'exploitation Windows est installé, procédez comme suit :

1. Sur votre système, accédez au répertoire dans lequel vous avez téléchargé le fichier compressé.
2. Procédez à l'extraction des fichiers d'installation de l'agent associés à votre offre (ou à vos offres) à l'emplacement où vous voulez installer le logiciel d'agent de surveillance.
   Le script d'installation .bat est extrait dans un répertoire nommé en fonction du fichier archive et de la version. Par exemple : *offre*_Agent_Install_8.1.4.0. Les fichiers binaires de l'agent et les fichiers liés à la configuration sont extraits dans des sous-répertoires de ce répertoire.
3. Ouvrez une invite de commande en tant qu'administrateur.
   a) Dans le menu **Démarrer**, tapez commande dans la zone de recherche.
   b) Cliquez sur **Invite de commandes** avec le bouton droit de la souris dans la liste qui s'affiche, puis sélectionnez **Exécuter en tant qu'administrateur**.
4. A partir de l'invite de commande, exécutez le script d'installation avec des privilèges d'administrateur à partir du répertoire nommé en fonction du fichier archive et de la version :

   ```
   cd offre_Agent_Install_version
   installAPMAgents.bat
   ```

   Restriction : Pour l'Agent WebSphere Applications, les privilèges d'administration doivent être les mêmes que ceux utilisés pour installer WebSphere Application Server.

   Pour installer les agents en mode silencieux, voir «Installation des agents en mode silencieux», à la page 147.
5. Si vous installez les agents, indiquez le nom du répertoire d'installation.

   Le chemin d'installation par défaut est C:\IBM\APM. Le nom du répertoire d'installation ne doit pas comporter plus de 80 caractères ni contenir des caractères non ASCII, spéciaux ou codés sur deux

octets. Les noms de répertoire dans le chemin doivent contenir uniquement les caractères suivants : `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ _\:0123456789()~-./`.

Remarque : Lorsque la création de noms de fichier courts (*8dot3Name*) est désactivée, si les noms de répertoire dans le chemin d'accès contiennent des espaces, l'installation n'est pas prise en charge.

Si vous mettez à niveau l'agent, cette étape est ignorée et l'agent est installé dans le répertoire d'installation précédent.

6. Lorsque vous êtes invité à accepter le contrat de licence, entrez 1 pour l'accepter et continuer ou 2 pour refuser.

   Après avoir saisi 1 (accepter), l'analyse des prérequis de votre environnement commence et prend un certain moment. Si des exigences ne sont pas satisfaites, un message vous dirige vers un fichier journal contenant la raison de l'échec. Si un prérequis est manquant (par exemple, bibliothèque manquante ou espace disque insuffisant), l'installation s'arrête. Vous devez corriger l'incident, et relancer le script d'installation.

   Remarque : Si l'installation s'arrête avec le message ci-après, vérifiez si le service du serveur est démarré (Démarrer -> Outils d'administration -> Services). S'il ne l'est pas, démarrez-le, puis exécutez à nouveau `installAPMAgents.bat`.

   ```
   This script [installAPMAgents.bat] must be run as Administrator.
   ```

7. Une fois l'installation terminée et la ligne de commande disponible, répétez ces étapes pour installer d'autres agents de surveillance.

Que faire ensuite

Configurez vos agents en fonction de vos besoins. Pour vérifier si votre agent de surveillance requiert une configuration manuelle, voir Chapitre 5, «Déploiement d'agents et de collecteurs de données», à la page 115. Pour des instructions de configuration, ou si vous souhaitez passer en revue les paramètres de configuration par défaut, voir Chapitre 7, «Configuration de votre environnement», à la page 163.

Avant d'installer de nouveaux agents, le programme d'installation de Windows arrête temporairement tous les agents en cours d'exécution à l'emplacement du produit installé. Une fois l'installation terminée, le programme d'installation redémarre tous les agents arrêtés. Vous devez redémarrer manuellement tout agent de surveillance que le programme d'installation ne démarre pas automatiquement.

- Si vous utilisez un proxy direct étant donné que votre pare-feu n'autorise pas les connexions HTTPS sortantes transparentes aux hôtes externes, vous devez éditer le fichier de configuration d'environnement de l'agent. Pour obtenir des instructions, voir «Configuration des agents pour qu'ils communiquent via un proxy direct», à la page 163.
- Si vous avez mis à niveau un agent d'une version précédente, identifiez les tâches de reconfiguration ou de migration à effectuer avant de vous connecter à la console Cloud APM. Pour plus d'informations sur ces tâches, voir «Mise à niveau de vos agents», à la page 1171.

Utilisez l'une des méthodes suivantes pour démarrer l'agent :

- Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**. Cliquez avec le bouton droit de la souris sur un agent et cliquez sur **Start**.
- Exécutez la commande suivante :

  ```
  nom-agent.bat start
  ```

Pour plus d'informations sur les commandes relatives aux agents de surveillance, y compris le nom à utiliser, voir «Utilisation des commandes de l'agent», à la page 181. Pour plus d'informations sur les agents démarrés automatiquement et manuellement, voir Chapitre 5, «Déploiement d'agents et de collecteurs de données», à la page 115.

Après une mise à niveau, vous devez redémarrer tous les agents qui ne sont pas automatiquement configurés et démarrés par le programme d'installation.

Après avoir configuré et démarré l'agent, affichez les données que l'agent collecte.

- Si vous n'êtes pas connecté, suivez les instructions figurant dans «Démarrage de la console Cloud APM», à la page 1003.
- Si vous voulez afficher les systèmes gérés de votre domaine IBM Tivoli Monitoring dans les Tableau de bord d'Application Performance, effectuez les tâches décrites dans «Intégration à IBM Tivoli Monitoring V6.3 », à la page 975.

Installation des agents en tant qu'utilisateur non superutilisateur

Si vous ne disposez pas des privilèges superutilisateur et que vous souhaitez installer un agent de surveillance, vous pouvez installer l'agent comme un utilisateur non superutilisateur. En outre, vous ne pouvez pas installer l'agent comme utilisateur non-superutilisateur si vous êtes administrateur d'hôte et que vous ne souhaitez pas exécuter l'agent de surveillance comme superutilisateur. Le flux d'installation est le même que pour un superutilisateur. Après une installation non superutilisateur, exécutez le script **UpdateAutoRun.sh** avec des droits d'accès de superutilisateur ou d'utilisateur sudo.

Avant de commencer

Pour identifier le système informatique de manière unique, l'Linux OS doit déterminer l'identificateur unique universel (UUID), le fabricant, le modèle et le numéro de série de la carte mère du système informatique. Ces informations sont obligatoires pour que l'agent puisse être ajouté à une application dans la console Cloud APM.

Procurez-vous les informations relatives au système d'exploitation en vérifiant que les entités suivantes existent sur l'ordinateur :

1. Vérifiez si la commande **/usr/bin/hal-get-property** est installée sur le système informatique et si le processus hald (démon HAL) est en cours d'exécution. Si la commande n'est pas installée, passez à l'étape 2. Si elle est installée, ignorez l'étape 2 et étape 3. Remarque : si la version du système d'exploitation est Red Hat 7, le processus hald n'est pas disponible.
2. Si la commande **/usr/bin/hal-get-property** n'est pas installée sur le système informatique, confirmez que le fichier `/sys/class/dmi/id/product_uuid` existe et qu'il contient l'identificateur unique universel du système informatique, et que l'utilisateur qui installe l'agent de système d'exploitation Linux a un accès en écriture à ce fichier. Si ce fichier n'existe pas, passez à l'étape 3. S'il existe, ignorez cette étape.
3. Si la commande **/usr/bin/hal-get-property** n'est pas installée et que le fichier `/sys/class/dmi/id/product_uuid` n'existe pas, assurez-vous que la commande **hostname** ou **hostnamectl** renvoie le nom d'hôte complet. Si ces commandes renvoient le nom d'hôte abrégé sans le domaine, définissez le nom d'hôte complet en entrant **"hostname <nom_hôte_complet>"** ou **"hostnamectl set-hostname <nom_hôte_complet>"**, où *<nom_hôte_complet>* doit être remplacé par le nom d'hôte complet.

Remarque : L'Linux OS récupère ces informations régulièrement de telle sorte que les commandes ou les fichiers mentionnés aux étapes précédentes doivent rester aux mêmes emplacements, même après l'installation.

Remarque : L'agent de système d'exploitation Linux ne prend pas en charge la surveillance de Docker lorsqu'il est exécuté en tant que non superutilisateur.

Procédure

1. Installez vos agents de surveillance sous Linux ou UNIX , comme décrit dans les rubriques «Installation des agents sur les systèmes Linux», à la page 130 et «Installation des agents sur les systèmes UNIX», à la page 124.
2. Facultatif : Si vous avez installé votre agent en tant qu'utilisateur sélectionné et que vous souhaitez configurer l'agent en tant qu'un autre utilisateur, exécutez le script `./secure.sh`.

   Pour plus d'informations sur le script **./secure.sh**, voir «Configuration des agents en tant qu'utilisateur non superutilisateur», à la page 188 et Sécurisation des fichiers d'installation de l'agent.

   Par exemple : **./secure.sh -g db2iadm1**

3. Facultatif : Au besoin, configurez vos agents de surveillance sous Linux ou UNIX (voir Chapitre 7, «Configuration de votre environnement», à la page 163).
4. Pour mettre à jour les scripts de démarrage du système, exécutez le script suivant avec des droits d'accès de superutilisateur ou d'utilisateur sudo: *rép_install*/bin/UpdateAutoRun.sh

Que faire ensuite

Si vous avez installé votre agent en tant qu'utilisateur superutilisateur et que vous souhaitez configurer l'agent de la même manière, aucune action spéciale n'est requise. Si vous avez installé votre agent en tant qu'utilisateur sélectionné et que vous souhaitez le configurer en tant qu'un autre utilisateur, voir «Configuration des agents en tant qu'utilisateur non superutilisateur», à la page 188.

Si vous avez installé et configuré votre agent en tant qu'utilisateur non superutilisateur et que vous souhaitez démarrer l'agent de la même manière, aucune action spéciale n'est requise. Si vous avez installé et configuré votre agent en tant qu'utilisateur sélectionné et que vous souhaitez le démarrer en tant qu'un autre utilisateur, voir «Démarrage des agents en tant qu'utilisateur non superutilisateur», à la page 1042.

Utilisez le même ID utilisateur pour l'installation et les mises à niveau des agents.

Si vous exécutez le script **UpdateAutoRun.sh** en tant que superutilisateur, l'agent est configuré de sorte à démarrer automatiquement suite au redémarrage du système d'exploitation. Si vous ne voulez pas que l'agent ait ce comportement, vous pouvez désactiver le démarrage automatique de l'agent. Pour plus d'informations, voir «Désactivation du démarrage automatique de l'agent sur les systèmes UNIX et Linux», à la page 188.

Sécurisation des fichiers d'installation de l'agent

Après avoir installé les agents de surveillance sous le nom d'un utilisateur non superutilisateur sur des systèmes Linux ou UNIX, vous pouvez exécuter le script `secure.sh` pour sécuriser l'installation des agents en supprimant les droits en écriture "world" et en définissant la propriété de fichier correcte.

Avant de commencer

- Vous devez disposer des droits d'écriture, de lecture et d'exécution sur le répertoire d'installation.
- L'installation des agents de surveillance et toute configuration d'agent doivent être effectuées sur le système et les agents doivent être correctement démarrés.
- Si vous exécutez des agents en utilisant des comptes utilisateur différents, ces comptes doivent être membres du même groupe. (Voir l'option `-g`.)

Pourquoi et quand exécuter cette tâche

Effectuez cette étape pour verrouiller les droits d'accès aux fichiers dans votre installation. Des options sont disponibles pour qu'aucun mot de passe root ne soit requis, pour spécifier un nom de groupe et pour afficher l'aide de la commande.

Procédure

- Exécutez la commande suivante à partir du répertoire *rép_install*/bin. Syntaxe :

```
secure.sh [-g common_group] [-n] [-h]
```

  - Dans le mode le plus simple, exécutez le script **./secure.sh** qui supprime les droits "world" et définit l'utilisateur en cours et le groupe de l'utilisateur comme propriétaires du fichier. Si le script est exécuté par un utilisateur non superutilisateur, le système demande le mot de passe root.
  - Si un utilisateur non superutilisateur exécute le script **./secure.sh** avec l'option `-n`, le système ne demande pas le mot de passe root. Dans ce cas, vous changez les droits de fichier et la propriété en utilisant les privilèges de l'utilisateur. Si le répertoire d'installation contient des fichiers détenus

par des utilisateurs différents et que l'utilisateur n'a pas de privilèges pour modifier les autorisations et la propriété des fichiers des autres utilisateurs, ce mode échoue.

- Si vous voulez définir un groupe comme propriétaire de groupe, le propriétaire doit fournir l'option `-g` avec un nom de groupe valide comme argument pour l'option. (Voir Exemple.)
  Lancez `secure.sh -g` *`groupe_commun`*.
  Cette commande modifie la propriété des fichiers et des répertoires de manière récursive.

  Si le groupe *groupe_commun* n'est pas le groupe principal de l'utilisateur, vous pouvez le définir comme étant le propriétaire de groupe des nouveaux fichiers créés dans un répertoire, en exécutant la commande suivante :

  ```
  chmod g+s rép_install/bin/sous_rép
  ```

  où, *sous_rép* est un sous-répertoire, par exemple `/opt/ibm/ccm/agent`.
- Exécutez le script **`./secure.sh`** avec l'option –h pour obtenir l'aide relative au script.

Résultats
Le répertoire d'installation n'autorise l'accès qu'à l'utilisateur ayant exécuté le script ou aux utilisateurs du groupe spécifié.

Exemple

Si l'utilisateur Alice est membre du groupe système "apmgroup", il peut utiliser ce groupe pour définir la propriété du groupe de fichiers à l'aide de la commande suivante :

```
./secure.sh -g apmgroup
```

Une fois que le script a été exécuté, le groupe est défini sur "apmgroup" pour tous les fichiers du répertoire *`rép_install`* pour le groupe.

Que faire ensuite

L'exécution du script **`./secure.sh`** doit entraîner la définition des droits suivants pour les agents.

```
rwx rwx ---
```

Après avoir exécuté le script, vérifiez les droits d'accès pour les fichiers d'agent. Par exemple, pour la surveillance des temps de réponse, vérifiez les fichiers dans *`rép_install`*`/arch/hu/lib/mod_wrt.so`. Si les droits d'accès pour ces fichiers ne sont pas correctement définis, mettez-les à jour manuellement. Par exemple, pour l'agent de surveillance des temps de réponse :

1. Définissez les droits d'accès, exécutez :

   ```
   chmod g+rx $AGENT_HOME/bin/rt-agent.sh
   ```

2. Définissez l'utilisateur et le groupe, exécutez :

   ```
   chown newuser:newgroup $AGENT_HOME/bin/rt-agent.sh
   ```

Installation des agents en mode silencieux

L'installation des agents en mode silencieux réduit la durée d'installation. Pour installer un agent de surveillance en mode silencieux, vous devez télécharger le fichier d'archive des images d'installation de celui-ci à partir du du site Web IBM Marketplace , décompresser les fichiers d'installation de l'agent, préparer un fichier de réponses silencieux et exécuter le script d'installation en mode silencieux.

Avant de commencer

1. Consultez les tâches prérequises pour l'installation des agents de surveillance, puis téléchargez et extrayez les fichiers d'installation des agents. Pour plus de détails, voir Installation des agents sur les systèmes UNIX, Installation des agents sur les systèmes Linux ou Installation des agents sur les systèmes Windows.
2. Pour préparer un fichier de réponses silencieux pour l'installation des agents, procédez comme suit :
   a. Recherchez le fichier d'installation silencieux pour votre ou vos offres *offre*_silent_install.txt, créez-en une copie et ouvrez-le dans un éditeur de texte.
   b. Supprimez la mise en commentaire du contrat de licence.
   c. Pour spécifier les agents que vous voulez installer, effectuez l'une des étapes suivantes :
      - Supprimez la mise en commentaire des agents individuels à installer. Par exemple :

        ```
        INSTALL_AGENT=os
        ```

        ```
        INSTALL_AGENT=ruby
        ```

      - Supprimez la mise en commentaire de INSTALL_AGENT=all pour installer tous les agents.
   d. Supprimez la mise en commentaire de AGENT_HOME et spécifiez le répertoire dans lequel vous voulez installer les agents.

      A faire : Linux Si vous mettez à niveau les agents sur un système Linux, ne spécifiez pas le répertoire /opt/ibm/apm/agent.
   e. Linux Si vous mettez à niveau les agents sur un système Linux, supprimez la mise en commentaire de MIGRATE_CONF=yes.
   f. Sauvegardez le fichier.

Procédure

1. Sur la ligne de commande, basculez vers le répertoire dans lequel vous avez extrait le script d'installation et exécutez la commande suivante :

   ```
   cd offre_Agent_Install_version
   ```

2. Facultatif : Cette étape est obligatoire UNIQUEMENT pour Solaris 10. Vous devez créer un lien lointain à ksh avant d'exécuter le script d'installation sous Solaris 10.
   a) Sauvegardez la commande /bin/sh :

   ```
   mv /bin/sh /bin/sh.bkup_origin
   ```

   b) Créez un lien lointain à la commande ksh :

   ```
   ln -s /bin/ksh /bin/sh
   ```

   c) Confirmez que le résultat pointe vers ksh :

   ```
   ls -l /bin/sh
   ```

3. Exécutez la commande d'installation :
   - Linux AIX

     ```
     ./installAPMAgents.sh -p chemin_d'accès_au_fichier_réponses_silencieux
     ```

   - Windows

     ```
     installAPMAgents.bat -p chemin_d'accès_au_fichier_réponses_silencieux
     ```

L'installation des agents échoue sous Windows si le scanner de prérequis ne parvient pas à obtenir le type de disque sur lequel l'agent sera installé. Si cela se produit, un résultat d'échec apparaît pour la propriété validDestLocation dans le fichier journal de l'installation. Dans ce cas, vous pouvez ignorer l'analyse des prérequis en ajoutant SKIP_PRECHECK=1 à la commande d'installation. Par exemple :

```
installAPMAgents.bat -p chemin_d'accès_au_fichier_réponses_silencieux SKIP_PRECHECK=1
```

Remarque : Windows Lorsque la création de noms de fichier courts (*8dot3Name*) est désactivée, si les noms de répertoire dans le chemin d'accès contiennent des espaces, l'installation n'est pas prise en charge.

Résultats
Les agents sont installés.

Que faire ensuite

Configurez les agents. Reportez-vous à la procédure et au tableau de commandes pour les systèmes Linux et UNIX et les systèmes Windows.

Contournement de l'analyse des prérequis

Lorsque vous installez des agents de surveillance, l'analyse des prérequis de votre environnement commence et prend un certain temps. Si des exigences ne sont pas satisfaites, un message vous dirige vers un fichier journal contenant la raison de l'échec. Dans certains scénarios d'installation, vous pouvez ignorer les messages d'avertissement ou ignorer complètement le contrôle des prérequis.

Pourquoi et quand exécuter cette tâche

Il existe deux niveaux de messages d'échec, WARN et FAIL, et deux niveaux de contournement :

- Si vous définissez la variable **IGNORE_PRECHECK_WARNING**, le programme d'installation ignore les messages d'avertissement (WARN).
- Si vous définissez la variable **SKIP_PRECHECK**, le programme d'installation ignore tous les messages d'échec.

Si l'installation de l'agent a échoué et que vous avez reçu un avertissement (WARN) de la part du programme de vérification des prérequis, prenez connaissance de l'avertissement. Si vous souhaitez poursuivre l'installation, définissez **IGNORE_PRECHECK_WARNING** et installez l'agent à nouveau.

Dans un environnement où des images de machine virtuelle servent de modèles, l'analyse des prérequis effectuée avant que l'installation ne commence ne peut être effectuée que sur la première image de modèle. Si une image de machine virtuelle réussit l'analyse, les autres machines virtuelles créées à partir de cette image le réussissent également. Vous pouvez gagner du temps en ignorant le contrôle des prérequis pour les autres machines virtuelles créées à partir de la même image. Définissez la variable **SKIP_PRECHECK** et installez l'agent à nouveau.

Le paramètre **SKIP_PRECHECK** est également approprié dans les cas où vous disposez d'un nouveau système d'exploitation qui, d'après le support IBM ou les rapports sur la compatibilité du produit logiciel, est pris en charge, mais pour lequel le programme de vérification des prérequis n'a pas encore été mis à jour. Assurez-vous d'abord d'installer l'agent, vérifiez le journal, et assurez-vous ensuite que ce nouveau système d'exploitation est le seul élément défaillant (et le seul élément que vous ignorez). En effet, lorsque la variable **SKIP_PRECHECK** est définie, le programme d'installation ignore l'ensemble des éléments figurant sur la liste de contrôle des prérequis.

Une fois que vous avez téléchargé et extrait les fichiers d'installation, suivez cette procédure pour ignorer les messages d'avertissement ou l'analyse des prérequis.

Procédure

Sur le système où vous prévoyez d'installer les agents de surveillance, entrez l'une des commandes suivantes :

- Ignorez les messages d'avertissement (WARN) lors du contrôle des prérequis :
  - Linux AIX `export IGNORE_PRECHECK_WARNING=1`
  - Windows `set IGNORE_PRECHECK_WARNING=1`
- Ignorez l'analyse des prérequis :
  - Linux AIX `export SKIP_PRECHECK=1`
  - Windows `set SKIP_PRECHECK=1`

Que faire ensuite

Pour restaurer le paramètre par défaut lors de la prochaine installation de l'agent avec le scanner de prérequis, désactivez la variable **IGNORE_PRECHECK_WARNING** ou **SKIP_PRECHECK** :

- Linux AIX `unset IGNORE_PRECHECK_WARNING`
- Windows `set IGNORE_PRECHECK_WARNING=`

ou

- Linux AIX `unset SKIP_PRECHECK`
- Windows `set SKIP_PRECHECK=`

Désinstallation de vos agents

Désinstallez un seul agent ou tous les agents d'un système géré.

Avant de commencer

Pour les agents multi-instance, vous devez supprimer toutes les instances d'agent d'agent avant de désinstaller l'agent. Sinon, les entrées d'agent ne seront pas effacées du registre. Pour supprimer des instances, exécutez la commande suivante :

- Windows *nom*`-agent.bat remove` *nom_instance*
- Linux AIX `./`*nom*`-agent.sh remove` *nom_instance*

où, *nom* est le nom de l'agent et *nom_instance* est le nom d'instance. Pour plus d'informations, voir «Utilisation des commandes de l'agent», à la page 181. Pour une liste des agents multiple-instance, voir Tableau 7, à la page 117.

Pour les agents suivants, une tâche spécifique à l'agent doit être exécutée avant de suivre la procédure de désinstallation :

- Pour Monitoring Agent for HTTP Server, vous devez supprimer l'instruction `Include` dans le fichier `http.conf`, par exemple, `"Include "/opt/ibm/apm/agent/tmp/khu/kvm65s2_8044.conf"`, avant de redémarrer IBM HTTP Server.
- Pour Monitoring Agent for Python, exécutez *rép_install*`/lx8266/pg/bin/uninstall.sh` pour supprimer les codes d'injection avant de désinstaller l'agent.
- Pour Monitoring Agent for PHP, exécutez *rép_install*`/bin/lx8266/pj/lib/uninstall.`*nom_instance*`.sh` pour déplacer les codes d'injection avant de désinstaller l'agent.
- Pour Monitoring Agent for WebSphere Applications, vous devez annuler la configuration du collecteur de données pour toutes les instances de serveur surveillées avant de désinstaller l'agent. Suivez les instructions décrites dans «Agent WebSphere Applications : Annulation de la configuration du collecteur de données», à la page 152.

Pour l'Agent WebSphere Applications, assurez-vous que l'ID utilisateur, utilisé pour désinstaller l'agent, dispose des droits complets en lecture et en écriture sur les répertoires `logs` et `runtime` et sur tous leurs sous-répertoires et fichiers que contient le répertoire de base du collecteur de données. Le répertoire principal du collecteur de données est le suivant :

  - Windows *rép_install*\dchome\7.3.0.14.08
  - Linux AIX *rép_install*/yndchome/7.3.0.14.08

- Pour l'Agent Node.js, vous devez retirer le plug-in de surveillance de votre application Node.js avant de désinstaller l'agent. Suivez les instructions décrites dans «Agent Node.js : Retrait du plug-in de surveillance», à la page 161.
- Pour l'agent Microsoft .NET, vous devez retirer le collecteur de données de vos applications .NET avant de désinstaller l'agent. Suivez les instructions décrites dans «agent Microsoft .NET : Retrait du collecteur de données .NET», à la page 162.
- Pour l'agent IBM Integration Bus, si vous avez configuré le suivi des transactions pour des courtiers avec l'exit utilisateur fourni par l'agent, vous devez supprimer l'exit utilisateur avant de désinstaller l'agent. Suivez les instructions de la rubrique «Suppression de l'exit utilisateur KQIUserExit», à la page 298.
- Pour Internet Service Monitoring, accédez à `<candle_home>\BIN` et exécutez le fichier ism-agent.bat avec `uninstall` comme argument. Si vous souhaitez désinstaller tous les agents de surveillance sur le serveur à l'aide du fichier smai-agent.bat, exécutez la commande ism-agent.bat avec l'argument `uninstall`, puis exécutez la commande smai-agent.bat
- Avant de désinstaller Monitoring Agent for SAP NetWeaver Java Stack, arrêtez toutes les instances de l'agent SAP NetWeaver Java Stack en exécutant la commande suivante :
  - Windows `sap_netweaver_java_stack-agent.bat stop instance_name`

Pourquoi et quand exécuter cette tâche

L'agent Oracle sur les systèmes Windows peut être désinstallé uniquement à l'aide de l'invite de commande.

Procédure

1. Sur la machine virtuelle ou le système où l'agent ou les agents de surveillance sont installés, ouvrez une ligne de commande et accédez au répertoire des fichiers binaires :
   - Linux AIX *rép_install*/bin
   - Windows *rép_install*\BIN

   où *rép_install* est le répertoire d'installation des agents de surveillance.
2. Pour désinstaller un agent de surveillance spécifique, entrez le nom du script de l'agent et l'option de désinstallation où *nom* représente le nom du script de l'agent :
   - Linux AIX `./nom-agent.sh uninstall`
   - Windows `nom-agent.bat uninstall`

   Pour une liste des noms de script d'agent produit, voir «Utilisation des commandes de l'agent», à la page 181.

   A faire : Pour Monitoring Agent for Microsoft .NET, vous devez exécuter la commande avec des privilèges d'administrateur.

   L'agent de surveillance est désinstallé du système géré.

   Si vous avez désinstallé tous les agents de surveillance de manière individuelle, continuez à supprimer les fichiers Framework. Voir Et ensuite ?.
3. Pour désinstaller tous les agents de surveillance du système géré avec une invite de confirmation, entrez le nom du script et l'option uninstall all :

- Linux AIX `./smai-agent.sh uninstall_all`
- Windows `smai-agent.bat uninstall_all`

Une invite de confirmation s'affiche. Tapez 1 pour continuer ou 2 pour annuler.

Tous les agents de surveillance sont désinstallés du système ou de la machine virtuelle.

4. Linux AIX

Sous Linux et UNIX, pour forcer la désinstallation de tous les agents de surveillance sans invite de confirmation, entrez le nom du script et l'option force uninstall all :

```
./smai-agent.sh uninstall_all force
```

Que faire ensuite

Pour Monitoring Agent for HTTP Server, après l'avoir désinstallé, supprimez manuellement les fichiers suivants :

- `/tmp/khu_cps.properties`
- `/tmp/httpserver-disc.error`

Pour Monitoring Agent for Python :

1. Supprimez le fichier de configuration Django `pyc` afin de vous assurer que le fichier `pyc` Django génère son binaire.
2. Redémarrez le serveur Apache pour supprimer le composant middleware chargé dans les processus Apache.

Pour Monitoring Agent for Ruby, pour désinstaller le collecteur de données de diagnostic :

1. Accédez au répertoire de base de votre application, ouvrez son `Gemfile` et retirez la ligne suivante dans le fichier : `gem 'stacktracer'`
2. Redémarrez l'application Ruby on Rails.
3. Désinstallez le collecteur de données de diagnostic. Entrez : `gem uninstall` *`Gemfile`*
4. Retirez le répertoire d'exécution du collecteur de données. L'emplacement par défaut de ce répertoire est *`rép_install`*`/install-images/kkm/dchome`

Pour Monitoring Agent for Microsoft .NET, procédez comme suit :

1. Supprimez les fichiers `dll` du collecteur de données en utilisant l'une des options suivantes :
   - Réamorcez le système d'exploitation.
   - Essayez de supprimer le fichier *`rép_install`*`\qe\bin64\CorProfLog.dll`.

     Une boîte de dialogue indiquant que le fichier est en cours d'utilisation (`File in Use`) s'affiche. Elle identifie les processus .NET en cours d'exécution.
   - Redémarrez chacun des processus .NET.
2. Redémarrez vos applications .NET.

Agent WebSphere Applications : Annulation de la configuration du collecteur de données

Si vous désinstallez l'Agent WebSphere Applications avant d'avoir annulé la configuration du collecteur de données, la désinstallation de l'agent échoue. Vous pouvez supprimer le collecteur de données d'une instance de serveur d'applications de trois façons : manuellement, en recourant à l'utilitaire interactif ou bien en exécutant le processus d'annulation de la configuration en mode silencieux.

Pour la surveillance des instances avec les ressources de surveillance PMI, l'annulation de configuration est indisponible. La surveillance des données PMI se poursuit tandis que le serveur est disponible.

Annulation de la configuration interactive du collecteur de données

Si vous ne voulez plus que le collecteur de données surveille une ou plusieurs instances de serveur d'applications, vous pouvez annuler la configuration du collecteur de données pour ces instances.

Avant de commencer

Utilisez l'ID utilisateur employé pour configurer le collecteur de données pour annuler la configuration du collecteur de données ; il s'agit également de l'ID utilisateur employé pour installer le serveur d'applications. Vérifiez que cet ID utilisateur dispose de droits en lecture et en écriture sur le répertoire de base du collecteur de données et sur tous ses sous-répertoires. Le répertoire de base du collecteur de données est le suivant, où *rép_install* est le répertoire d'installation de l'Agent WebSphere Applications.

- Windows *rép_install*\dchome\7.3.0.14.08
- Linux AIX *rép_install*/yndchome/7.3.0.14.08

Pourquoi et quand exécuter cette tâche

L'utilitaire d'annulation de configuration (`unconfig.sh` ou `unconfig.bat`) est un utilitaire de ligne de commande à menus permettant d'annuler la configuration du collecteur de données.

Procédure

1. Connectez-vous au système à l'aide de l'ID utilisateur employé pour configurer le collecteur de données.
2. Accédez au répertoire `bin` :
   - Windows *rép_install*\dchome\7.3.0.14.08\bin
   - Linux AIX *rép_install*/yndchome/7.3.0.14.08/bin
3. Facultatif : Définissez l'emplacement du répertoire de base Java avant de démarrer l'utilitaire.

   Exemple :

   Linux AIX
   ```
   export JAVA_HOME=/opt/IBM/AppServer80/java
   ```

   Windows
   ```
   set JAVA_HOME=C:\Progra~1\IBM\WebSphere\AppServer80\java
   ```
4. Démarrez l'utilitaire d'annulation de configuration à l'aide de la commande suivante :

   Linux AIX
   ```
   ./unconfig.sh
   ```

   Windows
   ```
   unconfig.bat
   ```
5. L'utilitaire recherche toutes les instances de serveur qui sont surveillées par le collecteur de données. Entrez le nombre qui correspond à l'instance de serveur d'applications dont vous voulez annuler la configuration pour la collecte de données ou entrez un astérisque (`*`) pour annuler la configuration de la collecte de données pour toutes les instances de serveur d'applications. Pour indiquer un sous-ensemble de serveurs, entrez les nombres, séparés par des virgules, qui représentent les serveurs. Par exemple : `1,2,3`.

   A faire :

   - Pour un environnement autonome, les instances de serveur d'applications doivent s'exécuter pendant la configuration. (Une instance de WebSphere Application Server Liberty n'a pas besoin d'être en cours d'exécution).
   - Dans un environnement de déploiement réseau, l'agent de noeud et le gestionnaire de déploiement doivent s'exécuter.
6. L'utilitaire vous invite à indiquer si vous voulez créer une sauvegarde de votre configuration en cours de WebSphere Application Server. Entrez 1 pour créer une sauvegarde de la configuration en cours. Sinon, entrez 2 et passez à l'étape 8.
7. L'utilitaire vous invite à spécifier le répertoire dans lequel stocker la sauvegarde de la configuration. Indiquez un répertoire dans lequel stocker la sauvegarde de la configuration ou acceptez le répertoire par défaut.

   L'utilitaire affiche le nom du répertoire de base de WebSphere ainsi que le profil WebSphere pour lequel une sauvegarde est créée.

8. L'utilitaire indique si la sécurité globale de WebSphere est activée pour le profil WebSphere Application que vous avez indiqué. Si la sécurité globale n'est pas activée, passez à l'étape 10.
9. L'utilitaire vous invite à indiquer si les paramètres de sécurité doivent être extraits depuis un fichier de propriétés de client. Entrez 1 pour permettre à l'utilitaire d'extraire le nom d'utilisateur et le mot de passe à partir du fichier de propriétés de client approprié et passez à l'étape «10», à la page 154. Sinon, entrez 2 pour entrer le nom d'utilisateur et le mot de passe.

   Le collecteur de données communique avec les services d'administration de WebSphere en utilisant l'invocation RMI (Remote Method Invocation) ou le protocole SOAP (Simple Object Access Protocol). Si la sécurité globale est activée pour un profil, vous devez indiquer l'ID utilisateur et le mot de passe d'un utilisateur qui est autorisé à se connecter à IBM WebSphere Application Server la console d'administration pour le profil. Vous avez également la possibilité de chiffrer le nom d'utilisateur et le mot de passe et de les stocker dans des fichiers de propriétés de client avant de configurer le collecteur de données. Vous devez utiliser le fichier `sas.client.props` pour une connexion RMI, ou le fichier `soap.client.props` pour une connexion SOAP.

   Si vous avez sélectionné l'option de sauvegarder la configuration en cours de WebSphere, l'utilitaire commence à sauvegarder la configuration.
10. L'utilitaire annule la configuration du collecteur de données pour les instances de serveur d'applications spécifiées. Un message d'état indique que l'annulation de la configuration du collecteur de données a abouti.
11. Une fois l'annulation de la configuration du collecteur de données terminée, redémarrez les instances du serveur d'applications.

    La configuration du collecteur de données entre en vigueur une fois que les instances de serveur d'applications ont redémarré. La surveillance des ressources PMI pour l'instance de serveur est toujours disponible.
12. Facultatif : Si vous souhaitez l'utiliser pour une instance de serveur après avoir annulé la configuration du collecteur de données, redémarrez l'agent de surveillance en exécutant les commandes suivantes :
    - Windows

      ```
      cd rép_install\bin
      was-agent.bat stop
      was-agent.bat start
      ```
    - Linux AIX

      ```
      cd rép_install/bin
      ./was-agent.sh
      stop
      ./was-agent.sh start
      ```

Résultats
L'utilitaire annule la configuration du collecteur de données pour les instances de serveur d'applications spécifiées.

Annulation de la configuration du collecteur de données en mode silencieux
Vous pouvez annuler la configuration du collecteur de données à l'aide de l'utilitaire d'annulation de configuration en mode silencieux.

Avant de commencer

Utilisez l'ID utilisateur employé pour configurer le collecteur de données pour annuler la configuration du collecteur de données ; il s'agit également de l'ID utilisateur employé pour installer le serveur d'applications. Vérifiez que cet ID utilisateur dispose de droits en lecture et en écriture sur le répertoire de base du collecteur de données et sur tous ses sous-répertoires. Le répertoire de base du collecteur de données est le suivant, où *rép_install* est le répertoire d'installation de l'Agent WebSphere Applications.

- Windows *rép_install*\dchome\7.3.0.14.08

- Linux AIX *rép_install*/yndchome/7.3.0.14.08

Pourquoi et quand exécuter cette tâche

Lorsque vous annulez la configuration du collecteur de données en mode silencieux, vous indiquez d'abord des options de configuration dans un fichier de propriétés. Un exemple de fichier de propriétés, `sample_silent_unconfig.txt`, est fourni avec l'utilitaire d'annulation de configuration. Le fichier est disponible dans le répertoire `bin` au sein du répertoire de base du collecteur de données.

Procédure

1. Connectez-vous au système à l'aide de l'ID utilisateur employé pour configurer le collecteur de données.
2. Spécifiez les options de configuration dans le fichier `properties.txt`.

   Les propriétés suivantes peuvent être utilisées pour annuler la configuration du collecteur de données en mode silencieux :

   Paramètres de connexion de WebSphere Application Server

   was.wsadmin.connection.host
   Indique le nom de l'hôte auquel l'outil wsadmin se connecte.

   Paramètres de sécurité globale de WebSphere Application Server

   was.wsadmin.username
   Spécifie l'ID utilisateur d'un utilisateur autorisé à se connecter à la console d'administration d'IBM WebSphere Application Server. Cet utilisateur doit posséder le rôle d'agent sur le serveur d'applications.

   was.wsadmin.password
   Indique le mot de passe qui correspond à l'utilisateur indiqué dans la propriété `was.wsadmin.username`.

   Paramètres de WebSphere Application Server

   was.appserver.profile.name
   Indique le nom du profil de serveur d'applications dont vous voulez annuler la configuration.

   was.appserver.home
   Indique le répertoire de base de WebSphere Application Server.

   was.appserver.cell.name
   Indique le nom de cellule de WebSphere Application Server.

   was.appserver.node.name
   Indique le nom de noeud de WebSphere Application Server.

   Sauvegarde de la configuration de WebSphere Application Server

   was.backup.configuration
   Indique si la configuration en cours du collecteur de données de WebSphere Application Server doit être ou non sauvegardée avant que vous ne procédiez à son annulation. Les valeurs valides sont `True` et `False`.

   was.backup.configuration.dir
   Indique l'emplacement du répertoire de sauvegarde.

   Paramètres de l'instance d'exécution de WebSphere Application Server

   was.appserver.server.name
   Indique une instance de serveur d'applications dans le profil de serveur d'applications pour laquelle vous voulez annuler la configuration du collecteur de données.

   Conseil : Le fichier de réponses silencieux peut avoir plusieurs instances de cette propriété.
3. Accédez au répertoire suivant :

   - Windows *rép_install*\dchome\7.3.0.14.08\bin

- Linux AIX *rép_install*/yndchome/7.3.0.14.08/bin

4. Exécutez la commande suivante :
   - Windows

     ```
     unconfig.bat -silent chemin_vers fichier_mode_silencieux
     ```

   - Linux AIX

     ```
     unconfig.sh -silent chemin_vers fichier_mode_silencieux
     ```

5. Une fois l'annulation de la configuration du collecteur de données terminée, redémarrez les instances du serveur d'applications.

   La configuration du collecteur de données entre en vigueur une fois que les instances de serveur d'applications ont redémarré. La surveillance des ressources PMI pour l'instance de serveur est toujours disponible.
6. Facultatif : Si vous souhaitez l'utiliser pour une instance de serveur après avoir annulé la configuration du collecteur de données, redémarrez l'agent de surveillance en exécutant les commandes suivantes :
   - Windows

     ```
     cd rép_install\bin
     was-agent.bat stop
     was-agent.bat start
     ```

   - Linux AIX

     ```
     cd rép_install/bin
     ./was-agent.sh
     stop
     ./was-agent.sh start
     ```

Suppression manuelle de la configuration du collecteur de données depuis une instance de serveur d'applications

Pour supprimer manuellement la configuration du collecteur de données depuis une instance de serveur d'applications, vous devez pouvoir vous connecter au serveur d'applications à l'aide de l'outil wsadmin. Ce n'est possible que si vous utilisez WebSphere Application Server Network Deployment et que si Deployment Manager est en cours d'exécution. Si WebSphere Application Server ne peut pas démarrer, vous devez le restaurer à partir de la sauvegarde effectuée lors de l'exécution de l'utilitaire de configuration.

Pourquoi et quand exécuter cette tâche

Vous pouvez supprimer manuellement la configuration du collecteur de données d'une instance de serveur d'applications, si l'une des conditions suivantes s'applique :

- Dans un environnement autre que Network Deployment, vous avez ajouté manuellement la configuration du collecteur de données pour l'instance de serveur d'applications et souhaitez annuler la configuration de la collecte de données. L'instance de serveur d'applications doit être en cours d'exécution.
- Dans un environnement Network Deployment, vous avez ajouté manuellement la configuration du collecteur de données pour l'instance de serveur d'applications et souhaitez annuler la configuration de la collecte de données. L'agent de noeud et le gestionnaire de déploiement sur le serveur d'applications doivent être en cours d'exécution.
- Dans un environnement Network Deployment, vous avez configuré l'instance de serveur d'applications pour la collecte des données manuellement et le serveur d'applications ne démarre pas. L'agent de noeud et le gestionnaire de déploiement sur le serveur d'applications doivent être en cours d'exécution.

Si vous avez configuré une instance de serveur d'applications autonome pour la collecte des données manuellement ou avec l'utilitaire de configuration ou de migration et que le serveur d'applications ne

démarre pas, vous devez restaurer la configuration WebSphere Application Server avec la configuration sauvegardée. Pour plus d'informations, voir «Restauration de la configuration du serveur d'applications depuis une sauvegarde», à la page 904.

A faire :

- Vous devez apporter des modifications manuelles à la configuration WebSphere Application Server pour les collecteurs de données en tant qu'administrateur WebSphere.
- Les modifications manuelles dans WebSphere Application Server pour la collecte des données doivent être exécutées par un administrateur WebSphere expérimenté uniquement. Toute erreur dans la modification manuelle de la configuration peut empêcher le démarrage du serveur d'applications.
- Si vous configurez manuellement le collecteur de données pour surveiller des instances de serveur d'application, vous ne pouvez pas employer l'utilitaire d'annulation de configuration pour annuler la configuration du collecteur de données.

Procédure

Pour supprimer manuellement la configuration du collecteur de données, procédez comme suit :

1. Connectez-vous à WebSphere Administration Server Console.
2. Cliquez sur **Serveurs**.
3. Développez **Type de serveur** et sélectionnez **Serveurs d'applications WebSphere**.
4. Cliquez sur le nom du serveur.
5. Dans l'onglet Configuration, accédez à **Infrastructure du serveur** > **Gestion des processus et Java** > **Définition des processus** > **Machine virtuelle Java** > **Propriétés supplémentaires : Propriétés personnalisées**.
6. Supprimez les propriétés personnalisées suivantes de la machine JVM, si elles existent :
   - `am.home`
   - `ITCAM.DC.ENABLED`
   - `TEMAGCCollector.gclog.path`
   - `com.ibm.tivoli.itcam.toolkit.ai.runtimebuilder.enable.rebuild`
   - `com.ibm.tivoli.jiti.injector.ProbeInjectorManagerChain`. `primaryInjectorFile`
7. Identifiez les arguments de JVM qui ont été ajoutés pour le collecteur de données.
   a) Dans le panneau de navigation, cliquez sur **Environnement** > **Variables WebSphere**.
   b) Si vous avez configuré le serveur d'applications pour la collecte de données manuellement, localisez les arguments JVM que vous avez ajoutés manuellement.

      Si vous avez configuré le serveur d'applications pour la collecte de données à l'aide des utilitaires de configuration, comparez les valeurs des arguments **AM_OLD_ARGS** et **AM_CONFIG_JVM_ARGS** pour déterminer quels arguments ont été ajoutés par l'utilitaire de configuration.
8. Cliquez sur **Serveur** > **Serveur d'applications** et sélectionnez le nom de serveur approprié.
9. Dans l'onglet Configuration, accédez à **Infrastructure du serveur** > **Gestion des processus et Java** > **Définition des processus** > **Machine virtuelle Java**.
10. Dans la zone **Arguments JVM génériques**, retirez les arguments JVM que vous avez identifiés à l'étape 7 pour le collecteur de données.
11. Cliquez sur **Appliquer** ou sur **OK**.
12. Dans la boîte de dialogue **Messages**, cliquez sur **Sauvegarder**.
13. Dans la boîte de dialogue **Sauvegarde dans la configuration maîtresse**, exécutez l'une des étapes suivantes :
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que la case à cocher **Synchroniser les modifications avec les noeuds** est sélectionnée, puis cliquez sur **Sauvegarder**.
    - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
14. Supprimez les entrées d'environnement qui ont été ajoutés pour le collecteur de données.

a) Dans l'onglet Configuration, accédez à **Infrastructure du serveur** > **Gestion des processus et Java** > **Définition des processus** > **Entrées d'environnement**.

b) Selon le système d'exploitation, supprimez l'entrée d'environnement suivante :

- UNIX **LIBPATH**
- Linux **LD_LIBRARY_PATH**
- Windows **PATH**

c) Supprimez l'entrée d'environnement **NLSPATH**.

15. Cliquez sur **Appliquer** ou sur **OK**.
16. Dans la boîte de dialogue **Messages**, cliquez sur **Sauvegarder**.
17. Dans la boîte de dialogue **Sauvegarde dans la configuration maîtresse**, exécutez l'une des étapes suivantes :
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que la case à cocher **Synchroniser les modifications avec les noeuds** est sélectionnée, puis cliquez sur **Sauvegarder**.
    - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
18. Dans le panneau de navigation, cliquez sur **Environnement** > **Variables WebSphere**.
19. Supprimez les variables suivantes :
    - **AM_CONFIG_JVM_ARGS**
    - **AM_OLD_JVM_ARGS**
    - **ITCAMDCHOME**
    - **ITCAMDCVERSION**
20. Dans la boîte de dialogue **Messages**, cliquez sur **Sauvegarder**.
21. Dans la boîte de dialogue **Sauvegarde dans la configuration maîtresse**, exécutez l'une des étapes suivantes :
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que la case à cocher **Synchroniser les modifications avec les noeuds** est sélectionnée, puis cliquez sur **Sauvegarder**.
    - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
22. Si vous avez configuré l'instance de serveur pour la collecte de données à l'aide de l'outil de configuration du collecteur de données, plutôt que manuellement, procédez comme suit :
    a) Accédez au répertoire *base_cd*/runtime.
    b) Renommez le fichier $profile.$cell.$node.$server.input.properties en $profile.$cell.$node.$server.input.properties.bak.
23. Si vous supprimez manuellement la configuration du collecteur de données à partir de toutes les instances de serveur d'applications dans un profil, procédez comme suit :
    a) Accédez au répertoire $appserverhome/bin.
    b) Exécutez la commande **osgiCfgInit.sh/bat -all** sur les systèmes Windows ou la commande **osgiCfgInit.sh -all** sur les systèmes UNIX et Linux.
24. Redémarrez l'instance de serveur d'applications surveillée par le collecteur de données.

Annulation manuelle de la configuration du collecteur de données

Après avoir configuré manuellement le collecteur de données pour l'Agent WebSphere Applications, vous devez annuler la configuration du collecteur de données manuellement pour pouvoir supprimer la collecte de données du serveur d'applications configuré.

Pourquoi et quand exécuter cette tâche

La procédure qui suit s'applique uniquement après avoir configuré manuellement le collecteur de données comme décrit dans «Configuration manuelle du collecteur de données si les utilitaires de configuration échouent», à la page 879. Si vous avez utilisé les utilitaires de configuration pour configurer le collecteur de données, vous devez également utiliser l'utilitaire d'annulation de configuration pour

annuler la configuration du collecteur de données. Pour plus d'informations, voir «Annulation de la configuration interactive du collecteur de données», à la page 152 ou «Annulation de la configuration du collecteur de données en mode silencieux», à la page 154.

Procédure

- Pour annuler manuellement la configuration du collecteur de données pour WebSphere Application Server, voir «Annulation manuelle de la configuration du collecteur de données pour WebSphere Application Server traditionnel», à la page 159.
- Pour annuler manuellement la configuration du collecteur de données pour le serveur Liberty, voir «Annulation manuelle de la configuration du collecteur de données pour WebSphere Application Server Liberty», à la page 160.

Annulation manuelle de la configuration du collecteur de données pour WebSphere Application Server traditionnel

Procédure

1. Connectez-vous à la console d'administration WebSphere en tant qu'administrateur.
2. Dans le panneau de navigation, cliquez sur **Servers**, développez **Server Type** et cliquez sur **WebSphere application servers**.
3. Cliquez sur le nom du serveur d'applications.
4. Dans la section **Server Infrastructure** de l'onglet Configuration, développez **Java Virtual Machine** et cliquez sur **Process Definition**.
5. Dans la section **Propriétés supplémentaires**, cliquez sur **Machine virtuelle Java**.
6. Dans la zone **Generic JVM arguments**, supprimez les entrées suivantes du contenu.

   ```
   -agentlib:am_ibm_16=${WAS_SERVER_NAME} -Xbootclasspath/p:${ITCAMDCHOME}/
   toolkit/lib/bcm-bootstrap.jar -Djava.security.policy=${ITCAMDCHOME}/itcamdc/
   etc/datacollector.policy -verbosegc
   ```

7. Cliquez sur **Appliquer**, puis sur **Sauvegarder**. Dans la boîte de dialogue Sauvegarde dans la configuration principale, effectuez les opérations suivantes :
   - Si vous êtes dans un environnement de déploiement réseau, vérifiez que **Synchroniser les modifications avec les noeuds** est sélectionné, puis cliquez sur **Sauvegarder**.
   - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
8. Dans le panneau de navigation, cliquez sur **Servers**, développez **Server Types**, cliquez sur **WebSphere application servers**, puis cliquez sur le nom du serveur.
9. Dans l'onglet Configuration, accédez à **Infrastructure du serveur** > **Gestion des processus et Java** > **Définition des processus** > **Entrées d'environnement**.
10. Selon le système d'exploitation, la plateforme matérielle et la machine virtuelle Java de serveur d'applications utilisés, supprimez l'entrée d'environnement suivante.
    - UNIX LIBPATH
    - Linux LD_LIBRARY_PATH
    - Windows PATH
11. Dans le panneau de navigation, cliquez sur **Environnement** > **Variables WebSphere**.
12. Supprimez la variable *ITCAMDCHOME* si elle existe.
13. Cliquez sur **Appliquer**, puis sur **Sauvegarder**. Dans la boîte de dialogue Sauvegarde dans la configuration principale, effectuez les opérations suivantes :
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que **Synchroniser les modifications avec les noeuds** est sélectionné, puis cliquez sur **Sauvegarder**.
    - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
14. Redémarrez l'instance du serveur d'applications.

15. Accédez au répertoire `runtime` dans le répertoire d'installation de l'agent et supprimez le fichier *nom_profil.nom_cellule.nom_noeud.nom_serveur*`.manual.input.properties`.
    - Linux AIX *rép_install*`/yndchome/7.3.0.14.08/runtime/`*profile_name.cell_name.node_name.server_name*`.manual.input.properties`
    - Windows *rép_install*`\dchome\7.3.0.14.08\runtime\`*profile_name.cell_name.node_name.server_name*`.manual.input.properties`

Annulation manuelle de la configuration du collecteur de données pour WebSphere Application Server Liberty

Procédure

1. Accédez au répertoire du serveur Liberty et ouvrez le fichier `jvm.options` dans le répertoire *nom_serveur* au sein du répertoire d'installation du serveur Liberty. Par exemple, `/opt/ibm/wlp/usr/servers/defaultServer`.
2. Supprimez les paramètres suivants du fichier `jvm.options`.

```
-agentlib:am_ibm_16=nom_serveur
–Xbootclasspath/p:base_cd/toolkit/lib/bcm-bootstrap.jar
-Djava.security.policy=base_cd/itcamdc/etc/datacollector.policy
-verbosegc
```

   où *nom_serveur* est le nom du serveur Liberty et *base_cd* est le répertoire de base du collecteur de données.
3. Ouvrez le fichier `server.xml` et supprimez les lignes suivantes :

```
<feature>webProfile-7.0</feature>
<feature>monitor-1.0</feature>
<feature>usr:itcam-730.140</feature>
```

4. Ouvrez le fichier `server.env` et supprimez la valeur d'entrée suivante de l'entrée d'environnement selon le système d'exploitation :

Tableau 8. Entrée d'environnement

Plateforme	Nom de l'entrée d'environnement	Valeur de l'entrée d'environnement
AIX R6.1 (machine virtuelle Java 64 bits)	LIBPATH	`/lib:`*base_cd*`/toolkit/lib/aix536`
AIX R7.1 (machine virtuelle Java 64 bits)	LIBPATH	`/lib:`*base_cd*`/toolkit/lib/aix536`
Solaris 10 (machine virtuelle Java 64 bits)	LIBPATH	`/lib:`*base_cd*`/toolkit/lib/sol296`
Solaris 11 (machine virtuelle Java 64 bits)	LIBPATH	`/lib:`*base_cd*`/toolkit/lib/sol296`
Linux x86_64 R2.6 (machine virtuelle Java 64 bits)	LD_LIBRARY_PATH	`/lib:`*base_cd*`/toolkit/lib/lx8266`
Linux Intel R2.6 (machine virtuelle Java 32 bits)	LD_LIBRARY_PATH	`/lib:`*base_cd*`/toolkit/lib/li6263`
Windows (machine virtuelle Java 32 bits)	PATH	`/lib;`*base_cd*`/toolkit/lib/win32`

Tableau 8. Entrée d'environnement (suite)		
Plateforme	**Nom de l'entrée d'environnement**	**Valeur de l'entrée d'environnement**
Windows (machine virtuelle Java 64 bits)	PATH	/lib;*base_cd*/toolkit/lib/win64

5. Redémarrez le serveur Liberty.
6. Accédez au répertoire `runtime` dans le répertoire d'installation de l'Agent WebSphere Applications et supprimez le fichier *nom_cellule.nom_noeud.nom_serveur*`.manual.input.properties`.
   - Linux AIX *rép_install*`/yndchome/7.3.0.14.08/runtime/`*cell_name.node_name.server_name*`.manual.input.properties`
   - Windows *rép_install*`\dchome\7.3.0.14.08\runtime\`*cell_name.node_name.server_name*`.manual.input.properties`

Agent Node.js : Retrait du plug-in de surveillance

Avant de désinstaller l'Agent Node.js, vous devez retirer le plug-in de surveillance de votre application Node.js.

Procédure

1. Supprimez les plug-in de collecteur de données au début du fichier d'application Node.js :
   - Si vous mettez à niveau l'Agent Node.js à partir de la version 01.00.12.00 vers la version 01.00.13.00, procédez comme suit :
     - Si vous avez activé la collecte des données de ressource, supprimez la ligne ci-après au début du fichier d'application Node.js :

       ```
       require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_index.js');
       ```

       où *KNJ_NPM_LIB_LOCATION* correspond au répertoire du dossier `lib` de votre répertoire d'installation global du package npm. Le répertoire par défaut est `/usr/local/lib`.
     - Si vous avez activé la collecte des données de ressource et la collecte des données de diagnostics approfondis, supprimez la ligne ci-après au début du fichier d'application Node.js :

       ```
       require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_deepdive.js');
       ```

     - Si vous avez activé la collecte des données de ressource, la collecte des données de diagnostics approfondis et la collecte des traces de méthode, supprimez la ligne ci-après au début du fichier d'application Node.js :

       ```
       require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_methodtrace.js');
       ```

   - Si vous mettez à niveau l'Agent Node.js à partir de la version 01.00.12.00 vers la version 01.00.13.00, procédez comme suit :
     - Si vous avez activé la collecte des données de ressource, supprimez la ligne ci-après au début du fichier d'application Node.js.

       ```
       require('rép_install/lx8266/nj/bin/plugin/knj_index.js');
       ```

       , où *rép_install* correspond au répertoire d'installation de l'Agent Node.js.
     - Si vous avez activé la collecte des données de ressource et la collecte des données de diagnostics approfondis, supprimez la ligne ci-après au début du fichier d'application Node.js.

       ```
       require('rép_install/lx8266/nj/bin/plugin/knj_deepdive.js');
       ```

– Si vous avez activé la collecte des données de ressource, la collecte des données de diagnostics approfondis et la collecte des traces de méthode, supprimez la ligne ci-après au début du fichier d'application Node.js .

```
require('rép_install/lx8266/nj/bin/plugin/knj_methodtrace.js');
```

2. Redémarrez l'application Node.js pour désactiver les plug-in de collecteur de données.
   - Si la version actuelle de votre Agent Node.js estversion 01.00.10.00, les plug-in du collecteur de données sont supprimés dès maintenant.
   - Si la version de votre Agent Node.js actuel est version 01.00.12.00, continuez à l'étape suivante.
3. Exécutez la commande `./uninstall.sh` à partir du répertoire *rép_install*`/lx8266/nj/bin` pour supprimer les paramètres d'agent précédents.

Que faire ensuite

Pour plus d'informations sur la désinstallation de l'Agent Node.js, voir «Désinstallation de vos agents», à la page 150.

agent Microsoft .NET : Retrait du collecteur de données .NET

Avant de désinstaller l'agent Microsoft .NET, vous devez retirer le collecteur de données .NET de vos applications .NET.

Procédure

1. Désenregistrez le collecteur de données.

   En tant qu'administrateur, entrez :

   ```
   cd rép_install\qe\bin configdc unregisterdc
   ```

   Où *rép_install* correspond au répertoire d'installation de l'agent Microsoft .NET.
2. Arrêtez toutes vos applications .NET pour désactiver le collecteur de données.

   Entrez `net stop was /y`
3. Pour vous assurer du nettoyage complet du collecteur de données .NET après la désinstallation, suivez ces étapes :
   a) A l'invite de commande, accédez au répertoire `<APM_HOME>\qe\bin`.
   b) Exécutez le fichier `ProcListCaller.bat`.
   c) Vérifiez le fichier journal `CorProfAttach.Log` dans le répertoire `<APM_HOME>\qe\logs`. Le fichier journal répertorie les processus auxquels le composant du profileur du collecteur de données .NET est connecté.
   d) Avant de désinstaller l'agent, arrêtez les processus du fichier `CorProfAttach.Log`.
   e) Si aucun processus n'est répertorié, désinstallez l'agent.

Que faire ensuite

Désinstallez l'agent Microsoft .NET. Voir «Désinstallation de vos agents», à la page 150.

Chapitre 7. Configuration de votre environnement

Si votre agent de surveillance requiert une configuration ou que vous souhaitez consulter les paramètres par défaut d'un agent, suivez les étapes fournies pour votre agent.

Rubriques communes

Certaines rubriques sont communes lors de la configuration des agents et des collecteurs de données.

Connectivité réseau

Pour vous assurer que les communications agent-serveur sont établies, testez la connexion de votre système au serveur Cloud APM.

Pour valider les communications, testez votre connectivité au centre de données Cloud APM. Pour veiller à ce que vos règles de pare-feu autorisent le trafic à partir de trois adresses IP spécifiques et du port 443, trouvez les trois adresses IP du centre de données dont vous avez besoin pour vérifier la connexion. Pour plus d'informations, voir Data Center IP addresses (SaaS only) dans Application Performance Management Developer Center. Vérifiez que vos agents peuvent se connecter à ces trois adresses IP à l'aide de la commande **openssl**. Pour plus d'informations sur l'utilisation de la commande **openssl**, voir Configuration des agents pour qu'ils communiquent via un proxy direct. Si vos agents ne peuvent pas se connecter, contactez votre équipe informatique locale. Celle-ci peut ajuster vos règles de pare-feu, activer le port 443 et activer le trafic TLS 1.2 à partir de vos serveurs, ou configurer un serveur proxy pour se connecter au serveur Cloud APM.

Si vos règles de pare-feu n'autorisent pas les connexions HTTPS sortantes transparentes à des hôtes externes, vous pouvez configurer vos agents de sorte qu'ils envoient le trafic à un proxy direct. Pour plus d'informations, voir «Configuration des agents pour qu'ils communiquent via un proxy direct», à la page 163.

Connectivité du navigateur

Pour vérifier la connectivité du navigateur à la console Cloud APM, localisez l'URL **Lancer** qui vous a été fournie par IBM lors de la mise à disposition de votre abonnement. Vous pouvez également vous connecter à votre compte et démarrer la console. Connectez-vous à la page **Products and Services** (http://ibm.biz/my-prodsvcs) avec vos détails d'abonnement IBM Marketplace. Cliquez sur **Lancer** pour démarrer la console et afficher l'URL, par exemple : `8b68ba1b9.agents.na.apm.ibmserviceengage.com`. Vérifiez que vous pouvez utiliser l'URL pour vous connecter à la console.

Communication sécurisée

La communication sécurisée entre les agents et le serveur Cloud APM nécessite TLS 1.2.

La communication entre les agents et le serveur Cloud APM dans IBM Cloud utilise HTTPS avec TLS 1.2 et les suites de chiffrement FIPS Suite B. Les chiffrements suivants sont utilisés :

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

La communication entre le navigateur et le serveur Cloud APM nécessite également TLS 1.2. Sur certains navigateurs, TLS 1.2 n'est pas activé par défaut ; il doit alors être activé manuellement.

Configuration des agents pour qu'ils communiquent via un proxy direct

Si vos règles de pare-feu n'autorisent pas les connexions HTTPS sortantes transparentes à des hôtes externes, vous devez configurer les agents de surveillance IBM de sorte qu'ils envoient le trafic à un proxy

direct. Editez la variable d'environnement KDH_FORWARDPROXY pour configurer les agents de sorte qu'ils communiquent via un proxy direct.

Avant de commencer

Pour déterminer l'adresse IP du centre de données Cloud APM auquel vos agents se connectent, voir Adresses IP du centre de données (APM Developer Center). Ajustez ensuite vos règles de pare-feu pour autoriser l'envoi des demandes à ces adresses IP à partir de votre proxy direct.

Vous pouvez utiliser la commande **openssl** pour vérifier si le système informatique où vos agents sont installés dispose d'une connectivité aux serveurs du centre de données Cloud APM. Vous pouvez également utiliser la commande **openssl** pour vérifier que votre réseau prend en charge les suites de chiffres utilisées par Cloud APM. Si les résultats de la commande **openssl** indiquent que le système informatique ne peut pas se connecter, vous devrez peut-être configurer un proxy direct. Si les résultats de la commande indiquent qu'il est impossible d'obtenir le certificat du serveur Cloud APM, travaillez de concert avec votre équipe réseau pour déterminer pourquoi les suites de chiffrement requises ne sont pas prises en charge. Pour obtenir la liste des suites de chiffrement utilisées par le Cloud APM, voir «Communication sécurisée», à la page 163.

Exécutez la commande **openssl**, comme indiqué dans l'exemple suivant :

```
echo quit | openssl s_client
-state -connect <nom-domaine>:443
-tls1_2 -cipher
ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384
```

où *nom-domaine* est le nom de domaine de votre abonnement Cloud APM (par exemple, `8b68ba1b9.agents.na.apm.ibmserviceengage.com`).

Pour déterminer le nom de domaine de votre abonnement, procédez comme suit :

1. Ouvrez le fichier de configuration d'environnement d'agent dans un éditeur de texte :

   Linux AIX `/opt/ibm/apm/agent/config/global.environment`

   Windows `rép_install\TMAITM6_x64\Kcp`ENV pour les systèmes Windows 64 bits et `rép_install\TMAITM6\Kcp`ENV pour les systèmes Windows 32 bits, où *cp* est le code produit de l'agent.

   Pour une liste des codes produit, voir «Utilisation des commandes de l'agent», à la page 181.

2. Recherchez la variable *IRA_ASF_SERVER_URL*. Cette valeur est au format `https://nom-domaine/ccm/asf/request`. Utilisez la portion de nom de domaine de la valeur avec la commande **openssl**.

Si la connexion aboutit, des messages semblables à ceux de l'exemple suivant sont affichés :

```
CONNECTED(00000003)
SSL_connect:before/connect initialization
SSL_connect:SSLv3 write client hello A
SSL_connect:SSLv3 read server hello A
depth=2 C = US, O = IBM Service Engage,
CN = ca_ec_384.ibmserviceengage.com
verify error:num=19:self signed certificate in certificate chain
verify return:0
SSL_connect:SSLv3 read server certificate A
SSL_connect:SSLv3 read server key exchange A
SSL_connect:SSLv3 read server certificate request A
SSL_connect:SSLv3 read server done A
SSL_connect:SSLv3 write client certificate A
SSL_connect:SSLv3 write client key exchange A
SSL_connect:SSLv3 write change cipher spec A
SSL_connect:SSLv3 write finished A
SSL_connect:SSLv3 flush data
SSL_connect:SSLv3 read finished A
```

```
---
Certificate chain
0 s:/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=*.agents.na.apm.ibmserviceengage.com
i:/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN =ca_ec_384.apm.ibmserviceengage.com
1 s:/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=ca_ec_384.apm.ibmserviceengage.com
i:/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
2 s:/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
i:/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICkjCCAhegAwIBAgIIXlr284nLPaMwDAYIKoZIzj0EAwMFADCBhDELMAkGA1UE
BgwCVVMxGzAZBgNVBAoMEklCTSBTZXJ2aWNlIEVuZ2FnZTErMCkGA1UECwwiQXBw
bGljYXRpb24gUGVyZm9ybWFuY2UgTWFuYWdlbWVudDErMCkGA1UEAwwiY2FfZWNf
Mzg0LmFwbS5pYm1zZXJ2aWNlZW5nYWdlLmNvbTAeFw0xMzEyMDIxNjM2MDlaFw0y
MzEyMDExNjM2MDlaMIGGMQswCQYDVQQGDAJVUzEbMBkGA1UECgwSSUJNIFNlcnZp
Y2UgRW5nYWdlMSswKQYDVQQLDCJBcHBsaWNhdGlvbiBQZXJmb3JtYW5jZSBNYW5h
Z2VtZW50MS0wKwYDVQQDDCQqLmFnZW50cy5uYS5hcG0uaWJtc2VydmljZWVuZ2Fn
ZS5jb20wdjAQBgcqhkjOPQIBBgUrgQQAIgNiAAQmrGoCkAMoNAC3F6MIo1zR8fcO
mczYXtUux2bhlOibn3jQdxamhDR91nr2RBerGjMIITKNXd2MaOr3b6m8euk1BAL3
KsbN9lqvw94kXg0BTO1IHAcdsZQB+AuEVVhmDVGjUDBOMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAU/zpE5TOnQ8LSuvbSWRfpbiGea08wHQYDVR0OBBYEFHL0At4O
GUdcOHVGg4Tfo4hl7LLGMAwGCCqGSM49BAMDBQADZwAwZAIwDWPHo5I04ZFVrkfk
St6gwH2UNF37jBscRN1lOE4SIwezZAqVs42BNMkWRjJBgiHzAjBm4m3zOjsXzNL8
+u8ALjQQCpBDT6dUHujzY5CRxG0xEHi5IXsXf4QwbctnjjvTeYA=
-----END CERTIFICATE-----
subject=/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=*.agents.na.apm.ibmserviceengage.com
issuer=/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=ca_ec_384.apm.ibmserviceengage.com
---
Acceptable client certificate CA names
/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=ca_ec_384.apm.ibmserviceengage.com
/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert
Global Root CA/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=*.agents.na.apm.ibmserviceengage.com
Server Temp Key: ECDH, prime256v1, 256 bits
---
SSL handshake has read 2659 bytes and written 261 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-ECDSA-AES128-GCM-SHA256
Server public key is 384 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1.2
Cipher : ECDHE-ECDSA-AES128-GCM-SHA256
Session-ID:
A18C31D0B45A1166357C917E1CFCD86A9FBEDB4A0EB768EF5390AC28C95CB7EF
Session-ID-ctx:
Master-Key:
252B8FE2731E51AC0B79A27C7BED33CA8B15AF4CFD015C98DBACA46EA01DC40B
```

```
9E6B56E62E0F332FF6B56266B5ADD7B0
Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1510772474
Timeout : 7200 (sec)
Verify return code: 19 (self signed certificate in certificate chain)
---
DONE
SSL3 alert write:warning:close notify
```

Si le système informatique ne peut pas se connecter au serveur Cloud APM, des messages semblables à ceux de l'exemple suivant sont affichés :

```
getaddrinfo: Name or service not known
connect:errno=2
```

Si le système informatique ne peut pas obtenir le certificat du serveur, par exemple, en raison d'un blocage des suites de chiffrement sur le réseau, des messages semblables à ceux de l'exemple suivant sont affichés :

```
SSL_connect:failed
---
no peer certificate available
---
No client certificate CA names sent
```

Pourquoi et quand exécuter cette tâche

Lorsqu'un proxy direct est utilisé, l'agent ouvre au préalable une connexion TCP au proxy. L'agent envoie une demande HTTP CONNECT et l'URL du noeud final cible (serveur Cloud APM) au proxy direct. Le proxy direct établit alors une connexion TCP au noeud final cible et crée une session de tunnellisation HTTPS entre l'agent et le serveur Cloud APM.

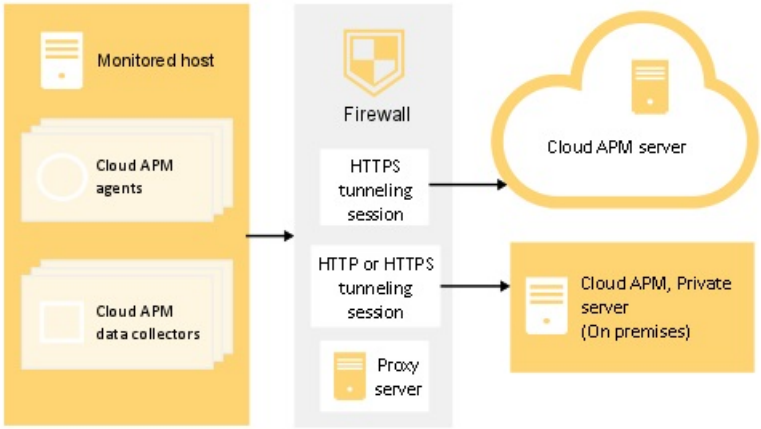


Figure 1. Diagramme de connexion pour l'utilisation d'un proxy direct

L'agent de surveillance ne prend pas en charge les proxys d'authentification, ce qui signifie que l'agent ne prend pas en charge la connexion à un proxy direct à l'aide d'un ID utilisateur et d'un mot de passe de proxy configurés.

Procédure

1. Ouvrez le fichier de configuration d'environnement d'agent dans un éditeur de texte :

Linux AIX Fichier *rép_install*/config/global.environment, où *rép_install* est le répertoire de base d'installation des agents. Le fichier global.environment configure tous les agents dans le répertoire d'installation.

Les paramètres personnalisés du fichier .global.environment sont perdus après la mise à niveau de l'agent. Pour conserver vos paramètres, effectuez les modifications de personnalisation dans les fichiers global.environment. Les paramètres de ce fichier ne sont pas écrasés par une mise à niveau de l'agent.

Windows Fichier *rép_install*\TMAITM6_x64\K*cp*ENV pour les agents 64 bits et fichier *rép_install*\TMAITM6\K*cp*ENV pour les agents 32 bits où *cp* est le code produit de l'agent. Configurez le fichier K*cp*ENV pour chaque agent.

Pour une liste des codes produit, voir «Utilisation des commandes de l'agent», à la page 181.

2. Editez la variable d'environnement KDH_FORWARDPROXY pour indiquer l'adresse et le port du proxy :

```
KDH_FORWARDPROXY=http://adresse-proxy:numéro-port-proxy
```

Exemple :

```
KDH_FORWARDPROXY=http://HostA:8085
```

3. Redémarrez l'agent pour implémenter les modifications. Voir «Utilisation des commandes de l'agent», à la page 181 .

Configuration des collecteurs de données pour qu'ils communiquent via un proxy direct

Si vos règles de pare-feu n'autorisent pas les connexions HTTPS sortantes transparentes à des hôtes externes, vous pouvez configurer les collecteurs de données pour l'envoi du trafic à un proxy direct. Editez la variable d'environnement APM_GW_PROXY_CONNECTION pour configurer les collecteurs de données pour la communication via un proxy direct.

Avant de commencer

Pour déterminer l'adresse IP du centre de données Cloud APM auquel sont connectés vos collecteurs de données, voir Adresses IP du centre de données (APM Developer Center). Ajustez ensuite vos règles de pare-feu pour autoriser l'envoi des demandes à ces adresses IP à partir de votre proxy direct.

Vous pouvez utiliser la commande **openssl** pour vérifier si le système informatique où sont installés vos collecteurs de données dispose d'une connectivité aux serveurs du centre de données Cloud APM. Vous pouvez également vérifier que votre réseau prend en charge les suites de chiffrement utilisées par Cloud APM. Si les résultats de la commande **openssl** indiquent que le système informatique ne peut pas se connecter, vous devrez peut-être configurer un proxy direct. Si les résultats de la commande indiquent qu'il est impossible d'obtenir le certificat du serveur Cloud APM, travaillez de concert avec votre équipe réseau pour déterminer pourquoi les suites de chiffrement requises ne sont pas prises en charge. Pour obtenir la liste des suites de chiffrement utilisées par le Cloud APM, voir «Communication sécurisée», à la page 163.

Exécutez la commande **openssl**, comme indiqué dans l'exemple suivant :

```
echo quit | openssl s_client
-state -connect <nom-domaine>:443
-tls1_2 -cipher
ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384
```

où *nom-domaine* est le nom de domaine pour votre abonnement Cloud APM.

Pour déterminer le nom de domaine de votre abonnement, voir «Configuration des agents pour qu'ils communiquent via un proxy direct», à la page 163.

Si la connexion aboutit, des messages semblables à ceux de l'exemple suivant sont affichés :

```
CONNECTED(00000003)
SSL_connect:before/connect initialization
SSL_connect:SSLv3 write client hello A
SSL_connect:SSLv3 read server hello A
```

```
depth=2 C = US, O = IBM Service Engage,
CN = ca_ec_384.ibmserviceengage.com
verify error:num=19:self signed certificate in certificate chain
verify return:0
SSL_connect:SSLv3 read server certificate A
SSL_connect:SSLv3 read server key exchange A
SSL_connect:SSLv3 read server certificate request A
SSL_connect:SSLv3 read server done A
SSL_connect:SSLv3 write client certificate A
SSL_connect:SSLv3 write client key exchange A
SSL_connect:SSLv3 write change cipher spec A
SSL_connect:SSLv3 write finished A
SSL_connect:SSLv3 flush data
SSL_connect:SSLv3 read finished A
---
Certificate chain
0 s:/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=*.agents.na.apm.ibmserviceengage.com
i:/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN =ca_ec_384.apm.ibmserviceengage.com
1 s:/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=ca_ec_384.apm.ibmserviceengage.com
i:/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
2 s:/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
i:/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICkjCCAhegAwIBAgIIXlr284nLPaMwDAYIKoZIzj0EAwMFADCBhDELMAkGA1UE
BgwCVVMxGzAZBgNVBAoMEklCTSBTZXJ2aWNlIEVuZ2FnZTErMCkGA1UECwwiQXBw
bGljYXRpb24gUGVyZm9ybWFuY2UgTWFuYWdlbWVudDErMCkGA1UEAwwiY2FfZWNf
Mzg0LmFwbS5pYm1zZXJ2aWNlZW5nYWdlLmNvbTAeFw0xMzEyMDIxNjM2MDlaFw0y
MzEyMDExNjM2MDlaMIGGMQswCQYDVQQGDAJVUzEbMBkGA1UECgwSSUJNIFNlcnZp
Y2UgRW5nYWdlMSswKQYDVQQLDCJBcHBsaWNhdGlvbiBQZXJmb3JtYW5jZSBNYW5h
Z2VtZW50MS0wKwYDVQQDDCQqLmFnZW50cy5uYS5hcG0uaWJtc2VydmljZWVuZ2Fn
ZS5jb20wdjAQBgcqhkjOPQIBBgUrgQQAIgNiAAQmrGoCkAMoNAC3F6MIo1zR8fcO
mczYXtUux2bhlOibn3jQdxamhDR91nr2RBerGjMIITKNXd2MaOr3b6m8euk1BAL3
KsbN9lqvw94kXg0BTO1IHAcdsZQB+AuEVVhmDVGjUDBOMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAU/zpE5TOnQ8LSuvbSWRfpbiGea08wHQYDVR0OBBYEFHL0At4O
GUdcOHVGg4Tfo4hl7LLGMAwGCCqGSM49BAMDBQADZwAwZAIwDWPHo5I04ZFVrkfk
St6gwH2UNF37jBscRN1lOE4SIwezZAqVs42BNMkWRjJBgiHzAjBm4m3zOjsXzNL8
+u8ALjQQCpBDT6dUHujzY5CRxG0xEHi5IXsXf4QwbctnjjvTeYA=
-----END CERTIFICATE-----
subject=/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=*.agents.na.apm.ibmserviceengage.com
issuer=/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=ca_ec_384.apm.ibmserviceengage.com
---
Acceptable client certificate CA names
/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=ca_ec_384.apm.ibmserviceengage.com
/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert
Global Root CA/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=*.agents.na.apm.ibmserviceengage.com
Server Temp Key: ECDH, prime256v1, 256 bits
---
SSL handshake has read 2659 bytes and written 261 bytes
```

```
---
New, TLSv1/SSLv3, Cipher is ECDHE-ECDSA-AES128-GCM-SHA256
Server public key is 384 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1.2
Cipher : ECDHE-ECDSA-AES128-GCM-SHA256
Session-ID:
A18C31D0B45A1166357C917E1CFCD86A9FBEDB4A0EB768EF5390AC28C95CB7EF
Session-ID-ctx:
Master-Key:
252B8FE2731E51AC0B79A27C7BED33CA8B15AF4CFD015C98DBACA46EA01DC40B
9E6B56E62E0F332FF6B56266B5ADD7B0
Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1510772474
Timeout : 7200 (sec)
Verify return code: 19 (self signed certificate in certificate chain)
---
DONE
SSL3 alert write:warning:close notify
```

Si le système informatique ne peut pas se connecter au serveur Cloud APM, des messages semblables à ceux de l'exemple suivant sont affichés :

```
getaddrinfo: Name or service not known
connect:errno=2
```

Si le système informatique ne peut pas obtenir le certificat du serveur, par exemple, en raison d'un blocage des suites de chiffrement sur le réseau, des messages semblables à ceux de l'exemple suivant sont affichés :

```
SSL_connect:failed
---
no peer certificate available
---
No client certificate CA names sent
```

Pourquoi et quand exécuter cette tâche

Lorsqu'un proxy direct est utilisé, le collecteur de données ouvre au préalable une connexion TCP au proxy. Le collecteur de données envoie une demande de connexion et l'URL du noeud final cible (serveur serveur Cloud APM) au proxy direct. Le proxy direct établit alors une connexion TCP au noeud final cible et crée une session de tunnellisation HTTPS entre le collecteur de données et le serveur Cloud APM.

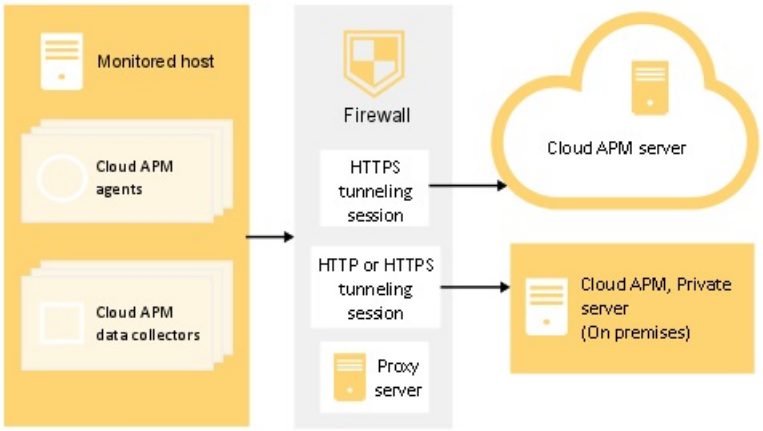


Figure 2. Diagramme de connexion pour l'utilisation d'un proxy direct

Certains collecteurs de données prennent en charge des proxy d'authentification, comme par exemple les collecteurs de données Node.js et Liberty. Ils prennent en charge la connexion à un proxy direct en utilisant un ID utilisateur et un mot de passe de proxy configuré.

Procédure

1. Pour configurer la communication de proxy direct pour les collecteurs de données Python, exécutez l'une des étapes suivantes :
   - Ouvrez le fichier de propriétés *<base_cd>*`/config.properties` du collecteur de données dans un fichier d'éditeur de texte, *<base_cd>* représentant le répertoire de base d'installation des collecteurs de données, par exemple, `/usr/lib/python2.7/site-packages/ibm_python_dc`. Mettez à jour la variable avec l'hôte et le numéro de port du proxy, par exemple `APM_GW_PROXY_CONNECTION =http://9.181.138.247:8085`. La modification de la variable dans ce fichier a une incidence sur toutes les applications dans lesquelles le collecteur de données Python est activé.

     Remarque : Pour configurer la communication d'un proxy direct pour une seule application, copiez le fichier *<base_cd>*`/config.properties` dans le répertoire de l'application unique. Mettez à jour la variable dans le répertoire de l'application.
   - Exécutez la commande suivante sur des systèmes Linux :

     ```
     export APM_GW_PROXY_CONNECTION =http://<hôte du proxy http>:<port du proxy http>
     ```

     par exemple,

     ```
     export APM_GW_PROXY_CONNECTION =http://9.181.138.247:8085
     ```
2. Pour configurer la communication de proxy direct pour les collecteurs de données Node.js, exécutez l'une des étapes suivantes :
   - Exécutez la commande suivante sur des systèmes Linux :

     ```
     export APM_GW_PROXY_CONNECTION =http://<hôte du proxy http>:<port du proxy http>
     ```

     par exemple,

     ```
     export APM_GW_PROXY_CONNECTION =http://9.181.138.247:8085
     ```
   - Si un nom d'utilisateur et un mot de passe sont requis pour l'accès au serveur proxy direct pour les collecteurs de données Node.js, exécutez la commande suivante sur des systèmes Linux :

     ```
     export APM_GW_PROXY_CONNECTION =http://<utilisateur du proxy http>:
     <mot de passe du proxy http>@<hôte du proxy http>:<port du proxy http>
     ```

par exemple,

```
export APM_GW_PROXY_CONNECTION =http://Joe:passw0rd@9.181.138.247:8085
```

3. Pour configurer la communication du proxy direct pour les collecteurs de données Liberty, modifiez le fichier *<base serveur Liberty>*/jvm.options, où *<base serveur Liberty>* est le répertoire de base du serveur Liberty, par exemple : /opt/ibm/wlp/usr/servers/defaultServer/jvm.options. Effectuez l'une des étapes suivantes :
   - Si l'authentification n'est pas requise, ajoutez le code suivant au fichier jvm.options :

     ```
     -Dhttp.proxyHost=<hôte du proxy http>
     -Dhttp.proxyPort=<port du proxy http>
     -Dhttps.proxyHost=<hôte du proxy https>
     -Dhttps.proxyPort=<port du proxy https>
     -Djava.net.useSystemProxies=true
     ```

   - Si un nom d'utilisateur et un mot de passe sont requis pour accéder au serveur proxy direct, ajoutez le code suivant au fichier jvm.options :

     ```
     -Dhttp.proxyHost=<hôte du proxy http>
     -Dhttp.proxyPort=<port du proxy http>
     -Dhttp.proxyUser=<utilisateur du proxy http>
     -Dhttp.proxyPassword=<mot de passe du proxy http>
     -Dhttps.proxyHost=<hôte du proxy https>
     -Dhttps.proxyPort=<port du proxy https>
     -Dhttps.proxyUser=<utilisateur du proxy https>
     -Dhttps.proxyPassword=<mot de passe du proxy https>
     -Djava.net.useSystemProxies=true
     ```

4. Redémarrez l'application locale pour implémenter les modifications.

Résultats
Vous avez configuré vos collecteurs de données pour qu'ils communiquent via un proxy direct.

Noms de systèmes gérés

Le nom de système géré (MSN) est utilisé pour identifier chaque agent Cloud APM dans votre environnement. Il s'agit également du nom d'instance qui apparaît sur le Tableau de bord d'Application Performance lorsque vous sélectionnez un groupe pour chaque système géré à partir de la section **Groupes** du navigateur. Pour éviter tout conflit, affectez des MSN uniques à vos agents.

Le format du MSN de l'agent varie en fonction du type d'agent. Il peut appartenir à l'une des catégories suivantes :

- «Format de MSN commun pour les agents à instance unique», à la page 171
- «Format de MSN commun pour les agents multi-instance», à la page 172
- «Format de MSN spécial», à la page 173

Format de MSN commun pour les agents à instance unique

Pour la plupart des agents à instance unique, le format commun du MSN est le suivant :

```
nom_hôte:pc
```

où :

- *nom_hôte* est le nom de l'ordinateur sur lequel l'agent est installé. Cette partie peut être modifiée au besoin.
- *pc* est le code d'agent à deux caractères en majuscules qui est non modifiable. Pour plus d'informations sur les codes des agents, voir «Utilisation des commandes de l'agent», à la page 181.
- : est le séparateur qui est non modifiable.

Exemple : linuxhost01:LZ est le MSN de l'Linux OS.

Les agents à instance unique qui ne respectent pas ce format de MSN sont répertoriés dans le Tableau 9, à la page 173.

Le MSN est limité à 32 caractères. Pour cette catégorie de MSN, 29 caractères peuvent être saisis pour le nom d'hôte car le code agent et le séparateur ne peuvent pas être modifiés.

Important : Si la longueur du MSN dépasse 32 caractères, une partie du MSN est tronquée et le MSN ne s'affiche pas correctement dans la console Cloud APM. Par exemple, si votre nom d'hôte est `VeryLongSalesDivisionServerName03`, votre nom de système géré doit être `VeryLongSalesDivisionServerName03:`*PC*, mais il sera tronqué à `VeryLongSalesDivisionServerName0`.

Format de MSN commun pour les agents multi-instance

Pour la plupart des agents multi-instance, le format commun du MSN est le suivant :

```
nom_instance:nom_hôte:pc
```

où :

- *nom_instance* est le nom de l'instance d'agent que vous spécifiez lors de la configuration de l'agent. Utilisez cette variable afin de garantir un MSN unique pour chaque instance de type d'agent sur chaque ordinateur hôte d'agent.

  A faire :

  – Les lettres de l'alphabet latin (a-z, A-Z), les chiffres arabes (0-9) et le trait d'union (-) peuvent être utilisés pour créer les noms d'instance d'agent.
  – Le caractère de soulignement (_) n'est pas autorisé dans les noms d'instance d'agent.
  – Le nom d'instance que vous indiquez est limité de la façon suivante :
    - Linux AIX 28 caractères moins la longueur de votre nom d'hôte sur les systèmes Linux ou AIX.
    - Windows 28 caractères moins la longueur de votre nom d'hôte lorsqu'un fichier de réponses silencieux est utilisé pour la configuration sur les systèmes Windows. Par exemple, si `Server-Name` comporte 11 caractères, les instances d'agent sur l'hôte `Server-Name` doivent donc comporter au maximum 17 caractères.
    - Windows 20 caractères moins la longueur par laquelle votre nom d'hôte dépasse 8 caractères lorsque la configuration de la console Cloud APM est utilisée sur les systèmes Windows. Par exemple, si `TestServer` comporte 10 caractères, qui dépasse 8 fois 2, les instances d'agent sur l'hôte `TestServer` doivent donc comporter au maximum 18 caractères.
- *nom_hôte* est le nom de l'ordinateur sur lequel l'agent est installé. Le composant de nom d'hôte du MSN peut être modifié si nécessaire.
- *pc* est le code d'agent à deux caractères en majuscules qui est non modifiable. Pour plus d'informations sur les codes des agents, voir «Utilisation des commandes de l'agent», à la page 181.
- `:` est le séparateur et ne peut pas être modifié.

Exemple : `jboss1:win2016:JE` est le MSN de l'agent JBoss.

Les agents multi-instance qui ne respectent pas ce format de MSN sont répertoriés dans le Tableau 9, à la page 173.

Le MSN est limité à 32 caractères. Pour cette catégorie de MSN, 28 caractères peuvent être saisis entre le nom d'instance et le nom d'hôte car le code agent et le séparateur ne peuvent pas être modifiés.

Important : Si la longueur du MSN dépasse 32 caractères, une partie du MSN est tronquée et le MSN ne s'affiche pas correctement dans la console Cloud APM. Par exemple, si vous indiquez `VeryLongInstanceName` comme nom d'instance et que le nom de serveur est `Production09`, le nom du système géré doit être `VeryLongInstanceName:Production09:`*PC*. Toutefois, il sera tronqué à `VeryLongInstanceName:Production0`.

Format de MSN spécial

Le format de MSN spécial s'applique aux agents dont les MSN ne respectent pas les deux formats communs de MSN décrits ci-dessus. Ces agents sont répertoriés dans le Tableau 9, à la page 173.

Le MSN spécial est limité à 32 caractères. Dans le Tableau 9, à la page 173, seules les chaînes en italique figurant la colonne du format de MSN peuvent être modifiées.

Tableau 9. Format de MSN spécial

Agents	Format de MSN	Exemple de MSN
agent Amazon EC2	B5:*nom_sousnoeud_ec2*:INS	B5:sales:INS
agent Amazon ELB	• AL:*nom_instance*A:APP • AL:*nom_instance*C:CLA • AL:*nom_instance*N:NET	• AL:elb-inst3A:APP • AL:elb-inst3C:CLA • AL:elb-inst3N:NET
Agent Azure Compute	AK:*nom_sousnoeud_azure_compute*:AVM	AK:azc-inst3:AVM
agent Citrix VDI	VD:*nom_site_citrix*:XDS	VD:xds1:XDS
agent DataPower	BN:*nom_système_datapower*:DPS	BN:datapower23:DPS
agent HTTP Server	HU:*alias_nomhôte*:HUS	HU:docker-ihs_httpd:HUS
agent IBM Integration Bus	*nom_courtier_surveillé*:*IDagent*:KQIB	TRADEBRK:AGT1:KQIB
Agent MQ Appliance	MK:*nomsection_nomhôte*:ARM	MK:bvtmin_linux150:ARM
Agent Node.js	NJ:*port_nomhôte*:NJA	NJ:KVM-014179_3000:NJA
Agent Oracle Database	• RZ:*nomhôte-nominstance_connexionbdd*:ASM • RZ:*nomhôte-nominstance_connexionbdd*:DG • RZ:*nomhôte-nominstance_connexionbdd*:RDB	RZ:11g-oracledbdemo-GVT-1BL:RDB
Agent Ruby	KM:*nomapp_nomhôte*:RAP	KM:nc9098036112_Blog:RAP
Agent SAP	• Instance SAP : *numéroinstance_IDs_nominstance-nomhôte*:Ins • SAP Process Integration : *nominstance-nomhôte*:PI • SAP Solution Manager : *nominstance-nomhôte*:Slm • Système SAP : *nominstance-nomhôte*:Sys	• PS5-IBMSAP3V1_PS5_11:Ins • PS5-IBMSAP3V1:PI • PS8-IBMSAP3V3:Slm • PS5-IBMSAP3V1:Sys

Tableau 9. Format de MSN spécial (suite)		
Agents	**Format de MSN**	**Exemple de MSN**
Agent SAP HANA Database	• Base de données SAP Hana : S7:*nombdd-IDsystèmes*:HDB • Système SAP Hana : *nominstance*:*nomhôte*:S7	• S7:HNA-HNA:HDB • HNA:PS8760:S7
Agent SAP NetWeaver Java Stack	• Cluster AS Java de SAP NW : *nominstance*:*nomhôte*:SV • Instance AS Java de SAP NW : SV:*IDsystèmes-IDmvj*:NWJ	• J01:VPT02F17:SV • SV:J01-83309750:NWJ
Agent UNIX OS	*nomhôte*:KUX	worklight17:KUX
Agent WebLogic	WB:*nominstance*:WLS	WB:Server1:WLS
Agent WebSphere Applications	• WebSphere Application Server : *alias_serveur*:*nomhôte*:KYNS • WebSphere Portal Server : *alias_serveur*:*nomhôte*:KYNR • WebSphere Process Server : *alias_serveur*:*nomhôte*:KYNP	simpletrade:worklight17:KYNS
agent WebSphere MQ	*nom_gest_files_attente_surveillé*:*nomagent*:MQ	TRADEQM:PoC:MQ
agent Windows OS	Primary:*nomhôte*:NT	Primary:TRADEIIS1:NT

Modification du nom de système géré de l'agent

Vous pouvez modifier le nom de système géré des agents Cloud APM de différentes manières. Pour certains agents, la modification du nom de système géré implique de modifier le nom d'hôte et/ou le nom d'instance d'agent dans le nom de système géré. Pour les autres agents, des procédures spécifiques sont requises pour modifier le nom de système géré.

Avant de commencer

Familiarisez-vous avec les formats de nom de système géré et les restrictions de dénomination, comme décrit dans «Noms de systèmes gérés», à la page 171.

Pourquoi et quand exécuter cette tâche

Pour la plupart des agents Cloud APM, vous pouvez utiliser le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte utilisé dans le nom de système géré. Pour modifier le nom d'instance de l'agent dans le nom de système géré pour les agents multi-instance, vous pouvez utiliser le paramètre de configuration de l'agent. Si vous avez configuré l'agent, vous devez le reconfigurer pour lui attribuer un autre nom d'instance. Une fois que vous avez reconfiguré l'agent, vous ne pourrez pas récupérer les données collectées par l'instance d'agent précédente.

Selon la partie du nom de système géré que vous voulez modifier, vous ne pourrez peut-être pas modifier le nom de système géré en utilisant une seule procédure.

Pour obtenir la méthode de modification du nom de système géré pour l'agent de votre choix, voir le Tableau 10, à la page 175.

Exception : La modification du nom de système géré n'est pas prise en charge par l'agent HTTP Server, l'Agent Node.js ou l'Agent Synthetic Playback.

Tableau 10. Méthodes de modification du nom de système géré pour les agents Cloud APM

Agent	**Méthode de modification du nom de système géré**
agent Amazon EC2	Utilisez le paramètre de configuration de l'agent pour modifier le nom du sous-noeud EC2 dans le nom de système géré ; voir «Paramètres de configuration de l'agent Amazon EC2», à la page 200.
agent Amazon ELB	Créez une instance d'agent portant un nouveau nom pour modifier le nom de système géré.
Agent Azure Compute	Utilisez le paramètre de configuration de l'agent pour modifier le nom du sous-noeud dans le nom de système géré ; voir «Paramètres de configuration de l'Agent Azure Compute», à la page 215.
agent Cassandra	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
agent Cisco UCS	Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance de l'agent ; voir «Paramètres de configuration de l'agent», à la page 224.
agent Citrix VDI	Utilisez le paramètre de configuration de l'agent pour modifier le nom de site Citrix ; voir «Paramètres de configuration de l'agent Citrix VDI», à la page 234.
agent Db2	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
agent DataPower	Utilisez le paramètre de configuration de l'agent pour modifier le nom de système géré ; voir «Configuration de l'agent DataPower», à la page 246.
agent DataStage	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
agent Hadoop	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 .

Tableau 10. Méthodes de modification du nom de système géré pour les agents Cloud APM (suite)	
Agent	**Méthode de modification du nom de système géré**
agent HMC Base	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
agent IBM Cloud	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
agent IBM Integration Bus	«Spécification d'un nom de système géré unique pour agent IBM Integration Bus», à la page 296
agent JBoss	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
agent Linux KVM	Utilisez les paramètres de configuration de l'agent ; voir «Configuration de la surveillance de Linux KVM», à la page 482.
Linux OS	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 .
agent Microsoft .NET	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 .
agent Microsoft Active Directory	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 .
agent Microsoft Exchange Server	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 .
agent Microsoft Hyper-V Server	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 .
agent Microsoft IIS	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 .
agent Microsoft Office 365	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 .

Tableau 10. Méthodes de modification du nom de système géré pour les agents Cloud APM (suite)	
Agent	**Méthode de modification du nom de système géré**
agent Microsoft SQL Server	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
agent MicrosoftSharePoint Server	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 .
Agent MongoDB	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent MySQL	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
agent NetApp Storage	Utilisez les paramètres de configuration de l'agent ; voir «Configuration de la surveillance de NetApp Storage», à la page 594.
Agent OpenStack	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent Oracle Database	Utilisez les paramètres de configuration de l'agent ; voir «Configuration de la surveillance d'Oracle Database», à la page 631.
Agent PHP	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent PostgreSQL	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.

Tableau 10. Méthodes de modification du nom de système géré pour les agents Cloud APM (suite)	
Agent	**Méthode de modification du nom de système géré**
agent RabbitMQ	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent de surveillance des temps de réponse	«Spécification d'un nom de système géré unique pour l'Agent de surveillance des temps de réponse», à la page 737
Agent Ruby	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 .
Agent SAP	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent SAP HANA Database	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent SAP NetWeaver Java Stack	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
agent Siebel	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent Skype for Business Server (anciennement agent Microsoft Lync Server)	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 .
Agent Sterling File Gateway	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.

Tableau 10. Méthodes de modification du nom de système géré pour les agents Cloud APM (suite)	
Agent	**Méthode de modification du nom de système géré**
Agent Sterling Connect Direct	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent Tomcat	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
Agent UNIX OS	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 .
Agent WebSphere Applications	Pour modifier le nom d'hôte dans le nom de système géré, voir How to change the host name used in managed system name for the WAS agent instance?. Pour modifier le nom de l'alias de serveur dans le nom de système géré, reconfigurez l'agent ; voir «Reconfiguration du collecteur de données en mode interactif», à la page 869.
agent WebSphere Infrastructure Manager	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 . Utilisez le paramètre de configuration de l'agent pour modifier le nom d'instance dans le nom de système géré.
agent WebSphere MQ	«Spécification de noms de systèmes gérés uniques pour plusieurs gestionnaires de files d'attente», à la page 964
agent Windows OS	Utilisez le paramètre **CTIRA_HOSTNAME** pour modifier le nom d'hôte dans le nom de système géré. Voir «Modification du nom d'hôte dans le nom de système géré», à la page 179 .

Modification du nom d'hôte dans le nom de système géré

Pourquoi et quand exécuter cette tâche

La modification du nom d'hôte dans le nom de système géré n'est pas une pratique courante. En effet, le nom d'hôte est automatiquement détecté et défini lors de la configuration d'agent. Ne modifiez le nom d'hôte dans le nom de système géré que si nécessaire et vérifiez que la valeur que vous spécifiez n'insère pas de troncatures en raison des restrictions de dénomination du nom de système géré.

Procédure

1. Arrêtez toutes les instances existantes de l'agent et attendez que la console Cloud APM indique que l'agent ou ses sous-noeuds soient hors ligne. S'il n'en existe aucune, passez à l'étape suivante.

   Pour plus d'informations sur l'arrêt des instances d'agent, voir «Utilisation des commandes de l'agent», à la page 181.

2. Si l'agent est un agent à instance unique, procédez comme suit pour modifier le paramètre **CTIRA_HOSTNAME**. La valeur que vous spécifiez pour le paramètre **CTIRA_HOSTNAME** est celle qui est appliquée à toutes les nouvelles instances d'agent.
   a) Effectuez une copie de sauvegarde du fichier suivant :
      - Linux AIX *rép_install*/config/*cp*.environment
      - Windows *rép_install*/TMAITM6_x64/k*pc*cma.ini

      où :
      - *rép_install* est le répertoire d'installation de l'agent.
      - *pc* est le code d'agent à deux caractères. Voir le tableau Noms et codes d'agent.
   b) Editez le fichier en modifiant la valeur de paramètre **CTIRA_HOSTNAME** comme suit, où *nouveau_nom_hôte* est la chaîne personnalisée utilisée à la place du nom d'hôte réel de l'ordinateur sur lequel l'agent est installé.
      - Linux AIX **CTIRA_HOSTNAME**=*nouveau_nom_hôte*
      - Windows **CTIRA_HOSTNAME**=*nouveau_nom_hôte* .TYPE=REG_EXPAND_SZ
   c) Sauvegardez vos modifications.
3. Si l'agent est un agent multi-instance, procédez comme suit pour modifier le paramètre **CTIRA_HOSTNAME**. En général, toutes les instances d'agent sur un ordinateur utilisent la même valeur de nom d'hôte. Si vous souhaitez en utiliser une autre, modifiez la valeur que vous avez indiquée dans **CTIRA_HOSTNAME** lors de l'exécution de cette étape.
   a) Effectuez une copie de sauvegarde des fichiers suivants :
      - Linux AIX *rép_install*/config/*pc_instance*.environment
      - Windows *rép_install*/TMAITM6_x64/k*pc*cma_*instance*.ini
   b) Editez le fichier en modifiant la valeur du paramètre **CTIRA_HOSTNAME** comme suit :
      - Linux AIX **CTIRA_HOSTNAME**=*nouveau_nom_hôte*
      - Windows **CTIRA_HOSTNAME**=*nouveau_nom_hôte* .TYPE=REG_EXPAND_SZ
   c) Sauvegardez vos modifications.
4. Windows
   Reconfigurez les instances d'agent existantes.
5. Démarrez toutes les instances de l'agent.

Que faire ensuite
Une fois que vous avez modifié le nom de système géré de l'agent, démarrez la console Cloud APM et modifiez vos applications en supprimant l'ancien nom du système géré et en le remplaçant par le nouveau.

Configuration d'agents

Après l'installation, certains agents sont configurés et démarrés automatiquement, alors que d'autres nécessitent une configuration manuelle mais démarrent automatiquement. Certains agents doivent être configurés et démarrés manuellement. Les agents multi-instances nécessitent la création d'une première instance et un démarrage manuel.

Avant de commencer

Lorsque vous installez un agent, un exemple de fichier de configuration silencieux est placé dans le répertoire `/opt/ibm/apm/agent/samples`, par exemple, `ynv_silent_config_agent.txt` et `datapower_silent_config.txt`.

Remarque : Certains agents, tels que Monitoring Agent for WebSphere Applications, ont plusieurs fichiers de configuration en mode silencieux pour différentes tâches telles que la configuration du collecteur de données.

Pourquoi et quand exécuter cette tâche

Pour obtenir des détails sur le déploiement des agents, voir Chapitre 5, «Déploiement d'agents et de collecteurs de données», à la page 115.

Pour configurer un agent, vous pouvez utiliser la ligne de commande ou un fichier de réponses silencieux tel que décrit dans cette procédure.

Les méthodes de configuration varient en fonction des agents. Suivez la procédure fournie pour votre agent.

Procédure

- Exécutez la commande *nom-agent*`.sh config`.
  Pour plus de commandes, voir le Tableau 12, à la page 184 et le Tableau 13, à la page 185.
- Editez le fichier de réponses silencieux, puis exécutez l'une des commandes suivantes :
  - Pour les agents à instance unique, exécutez la commande suivante :

    ```
    nom-agent.sh config fichier_réponses
    ```

  - Pour les agents à plusieurs instances, exécutez la commande suivante :

    ```
    nom-agent.sh config nom_instance fichier_réponses
    ```

  - où *nom_instance* est le nom de l'instance qui peut être attribué pour indiquer ce que vous surveillez.
- Windows
  Pour les agents pris en charge sur les systèmes Windows, vous pouvez effectuer certaines tâches de configuration à l'aide de la fenêtre IBM Cloud Application Performance Management. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**. Pour plus d'informations, voir «Utilisation de la fenêtre IBM Cloud Application Performance Management sur les systèmes Windows», à la page 186.
- Pour effectuer une configuration avancée pour certains agents, comme la configuration du suivi des transactions ou de la collecte des données, et l'activation des données de diagnostic, utilisez la fenêtre **Configuration d'agent**. Pour plus d'informations, voir «Page Configuration d'agent», à la page 187.

Utilisation des commandes de l'agent

Les scripts qui sont utilisés pour installer les agents de surveillance sont également utilisés pour vérifier le statut d'un agent installé, l'arrêter, le démarrer ou le désinstaller.

Pourquoi et quand exécuter cette tâche

Le nom d'agent et les codes agent sont fournis à titre de référence.

Utilisez le nom de l'agent dans les commandes suivantes :

Linux AIX *nom*`-agent.sh`

Windows *nom*`-agent.bat`

où *nom* correspond au nom de l'agent qui est spécifié dans le Tableau 11, à la page 182.

Tableau 11. Noms et codes d'agent

Agent de surveillance	***nom***	**Code agent à deux lettres**
Monitoring Agent for Amazon EC2	`amazon_ec2`	`b5`
Monitoring Agent for Azure Compute	`azure_compute`	`ak`
Monitoring Agent for Cassandra	`cassandra`	`zc`
Monitoring Agent for Cisco UCS	`cisco_ucs`	`v6`
Monitoring Agent for Citrix Virtual Desktop Infrastructure	`citrix_vdi`	`vd`
Monitoring Agent for DataPower	`datapower`	`bn`
Monitoring Agent for Db2	`db2`	`ud`
Monitoring Agent for Hadoop	`hadoop`	`h8`
Monitoring Agent for HMC Base	`hmc_base`	`ph`
Monitoring Agent for HTTP Server	`http_server`	`hu`
Monitoring Agent for IBM Cloud	`ibm_cloud`	`fs`
Monitoring Agent for IBM Integration Bus	`iib`	`qi`
Monitoring Agent for MQ Appliance	`ibm_mq_appliances`	`mk`
Monitoring Agent for InfoSphere DataStage	`datastage`	`dt`
Monitoring Agent for JBoss	`jboss`	`je`
Monitoring Agent for Linux KVM	`linux_kvm`	`v1`
Monitoring Agent for Linux OS	`os`	`lz`
Monitoring Agent for MariaDB	`mariadb`	`mj`
Monitoring Agent for Microsoft Active Directory	`msad`	`3z`
Monitoring Agent for Microsoft Cluster Server	`mscs`	`q5`
Monitoring Agent for Microsoft Exchange Server	`msexch`	`ex`
Monitoring Agent for Microsoft Hyper-V Server	`microsoft_hyper-v_server`	`hv`
Monitoring Agent for Microsoft Internet Information Services	`msiis`	`q7`
Monitoring Agent for Skype for Business Server (anciennement Microsoft Lync Server)	`skype_for_business_server`	`ql`
Monitoring Agent for Microsoft .NET	`dotnet`	`qe`
Monitoring Agent for Microsoft Office 365	`microsoft_office365`	`mo`
Monitoring Agent for Microsoft SharePoint Server	`ms_sharepoint_server`	`qp`
Monitoring Agent for Microsoft SQL Server	`mssql`	`oq`
Monitoring Agent for MongoDB	`mongodb`	`kj`
Monitoring Agent for MySQL	`mysql`	`se`
Monitoring Agent for NetApp Storage	`netapp_storage`	`nu`

Tableau 11. Noms et codes d'agent (suite)		
Agent de surveillance	***nom***	**Code agent à deux lettres**
Monitoring Agent for Node.js	nodejs	nj
Monitoring Agent for OpenStack	openstack	sg
Monitoring Agent for Oracle Database	oracle_database	rz
Monitoring Agent for PHP	php	pj
Monitoring Agent for PostgreSQL	postgresql	pn
Monitoring Agent for Python	python	pg
Monitoring Agent for RabbitMQ	rabbitMQ	zr
Monitoring Agent for Ruby	ruby	km
Monitoring Agent for SAP Applications	sap	sa
Monitoring Agent for SAP HANA Database	sap_hana_database	s7
Monitoring Agent for SAP NetWeaver Java Stack	sap_netweaver_java_stack	sv
Monitoring Agent for Siebel	siebel	uy
Monitoring Agent for Sterling Connect Direct	sterling_connect_direct-agent	FC
Monitoring Agent for Sterling File Gateway	file_gateway	fg
Monitoring Agent for Sybase Server	sybase	oy
Monitoring Agent for Synthetic Playback	synthetic_transactions	sn
Monitoring Agent for Tomcat	tomcat	ot
Monitoring Agent for UNIX OS	os	ux
Monitoring Agent for VMware VI	vmware_vi	vm
Monitoring Agent for WebLogic	oracle_weblogic	wb
Monitoring Agent for WebSphere Applications	was	yn
Monitoring Agent for WebSphere Infrastructure Manager	wim	d0
Monitoring Agent for WebSphere MQ	mq	mq
Monitoring Agent for Windows OS	os	nt
Agent de surveillance des temps de réponse	rt	t5

Procédure

- Linux AIX
  Sur le système où vous voulez envoyer une commande à l'agent de surveillance, accédez au répertoire *rép_install*/bin. Entrez n'importe laquelle des commandes du Tableau 12, à la page 184 où *nom* correspond au nom de l'agent spécifié dans le Tableau 11, à la page 182.

Tableau 12. Commandes pour les systèmes UNIX et Linux

Commande	Description
`./`*nom*`-agent.sh status`	Vérifie le statut de l'agent. Le statut peut être "en cours d'exécution" ou "pas en cours d'exécution". Lorsque l'agent est en cours d'exécution, le statut de la connexion entre l'agent et le serveur Cloud APM est également vérifié. Les statuts de connexion négative possibles sont : Connection failed, Error detected, Disconnected-error. Le statut de connexion positive est Connected ; il s'agit du statut attendu. Le statut transitionnel est Connecting. Le statut Unknown indique que le statut de l'agent ne peut pas être reconnu, probablement en raison d'erreurs dans le système de fichiers ou dans le fichier journal de l'agent.
`./`*nom*`-agent.sh start`	Démarre l'agent de surveillance. Si l'agent possède des instances, entrez un nom d'instance après la commande.
`./`*nom*`-agent.sh stop`	Arrête l'agent. Si l'agent possède des instances, entrez un nom d'instance après la commande.
`./`*nom*`-agent.sh prereqcheck`	Exécute une analyse prérequise. Cette option de commande est disponible pour la plupart des agents.
`./`*nom*`-agent.sh install`	Installe l'agent de surveillance. Pour plus d'informations, voir «Installation des agents sur les systèmes UNIX», à la page 124 et «Installation des agents sur les systèmes Linux», à la page 130.
`./`*nom*`-agent.sh config` *nom_instance chemin_fichier_config_silencieux*	Configure l'agent de surveillance. Exécutez la commande à partir du répertoire *rép_install*`/bin` et ajoutez si nécessaire le chemin du fichier de réponses. Si l'agent possède plusieurs instances, entrez un nom d'instance. Pour plus d'informations sur les agents qui possèdent plusieurs instances, voir Tableau 7, à la page 117 . *fichier_config_silencieux* est facultatif. Si vous ne spécifiez pas un fichier pour la configuration en mode silencieux, vous pouvez configurer l'agent de surveillance de manière interactive en suivant les invites.
`./`*name*`-agent.sh uninstall`	Désinstalle l'agent de surveillance. Pour plus d'informations, voir «Désinstallation de vos agents», à la page 150.
`./smai-agent.sh uninstall_all`	Désinstalle tous les agents de surveillance sur le système géré.
`./`*nom*`-agent.sh remove` *nom_instance*	Supprime une instance d'un agent à plusieurs instances.

Tableau 12. Commandes pour les systèmes UNIX et Linux (suite)	
Commande	**Description**
`./`*nom*`-agent.sh`	Affiche une description des fonctions disponibles avec le script.

- Windows

Sur le système où vous voulez envoyer une commande à l'agent de surveillance, accédez au répertoire *rép_install*`\BIN` à l'invite de commande, par exemple : `C:\IBM\APM\bin`. Entrez n'importe laquelle des commandes du Tableau 13, à la page 185 où *nom* correspond au nom de l'agent spécifié dans le Tableau 11, à la page 182.

Tableau 13. Commandes pour les systèmes Windows	
Commande	**Description**
nom`-agent.bat status`	Vérifie le statut de l'agent. Vérifie le statut de la connexion entre l'agent et le serveur Cloud APM. Les statuts de connexion négative possibles sont : Connection failed, Error detected, Disconnected-error. Le statut de connexion positive est Connected ; il s'agit du statut attendu. Le statut transitionnel est Connecting. Le statut Unknown indique que le statut de l'agent ne peut pas être reconnu, probablement en raison d'erreurs dans le système de fichiers ou dans le fichier journal de l'agent.
nom`-agent.bat start`	Démarre l'agent de surveillance. Si l'agent possède des instances, entrez un nom d'instance après la commande.
nom`-agent.bat stop`	Arrête l'agent. Si l'agent possède des instances, entrez un nom d'instance après la commande.
nom`-agent.bat prereqcheck`	Exécute une analyse prérequise. Cette option de commande est disponible pour la plupart des agents.
nom`-agent.bat install`	Installe l'agent de surveillance. Pour plus d'informations, voir «Installation d'agents», à la page 142.
nom`-agent.bat config` *nom_instance chemin_fichier_config_silencieux*	Configure l'agent de surveillance. Exécutez la commande à partir du répertoire *rép_install*`\bin` et ajoutez si nécessaire le chemin du fichier de réponses. Si l'agent possède plusieurs instances, entrez un nom d'instance. Pour plus d'informations sur les agents qui possèdent plusieurs instances, voir Tableau 7, à la page 117 . *fichier_config_silencieux* est facultatif. Si vous ne spécifiez pas un fichier pour la configuration en mode silencieux, vous pouvez configurer l'agent de surveillance de manière interactive en suivant les invites.

Tableau 13. Commandes pour les systèmes Windows (suite)	
Commande	**Description**
nom-agent.bat uninstall	Désinstalle l'agent de surveillance. Pour plus d'informations, voir «Désinstallation de vos agents», à la page 150.
smai-agent.bat uninstall_all	Désinstalle tous les agents de surveillance sur le système géré.
nom-agent.bat remove *nom_instance*	Supprime une instance d'un agent à plusieurs instances.
nom-agent.bat	Affiche une description des fonctions disponibles avec le script.

Commande de version d'agent

- Pour afficher la version d'un agent dans votre environnement, exécutez les commandes suivantes :
  - Linux AIX

    ```
    rép_install/bin/cinfo
    ```

    Entrez 1 pour afficher les versions.
  - Windows

    ```
    rép_install/InstallITM/kincinfo
    ```

Tâches associées

«Utilisation de la fenêtre IBM Cloud Application Performance Management sur les systèmes Windows», à la page 186

Utilisation de la fenêtre IBM Cloud Application Performance Management sur les systèmes Windows

Les agents pris en charge sous Windows possèdent un utilitaire d'interface graphique que vous pouvez utiliser pour exécuter la configuration d'agent et vérifier le statut de connexion.

L'utilitaire de configuration d'interface graphique n'est disponible ni pour Monitoring Agent for WebSphere MQ, ni pour Monitoring Agent for IBM Integration Bus.

Procédure

- Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.

Résultats

La fenêtre IBM Cloud Application Performance Management apparaît. Chaque composant d'agent installé est répertorié avec son statut de configuration, qu'il soit démarré ou arrêté, le statut de connexion, le numéro de version et d'autres informations.

Que faire ensuite

Démarrez ou arrêtez un agent ou configurez ses paramètres en cliquant sur l'agent à l'aide du bouton droit de la souris, puis en sélectionnant une option.

Page Configuration d'agent

Utilisez la page **Configuration d'agent** pour configurer de manière centralisée les paramètres d'agents tels que l'Agent de surveillance des temps de réponse et l'Agent WebSphere Applications.

Utilisation générale

Lorsque l'utilisateur clique sur **Configuration système** > **Configuration d'agent** dans la barre de navigation, un tableau de bord à onglets s'affiche. Il contient un onglet pour chaque agent de surveillance configurable. Le tableau présente des colonnes comportant des informations de configuration, notamment le nom et l'adresse IP de chaque système géré, avec une ligne pour chaque système géré.

Actions
Utilisez les options Actions pour activer ou désactiver les fonctions telles que le suivi des transactions ou la collecte des données.

Redimensionnement de colonne
Faites glisser la bordure d'un en-tête de colonne pour régler la largeur de la colonne.

Tri de colonne
Cliquez à l'intérieur d'un en-tête de colonne pour procéder au tri en fonction de cette colonne. Cliquez de nouveau sur le même en-tête de colonne pour passer de l'ordre de tri croissant à l'ordre de tri décroissant et inversement.

Filtre de tableau
Cliquez à l'intérieur de la zone de texte de filtre et entrez le début de la valeur qui va servir à filtrer la table. Au fur et à mesure de la saisie, les lignes de table qui ne répondent pas aux critères sont filtrées et la ligne ***Total*** est mise à jour en fonction du nombre de lignes trouvées.

Cliquez sur "x" dans la zone de filtre ou appuyez sur la touche Retour arrière pour désactiver le filtre.

Configuration d'agent

Pour plus d'informations sur les paramètres des agents spécifiques, reportez-vous aux rubriques suivantes :

- agent DataPower: «Configuration de la surveillance DataPower», à la page 237
- agent IBM Integration Bus: «Configuration du suivi des transactions pour l'agent IBM Integration Bus», à la page 296
- Internet Service Monitoring«Configuration de l'agent sur des systèmes Windows», à la page 456
- agent JBoss: «Configuration du collecteur de données de suivi des transactions de l'agent agent JBoss», à la page 478
- agent Microsoft .NET: «Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 538
- Surveillance du fichier journal d'agent de système d'exploitation : «Ajout ou suppression de la configuration de surveillance des fichiers journaux pour les agents de système d'exploitation», à la page 650
- Agent de surveillance des temps de réponse: «Configuration à l'aide de la page Configuration d'agent», à la page 711
- Géolocalisation : «Personnalisation des valeurs de localisation Transaction utilisateur final», à la page 733
- Agent Ruby: «Désactivation ou activation des données de diagnostic pour les applications Ruby», à la page 745
- Agent SAP NetWeaver Java Stack: «Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 791
- Agent Tomcat: «Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 829
- Agent WebLogic: «Configuration du suivi des transactions pour l'Agent WebLogic», à la page 849

- Agent WebSphere Applications: «Configuration dynamique de la collecte des données sur la page Configuration d'agent», à la page 901
- agent WebSphere MQ: «Configuration du suivi des transactions pour l'agent WebSphere MQ», à la page 966

Configuration des agents en tant qu'utilisateur non superutilisateur
Pour configurer votre agent en tant qu'utilisateur non superutilisateur, créez un groupe commun sur le système et faites de chaque utilisateur un membre de ce groupe.

Avant de commencer

Si vous avez installé votre agent en tant que superutilisateur ou utilisateur non superutilisateur et souhaitez configurer l'agent de la même manière, aucune action spéciale n'est requise.

Si vous avez installé votre agent en tant qu'un utilisateur sélectionné et que vous souhaitez configurer l'agent en tant qu'un autre utilisateur, créez un groupe commun sur le système. Définissez tous les utilisateurs de gestion d'agent comme membres de ce groupe commun. Transférez la propriété de tous les fichiers et répertoires d'agent vers ce groupe.

Remarque :

- Pour l'agent HTTP Server, si vous configurez l'agent en tant qu'utilisateur non superutilisateur, ce dernier doit avoir le même ID utilisateur que l'utilisateur qui a démarré IBM HTTP Server. Sinon, l'agent a des difficultés à reconnaître le IBM HTTP Server.
- Pour l'agent IBM Integration Bus, si l'installation d'IBM Bus Integration est un déploiement à utilisateur unique, utilisez le même ID utilisateur que l'utilisateur qui a installé IBM Integration Bus pour configurer l'agent. Pour configurer l'agent, procédez comme suit pour cet ID utilisateur.

Procédure

1. Installez vos agents de surveillance sous Linux ou UNIX comme décrit dans «Installation des agents sur les systèmes Linux», à la page 130 et «Installation des agents sur les systèmes UNIX», à la page 124.
2. Exécutez le script `./secure.sh` avec le nom de groupe de l'utilisateur non superutilisateur afin de sécuriser les fichiers et définissez la propriété de groupe de fichiers sur les fichiers.
   Par exemple : **`./secure.sh -g db2iadm1`**
3. Au besoin, configurez vos agents de surveillance sous Linux ou AIX (voir Chapitre 7, «Configuration de votre environnement», à la page 163).
4. Pour mettre à jour les scripts de démarrage du système, exécutez le script suivant en tant que superutilisateur ou utilisateur sudo: *rép_install*`/bin/UpdateAutoRun.sh`

Que faire ensuite

Pour plus d'informations sur le script **`./secure.sh`**, voir Sécurisation des fichiers d'installation de l'agent.

Utilisez le même ID utilisateur pour l'installation et les mises à niveau de l'agent.

Désactivation du démarrage automatique de l'agent sur les systèmes UNIX et Linux
Sur le système UNIX ou Linux, un agent peut démarrer automatiquement suite au redémarrage du système d'exploitation. Si vous ne voulez pas que l'agent démarre automatiquement après le redémarrage du système, vous pouvez désactiver le démarrage automatique de l'agent.

Pourquoi et quand exécuter cette tâche

Si vous installez un agent en tant que superutilisateur sur le système UNIX ou Linux, celui-ci peut démarrer automatiquement après le redémarrage du système. Sinon, si vous installez un agent en tant qu'utilisateur non superutilisateur, mais que vous exécutez le script **`UpdateAutoRun.sh`** en tant que

superutilisateur suite à l'installation, l'agent peut démarrer automatiquement suite au redémarrage du système.

Procédure

1. Pour désactiver le démarrage automatique sur certains agents, procédez comme suit :
   a. Pour l'Linux OS et l'agent WebSphere® Applications, ajoutez le code suivant au fichier `rép_install_agent/registry/kcirunas.cfg` :

```
<productCode>lz</productCode>
 <default>
   <autoStart>no</autoStart>
 </default>
 <productCode>yn</productCode>
 <default>
   <autoStart>no</autoStart>
 </default>
```

   b. Exécutez la commande **`rép_install_agent/bin/UpdateAutoRun.sh`**.
2. Pour activer le démarrage automatique sur certains agents, procédez comme suit :
   a. Pour l'Linux OS et l'agent WebSphere Application, redéfinissez la valeur de la balise *<autoStart>* sur **yes** dans le fichier `rép_install_agent/registry/kcirunas.cfg`.
   b. Ouvrez le fichier `rép_install_agent/registry/AutoStart` et vérifiez son contenu.
   c. Supprimez le fichier `/etc/init.d/ITMAgents{$Num}`, où *{$Num}* est un nombre positif dans le fichier `rép_install_agent/registry/AutoStart`. Si la valeur est 1, vous devez supprimer le fichier `/etc/init.d/ITMAgents1`.
   d. Exécutez la commande **`rép_install_agent/bin/UpdateAutoRun.sh`**.

Résultats
Une fois que le système a redémarré, aucun script d'agent ne s'exécute automatiquement pour démarrer l'agent.

Procédure générale de configuration des collecteurs de données

Pour afficher dans la console Cloud APM les données de surveillance concernant vos applications à l'aide d'un collecteur de données, vous devez accomplir plusieurs tâches de configuration.

Pourquoi et quand exécuter cette tâche

Cette procédure, qui inclut des étapes obligatoires, conditionnelles et facultatives, constitue un plan de configuration de la surveillance pour vos applications. Effectuez les étapes nécessaires en fonction de vos besoins.

Procédure

1. Téléchargez et procédez à l'extraction du package de collecteur de données. Pour obtenir des instructions, voir «Téléchargement de vos agents et de vos collecteurs de données», à la page 105.
2. Configurez le collecteur de données pour qu'il collecte des données de surveillance sur les applications IBM Cloud et sur site et les envoie au serveur Cloud APM. Effectuez une ou plusieurs des tâches suivantes en fonction du type de votre application :

   Applications Liberty

   - «Configuration du collecteur de données Liberty pour les applications sur site», à la page 906
   - «Configuration du collecteur de données Liberty pour les applications IBM Cloud», à la page 910

   Applications Node.js

   - «Configuration du collecteur de données Node.js autonome pour les applications IBM Cloud(anciennement Bluemix)», à la page 608

- «Configuration du collecteur de données Node.js autonome pour les applications sur site», à la page 615

Applications Python

- «Configuration du collecteur de données Python pour les applications IBM Cloud», à la page 689
- «Configuration du collecteur de données Python pour les applications sur site», à la page 695

Applications Ruby

- «Configuration du collecteur de données Ruby pour les applications IBM Cloud», à la page 745

Applications Java

- «Configuration de la surveillance de J2SE», à la page 461

3. Si le fichier de clés ou le serveur Cloud APM est modifié, reconnectez le collecteur de données au serveur Cloud APM. Pour obtenir des instructions, voir «Reconnexion du collecteur de données au serveur Cloud APM», à la page 190.

Que faire ensuite

Après avoir accompli toutes les tâches de configuration nécessaires, vous pouvez vérifier que les données d surveillance de votre application IBM Cloud sont affichées dans la console Cloud APM.

Reconnexion du collecteur de données au serveur Cloud APM

Si le serveur Cloud APM, le fichier de clés ou le mot de passe du fichier de clés est modifié, vous devez définir plusieurs variables d'environnement pour reconnecter le collecteur de données au serveur Cloud APM.

Avant de commencer

Si le fichier de clés est modifié, chiffrez d'abord le mot de passe en texte normal de votre fichier de clés en Base64. Si vous êtes un utilisateur Linux, exécutez la commande suivante :

```
echo -n mot_de_passe_fichier_clés | base64
```

Le résultat de la commande est votre mot de passe chiffré. Par exemple, si votre mot de passe en texte normal est `mot de passe`, le résultat de la commande `cGFzc3dvcmQ=` est votre mot de passe chiffré. Vous utilisez alors le mot de passe chiffré pour définir `APM_KEYFILE_PSWD:` *`mot_de_passe_fichier_clés_chiffré`* et `APM_KEYFILE_PSWD=`*`mot_de_passe_fichier_clés_chiffré`* dans les configurations ci-après.

Procédure

- Pour reconnecter les collecteurs de données au serveur Cloud APM pour les applications IBM Cloud, voir «Reconnexion des collecteurs de données pour les applications IBM Cloud», à la page 190.
- Pour reconnecter les collecteurs de données au serveur Cloud APM pour les applications sur site, voir «Reconnexion du collecteur de données pour les applications sur site», à la page 192.

Reconnexion des collecteurs de données pour les applications IBM Cloud

Pourquoi et quand exécuter cette tâche

Vous disposez des deux options suivantes pour reconnecter le collecteur de données au serveur Cloud APM :

- Editez le `manifest.yml` de votre application pour définir les variables.
- Définissez les variables dans l'interface utilisateur de IBM Cloud.

Procédure

- Pour utiliser le fichier `manifest.yml` de votre application IBM Cloud afin de reconnecter le collecteur de données, effectuez les étapes suivantes :
  a) Editez les variables dans le fichier `manifest.yml` de votre application IBM Cloud en fonction des modifications.
     – Pour configurer la passerelle en vue d'utiliser *HTTP*, définissez la variable suivante :

```
APM_BM_GATEWAY_URL: http://IP_ou_nom_d'hôte_du_serveur:80
```

     – Pour configurer la passerelle en vue d'utiliser *HTTPS*, définissez les trois variables suivantes :

```
APM_BM_GATEWAY_URL: https://IP_ou_nom_d'hôte_du_serveur:443
APM_KEYFILE_PSWD: mot_de_passe_fichier_clés_chiffré
APM_KEYFILE_URL: http://serveur_http_hébergé:port/nom_fichier_clés
```

     Conseil : Le fichier de clés du collecteur de données Liberty est un fichier `.jks`. Pour les collecteurs de données Python, Node.js et Liberty, les fichiers de clés sont des fichiers `.p12`.
  b) Accédez au répertoire de votre application IBM Cloud et exécutez la commande suivante :

```
cf push
```

- Pour utiliser l'interface utilisateur de IBM Cloud afin de reconnecter le collecteur de données, effectuez l'étape suivante :
  a) Connectez-vous à l'interface utilisateur de IBM Cloud.
  b) Cliquez sur l'application IBM Cloud.
  c) Cliquez sur **Runtime** (Exécution) dans le panneau de gauche.
  d) Accédez à l'onglet **Variable d'environnement**.
  e) Dans la section **définies par l'utilisateur**, utilisez l'une des méthodes suivantes pour définir les variables selon vos besoins :
     – Pour configurer la passerelle en vue d'utiliser *HTTP*, définissez la variable suivante :

```
APM_BM_GATEWAY_URL: http://IP_ou_nom_d'hôte_du_serveur:80
```

     – Pour configurer la passerelle en vue d'utiliser *HTTPS*, définissez les trois variables suivantes :

```
APM_BM_GATEWAY_URL: https://IP_ou_nom_d'hôte_du_serveur:443
APM_KEYFILE_PSWD: mot_de_passe_fichier_clés_chiffré
APM_KEYFILE_URL: http://serveur_http_hébergé:port/nom_fichier_clés
```

     Conseil : Le fichier de clés du collecteur de données Liberty est un fichier `.jks`. Pour les collecteurs de données Python, Node.js et Liberty, les fichiers de clés sont des fichiers `.p12`.
  f) A partir du répertoire dans lequel vous exécutez la commande **`cf push`** pour transmettre votre application, exécutez la commande suivante pour que vos modifications prennent effet :

```
cf restage <nom_app>
```

Résultats
Les valeurs des variables sont définies correctement pour connecter le collecteur de données au serveur Cloud APM.

Reconnexion du collecteur de données pour les applications sur site

Pourquoi et quand exécuter cette tâche

En modifiant le fichier `global.environment` ou `dc.java.properties`, vous pouvez personnaliser la connexion entre le collecteur de données et le serveur Cloud APM.

Procédure

1. Recherchez le fichier correspondant qui contient les variables de connexion.
   a) Pour le collecteur de données Liberty, le collecteur de données Node.js et le collecteur de données Python, recherchez le fichier `global.environment` en fonction des informations du tableau suivant :

Nom du collecteur de données	Répertoire du fichier `global.environment`
collecteur de données Liberty	Dossier `itcamdc/etc/global.environment` dans lequel votre collecteur de données Liberty est installé.
collecteur de données Node.js	Dossier `ibmapm/etc` dans lequel votre collecteur de données Node.js est installé.
collecteur de données Python	Dossier `etc` dans lequel votre collecteur de données Python est installé.

   b) Pour le collecteur de données J2SE, recherchez le fichier `dc.java.properties` dans le dossier *DC_HOME*`/itcamdc/etc`. *DC_HOME* représente le répertoire dans lequel votre collecteur de données J2SE est installé.
2. Editez les variables dans le fichier correspondant en fonction des modifications.
   a) Pour le collecteur de données Liberty, le collecteur de données Node.js et le collecteur de données Python, éditez le fichier `global.environment` en fonction de l'instruction suivante :
      - Pour configurer la passerelle en vue d'utiliser *HTTP*, définissez la variable suivante :

```
APM_BM_GATEWAY_URL= http://IP_ou_nom_d'hôte_du_serveur:80
```

      - Pour configurer la passerelle en vue d'utiliser *HTTPS*, définissez les variables suivantes :

```
APM_BM_GATEWAY_URL= https://IP_ou_nom_d'hôte_du_serveur:443
APM_KEYFILE_PSWD=mot_de_passe_fichier_clés_chiffré
APM_KEYFILE_URL=http://serveur_http_hébergé_:port/nom_fichier_clés
```

      Conseil : le fichier de clés du collecteur de données Liberty est un fichier `.jks`. Pour les collecteurs de données Python, Node.js et Liberty, les fichiers de clés sont des fichiers `.p12`.
   b) Pour le collecteur de données J2SE, éditez le fichier `dc.java.properties` en fonction de l'instruction suivante :
      - Pour configurer la passerelle en vue d'utiliser *HTTP*, définissez la variable suivante :

```
apm.http.type=http
```

        Si la valeur de cette variable reste vide, `http` est la valeur par défaut
      - Pour configurer la passerelle en vue d'utiliser *HTTPS*, définissez les variables suivantes :

```
apm.ssl.password=mot_de_passe_fichier_clés_chiffré
apm.http.type=https
```

      Important : si le mot de passe est modifié, remplacez le fichier *DC_HOME*`/itcamdc/etc/keyfile.jks` par le fichier `/opt/ibm/ccm/keyfiles/default.agent/keyfiles/`

keyfile.jks du serveur Cloud APM, *DC_HOME* correspondant au répertoire de base de votre collecteur de données J2SE.

3. Facultatif : Si vous n'utilisez pas le fichier de clés par défaut pour votre collecteur de données Node.js, définissez la variable suivante :

   ```
   APM_SNI=hôte_propriétaire_dans_le_fichier_clés
   ```

   Conseil : pour déterminer la valeur de la variable *hôte_propriétaire*, ouvrez le fichier de clés que vous utilisez et recherchez owner. Ensuite, définissez la variable *APM_SNI* sur la même valeur qu'*owner*.
4. Redémarrez l'application pour appliquer la modification.

Résultats
Les valeurs des variables sont définies correctement pour connecter le collecteur de données au serveur Cloud APM.

Exemple de fichier `manifest.yml`
Pour voir le contenu du fichier manifest.yml d'une application IBM Cloud, consultez les lignes suivantes :

```
applications:

- disk_quota: 1024M
  host: myBluemixApp
  name: myBluemixApp
  path: .
  domain: mybluemix.net

  instances: 1
  memory: 512M

  env:
    KNJ_ENABLE_TT: "true"
    KNJ_SAMPLING: 1
```

Suppression de collecteurs de données de la console Cloud APM
Une fois que vous avez annulé la configuration d'un collecteur de données, vous devez également supprimer le collecteur de données des applications et des groupes de ressources auxquels il a été ajouté. Sinon, la console Cloud APM indique qu'aucune donnée n'est disponible pour l'application et n'indique pas que le collecteur de données est hors ligne.

Procédure

1. Supprimez le collecteur de données des applications auxquelles vous l'avez ajouté en éditant manuellement ces applications.

   Cette opération est similaire à la suppression d'agents hors ligne de votre application. Voir «Affichage et suppression des agents en ligne», à la page 1135.
2. Supprimez le collecteur de données des groupes de ressources personnalisés auxquels vous l'avez ajouté.

   Pour plus d'informations, voir «Gestionnaire de groupes de ressources», à la page 1008.
3. Ouvrez un ticket pour que l'équipe chargée des opérations Cloud APM effectue les étapes suivantes sur le serveur Cloud APM :
   a) Editez le fichier *rép_install*/serveragents/config/hostname_bi.cfg pour supprimer les lignes du collecteur de données dont la configuration a été annulée.
   b) Redémarrez le composant serveur des collecteurs de données en exécutant la commande suivante en tant que superutilisateur :

      ```
      apm restart biagent
      ```

Résultats

Après quelques minutes, la console Cloud APM indique que le collecteur de données est hors ligne dans l'application **Mes composants** et dans l'interface utilisateur **Gestionnaire de groupes de ressources** si vous sélectionnez le groupe de ressources système du collecteur de données.

Une fois que l'intervalle spécifié par la propriété de configuration **Délai avant suppression d'un système hors ligne** de la page **Configuration avancée** est écoulé, le collecteur de données est automatiquement supprimé de **Mes composants** et de son groupe de ressources système.

Conseil : Vous pouvez régler le paramètre **Délai avant suppression d'un système hors ligne** au niveau de la page **Configuration avancée** pour augmenter ou réduire le délai avant suppression de l'agent hors ligne dans le cadre de la vue. Pour plus d'informations, voir «Fonction d'abonnement d'agent», à la page 1105.

A faire : Si le collecteur de données a fourni des données de suivi des transactions au serveur Cloud APM, la console Cloud APM peut continuer d'afficher le collecteur de données dans l'application **Mes composants** et afficher le message The `agent is invalid` pour le collecteur de données une fois le délai spécifié par le paramètre **Délai avant suppression d'un système hors ligne** écoulé. Si vous avez installé Cloud APM 8.1.4.0 Server, correctif temporaire 3 ou ultérieur, un collecteur de données non valide sera supprimé de l'application **Mes composants** huit jours après l'arrêt de la réception des données de suivi des transactions du collecteur de données.

Configuration de la surveillance d'Amazon EC2

agent Amazon EC2 permet de surveiller de manière centralisée la santé, la disponibilité et les performances de vos instances Amazon Elastic Compute Cloud (EC2). L'agent affiche un ensemble complet de mesures qui vous aident à prendre des décisions avisées concernant votre environnement EC2. Ces mesures incluent l'utilisation de l'UC, l'utilisation d'Elastic Block Store (EBS), l'utilisation du réseau, les mises à jour de maintenance d'Amazon Web Services (AWS) et la performance des disques.

Avant de commencer

- Lisez l'intégralité de la rubrique «Configuration de la surveillance d'Amazon EC2», à la page 194 pour déterminer les éléments nécessaires à l'achèvement de la configuration.
- Les instructions figurant dans cette rubrique concernent l'édition la plus récente de l'agent, sauf indication contraire.
- Assurez-vous que votre environnement possède la configuration système requise pour l'agent Amazon EC2. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Amazon EC2.
- Vérifiez que les informations suivantes sont disponibles :
  - Une liste des noms de région AWS contenant les instances EC2 à surveiller.
  - Les droits de sécurité AWS (ID de clé d'accès et clé d'accès secrète) avec l'autorisation d'accès à chaque région AWS.
- Assurez-vous que les droits de sécurité AWS qui sont utilisés pour chaque région AWS sont rattachés à un groupe qui inclue au moins la règle *AmazonEC2ReadOnlyAccess*.

Pourquoi et quand exécuter cette tâche

L'agent Amazon EC2 est à la fois un agent à plusieurs instances et un agent de sous-noeud. Vous pouvez créer une instance d'agent à plusieurs sous-noeuds (une pour chaque région Amazon EC2) ou une instance d'agent pour chaque région Amazon EC2 avec un sous-noeud pour cette région. Vous pouvez également créer une combinaison de chaque type de configuration. Après avoir configuré les instances d'agent, démarrez chacune d'elles manuellement. Si vous disposez de plus de 50 ressources par région Amazon EC2, nous vous suggérons de créer une instance d'agent par région, ou d'utiliser le balisage dans vos instances EC2 et de filtrer les agences d'agent selon les balises que vous créez à l'aide du paramètre de condition de filtrage de l'agent.

Procédure

1. Configurez l'agent sur des systèmes Windows avec la fenêtre **IBM Performance Management** ou le fichier de réponses silencieux.
   - «Configuration de l'agent sur des systèmes Windows», à la page 195.
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 199.
2. Configurez l'agent sur des systèmes Linux avec le script qui génère des invites pour les réponses ou le fichier de réponses silencieux.
   - «Configuration de l'agent en répondant à des invites.», à la page 198.
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 199.

Que faire ensuite

Dans la console Cloud APM, accédez à votre Tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Pour identifier et résoudre les incidents, reportez-vous au forum Cloud Application Performance Management.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent Amazon EC2 sur les systèmes d'exploitation Windows dans la fenêtre IBM Cloud Application Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur le modèle **Monitoring Agent for Amazon EC2**, puis cliquez sur **Configure agent**.

   A faire : Après avoir configuré une instance d'agent pour la première fois, l'option **Configure agent** est désactivée. Pour reconfigurer l'instance d'agent, cliquez dessus avec le bouton droit de la souris et sélectionnez **Reconfigure**.
3. Entrez un nom d'instance unique, puis cliquez sur **OK**. N'utilisez que des lettres latines, des chiffres arabes, le caractère de soulignement et le caractère moins dans le nom de l'instance. Par exemple, `ec2-inst3`.

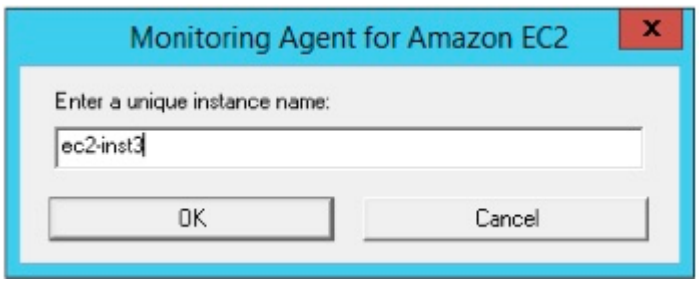


Figure 3. Fenêtre de saisie d'un nom d'instance unique.

4. Cliquez sur **Suivant** dans la fenêtre du nom d'instance de l'agent.

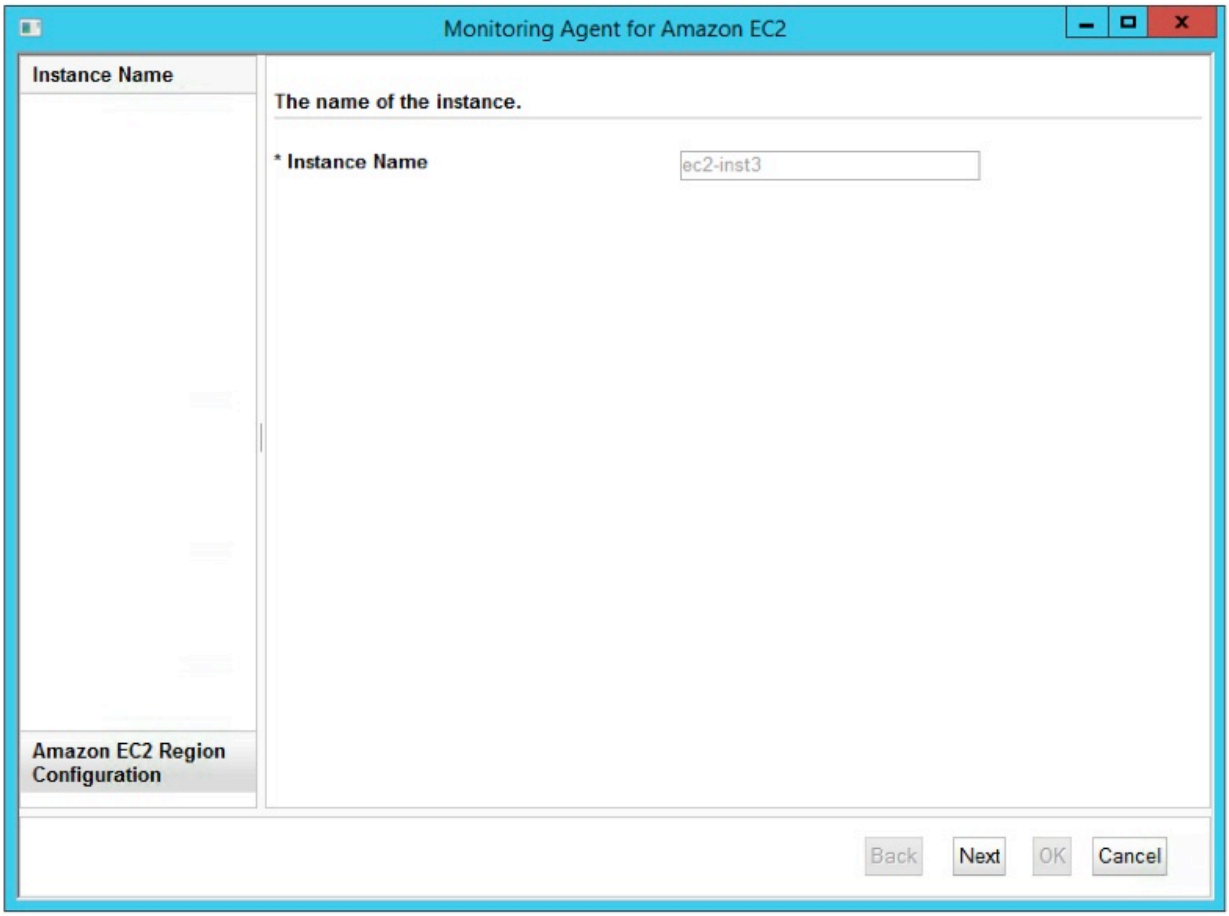


Figure 4. Fenêtre du nom d'instance de l'agent.

5. Entrez les paramètres du modèle d'instance **Amazon EC2 Region Configuration**.

   Remarque : Cette section ne décrit pas la configuration d'instance de région Amazon EC2. Il s'agit d'un modèle de section des paramètres utilisés comme valeurs par défaut lorsque vous ajoutez les configurations d'instance de région Amazon EC2 réelles à l'étape 6.

   Pour obtenir une description de chaque paramètre de configuration, voir Tableau 14, à la page 200.

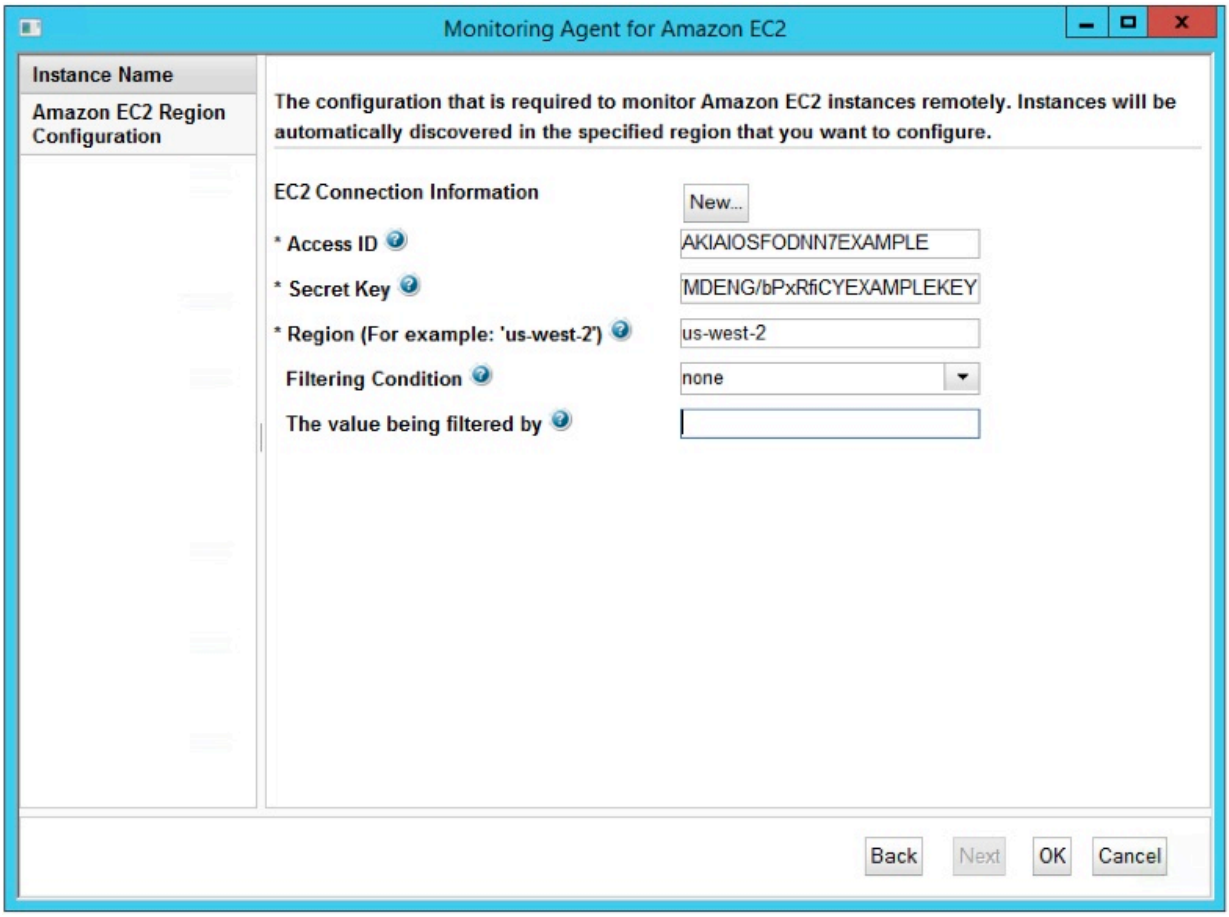


Figure 5. Fenêtre de spécification des paramètres du modèle d'instance de région Amazon EC2.

6. Cliquez sur **Nouveau** et entrez les paramètres d'instance de région Amazon EC2, puis cliquez sur **Suivant**.

   Voir Tableau 14, à la page 200 pour obtenir une description de chaque paramètre de configuration.

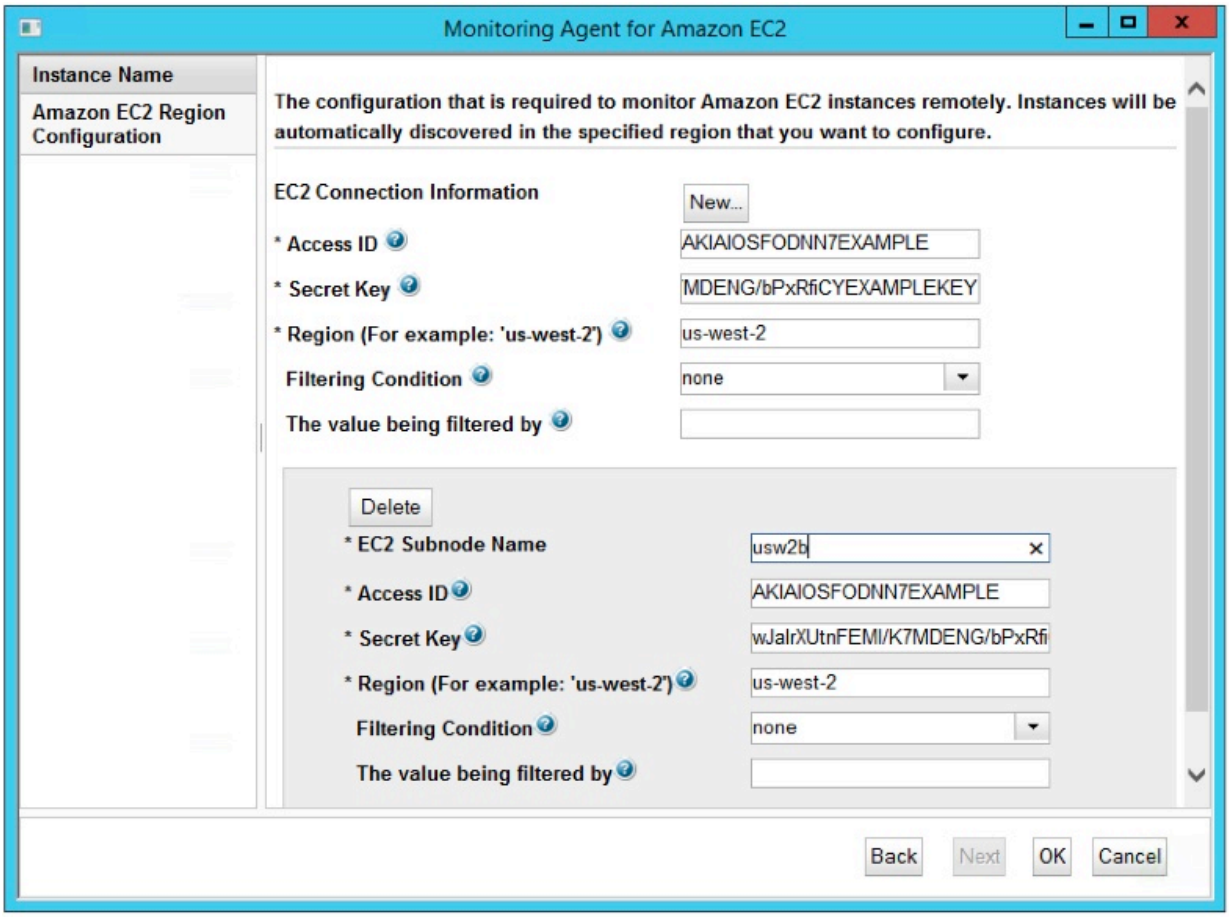


Figure 6. Fenêtre de spécification des paramètres d'instance de région Amazon EC2.

7. Cliquez sur **OK** pour terminer la configuration.
8. Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur l'instance que vous avez configurée, puis cliquez sur **Démarrer**.

Configuration de l'agent en répondant à des invites.

Après avoir installé l'agent Amazon EC2, vous devez le configurer pour pouvoir le démarrer. Si l'agent Amazon EC2 est installé sur un ordinateur Linux, vous pouvez suivre ces instructions pour le configurer de manière interactive en suivant des invites de ligne de commande.

Pourquoi et quand exécuter cette tâche

A faire : Si vous reconfigurez une instance d'agent configurée, la valeur définie dans la dernière configuration s'affiche pour chaque paramètre. Pour effacer une valeur existante, appuyez sur la touche Espace lorsque le paramètre s'affiche.

Procédure

Procédez comme suit pour configurer l'agent Amazon EC2 en exécutant un script et en répondant aux invites.

1. Exécutez la commande suivante :

```
rép_install/bin/amazonec2-agent.sh config nom_instance
```

où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent.

Exemple

```
/opt/ibm/apm/agent/bin/amazonec2-agent.sh config ec2-inst3
```

2. Répondez aux invites pour définir les valeurs de configuration de l'agent.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'agent Amazon EC2», à la page 200.

3. Exécutez la commande suivante pour démarrer l'agent :

   ```
   rép_install/bin/amazonec2-agent.sh start nom_instance
   ```

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

   Exemple

   ```
   /opt/ibm/apm/agent/bin/amazonec2-agent.sh start ec2-inst3
   ```

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration de l'agent. Ce mode de configuration est appelé mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

- Configurez l'agent Amazon EC2 en mode silencieux :
  a) Ouvrez le fichier `amazonec2_silent_config.txt` qui se trouve dans l'un des chemins ci-après, dans un éditeur de texte.
     – Linux *rép_install*`/samples/amazonec2_silent_config.txt`

       Par exemple, `/opt/ibm/apm/agent/samples/amazonec2_silent_config.txt`
     – Windows *rép_install*`\samples\amazonec2_silent_config.txt`

       Par exemple, `C:\IBM\APM\samples\amazonec2_silent_config.txt`

     où *rép_install* représente le chemin d'installation de l'agent.
  b) Dans le fichier `amazonec2_silent_config.txt`, spécifiez des valeurs pour tous les paramètres obligatoires et modifiez les valeurs des autres paramètres si nécessaire.

     Voir «Paramètres de configuration de l'agent Amazon EC2», à la page 200 pour obtenir une description de chaque paramètre de configuration.
  c) Sauvegardez et fermez le fichier `amazonec2_silent_config.txt`, puis exécutez la commande suivante :
     – Linux *rép_install*`/bin/amazonec2-agent.sh config` **nom_instance** *rép_install*`/samples/amazonec2_silent_config.txt`

       Par exemple, **/opt/ibm/apm/agent/bin/amazonec2-agent.sh config ec2-inst3 /opt/ibm/apm/agent/samples/amazonec2_silent_config.txt**

– Windows *rép_install*\bin\amazonec2-agent.bat config **nom_instance** *rép_install*\samples\amazonec2_silent_config.txt

Par exemple, **C:\IBM\APM\bin\amazonec2-agent.bat config ec2-inst3 C:\IBM\APM\samples\amazonec2_silent_config.txt**

où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent.

Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.

d) Exécutez la commande suivante pour démarrer l'agent :

– Linux *rép_install*/bin/amazonec2-agent.sh start **nom_instance**

Par exemple, **/opt/ibm/apm/agent/bin/amazonec2-agent.sh start ec2-inst3**

– Windows *rép_install*\bin\amazonec2-agent.bat start **nom_instance**

Par exemple, **C:\IBM\APM\bin\amazonec2-agent.bat start ec2-inst3**

où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

Paramètres de configuration de l'agent Amazon EC2

Les paramètres de configuration de l'agent Amazon EC2 sont regroupés dans un tableau.

1. Configuration de zone Amazon EC2 - Paramètres permettant de surveiller à distance les instances Amazon EC2. Les instances sont automatiquement reconnues dans la zone spécifiée que vous souhaitez configurer.

Tableau 14. Configuration de zone Amazon EC2

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Nom du sous-noeud EC2	Nom du sous-noeud EC2 pour la collecte des données. Par exemple, *usw2a*. Cet alias fait partie du nom de système géré et il est utilisé pour identifier visuellement l'environnement surveillé dans la console Cloud APM. **Remarque :** Cet alias peut être toute valeur que vous choisissez pour représenter l'instance de sous-noeud Amazon EC2 avec les restrictions suivantes. Les lettres de l'alphabet latin (a-z, A-Z), les chiffres arabes (0-9), le trait d'union (-) et le caractère de soulignement (_) peuvent être utilisés pour créer des noms d'instance de sous-noeud d'agent. La longueur maximale d'un nom de sous-noeud EC2 est de 25 caractères.	Chacun des paramètres suivants doit avoir un suffixe de nom de sous-noeud d'agent qui est le même pour chaque paramètre d'une instance de sous-noeud d'agent. Les nouvelles instances de sous-noeud d'agent doivent utiliser un nom unique pour leur jeu de paramètres. Par exemple, une instance de sous-noeud d'agent peut utiliser *.usw2a* et une autre instance de sous-noeud d'agent peut utiliser *.usw2b* à la place de *.subnode_name* dans les noms de paramètres qui suivent.
ID d'accès	ID de clé d'accès de droits de sécurité AWS servant à l'authentification auprès de la zone Amazon spécifiée. Par exemple, "AKIAxxxxxxxxxxxxxx".	**KB5_INS_ACCESS_ID.subnode_name**

Tableau 14. Configuration de zone Amazon EC2 (suite)

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Clé confidentielle	Clé d'accès confidentielle de droits d'accès de sécurité AWS servant à l'authentification auprès de la zone Amazon spécifiée. Par exemple, "kK7txxxxxxxxxxxxxxxxxxxxxxxx".	**KB5_INS_SECRET_KEY.subnode_name**
Zone	Zone AWS à surveiller. Par exemple, 'us-west-2'.	**KB5_INS_REGION.subnode_name**
Condition de filtrage	Type de filtrage réalisé. Vous pouvez utiliser des balises personnalisées sur les instances EC2 pour limiter les instances EC2 surveillées par l'agent. Pour plus d'informations, voir Balisage de vos ressources Amazon EC2. Options de filtrage, **néant** Toutes les instances EC2 au sein de la zone sont surveillées. **Valeur de filtre** est ignorée. **tagName** Les instances EC2 avec la clé de balise qui est spécifiée dans **Valeur de filtre** sont surveillées, quelle que soit la valeur réelle dans la valeur de balise d'instance EC2 correspondante. Par exemple, pour surveiller toutes les instances EC2 qui ont la clé de balise *Stack*, quelle que soit leur valeur de balise, spécifiez `Stack` dans **Valeur de filtre**. **tagName|tagValue** Les instances EC2 dont la clé de balise et la paire de valeurs de balise sont séparées par une barre verticale (|), et qui sont spécifiées dans **Valeur de filtre** sont surveillées. Par exemple, pour surveiller toutes les instances EC2 qui ont la clé de balise *Stack* et la valeur de balise *Production*, spécifiez `Stack|Production` dans **Valeur de filtre**. **monitoring-tag** Les instances EC2 qui ont au moins une balise sont surveillées. **Valeur de filtre** est ignorée.	**FILTER_CONDITION.subnode_name** Les valeurs possibles sont les suivantes : **néant** none **tagName** tagName **tagName|tagValue** tagName|tagValue **monitoring-tag** monitoring-tag

Tableau 14. Configuration de zone Amazon EC2 (suite)		
Nom du paramètre	**Description**	**Nom du paramètre de fichier de configuration en mode silencieux**
Valeur de filtre	Valeur de la balise en fonction de laquelle les instances EC2 sont filtrées lorsque `tagName` ou `tagName|tagValue` est sélectionné pour la **`Condition de filtrage`**.	**`FILTER_VALUE.subnode_name`**

Configuration de la surveillance d'AWS Elastic Load Balancer

L'agent Amazon ELB permet de surveiller de manière centralisée la santé, la disponibilité et les performances de vos équilibreurs de charge élastiques AWS. L'agent affiche un ensemble complet de mesures pour chaque type d'équilibreur de charge, application, réseau et classique, qui vous aident à prendre des décisions avisées concernant votre environnement AWS Elastic Load Balancer.

Avant de commencer

- Lisez l'intégralité de la rubrique «Configuration de la surveillance d'AWS Elastic Load Balancer», à la page 202 pour déterminer les éléments nécessaires à l'achèvement de la configuration.
- Les instructions figurant dans cette rubrique concernent l'édition la plus récente de l'agent, sauf indication contraire.
- Assurez-vous que votre environnement possède la configuration système requise pour l'agent Amazon ELB. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Amazon ELB.
- Vérifiez que les informations suivantes sont disponibles :
  - Les droits de sécurité AWS (ID de clé d'accès et clé d'accès secrète) avec l'autorisation d'accès à chaque région AWS avec les équilibreurs de charge élastiques.

Pourquoi et quand exécuter cette tâche

L'agent Amazon ELB est à la fois un agent à plusieurs instances et un agent de sous-noeud. Les sous-noeuds sont créés automatiquement pour chaque type d'équilibreur de charge élastique disponible dans votre environnement AWS.

Procédure

1. Configurez l'agent sur des systèmes Windows avec la fenêtre **IBM Performance Management** ou le fichier de réponses silencieux.
   - «Configuration de l'agent sur des systèmes Windows», à la page 203.
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 205.
2. Configurez l'agent sur des systèmes Linux avec le script qui génère des invites pour les réponses ou le fichier de réponses silencieux.
   - «Configuration de l'agent en répondant aux invites», à la page 204.
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 205.

Que faire ensuite

Dans la console Cloud APM, accédez à votre Tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Pour identifier et résoudre les incidents, reportez-vous au forum Cloud Application Performance Management.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent Amazon ELB sur les systèmes d'exploitation Windows dans la fenêtre IBM Cloud Application Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur le modèle **Monitoring Agent for AWS Elastic Load Balancer**, puis cliquez sur **Configure agent**.

   A faire : Après avoir configuré une instance d'agent pour la première fois, l'option **Configure agent** est désactivée. Pour reconfigurer l'instance d'agent, cliquez dessus avec le bouton droit de la souris et sélectionnez **Reconfigure**.
3. Entrez un nom d'instance unique, puis cliquez sur **OK**. N'utilisez que des lettres latines, des chiffres arabes, le caractère de soulignement et le caractère moins dans le nom de l'instance. Par exemple, `elb-inst3`. Pour plus d'informations, voir *nom_instance* sous «Format de MSN commun pour les agents multi-instance», à la page 172.

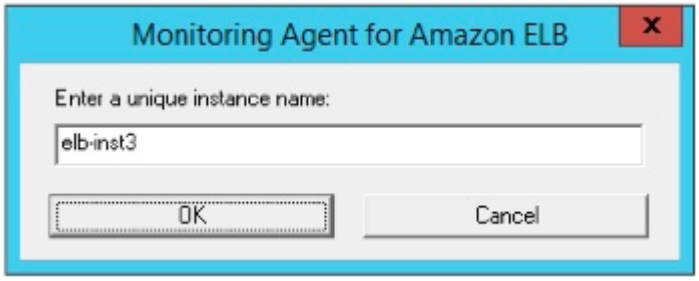


Figure 7. Fenêtre de saisie d'un nom d'instance d'agent unique.

4. Entrez les **données d'identification d'abonnement Amazon ELB**, puis cliquez sur **Suivant**.

   Voir «Paramètres de configuration de l'agent Amazon ELB», à la page 207 pour obtenir une description de chaque paramètre de configuration.

   Important : Windows Si votre **clé secrète/mot de passe** contient le signe égal (=), vous devez la/le saisir à nouveau chaque fois que vous reconfigurez l'agent.

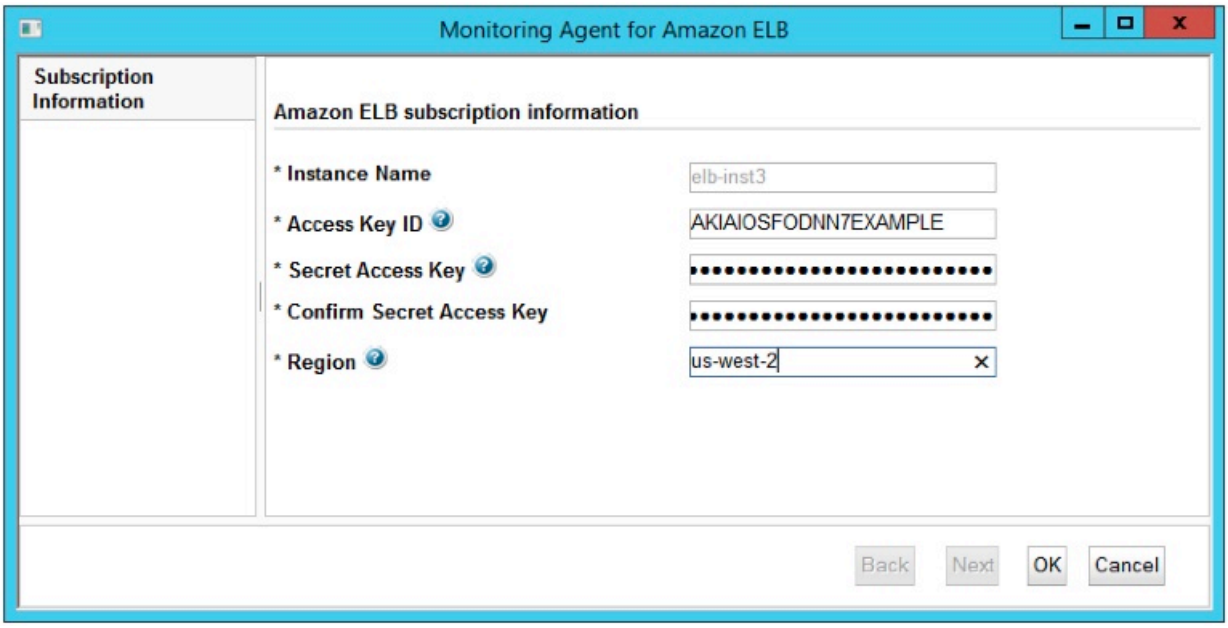


Figure 8. Fenêtre des données d'identification d'abonnement Amazon ELB.

5. Cliquez sur **OK** pour terminer la configuration.
6. Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur l'instance que vous avez configurée, puis cliquez sur **Démarrer**.

Configuration de l'agent en répondant aux invites

Après avoir installé l'agent Amazon ELB, vous devez le configurer pour pouvoir le démarrer. Si l'agent Amazon ELB est installé sur un ordinateur Linux, vous pouvez suivre ces instructions pour le configurer de manière interactive en suivant des invites de ligne de commande.

Pourquoi et quand exécuter cette tâche

A faire : Si vous reconfigurez une instance d'agent configurée, la valeur définie dans la dernière configuration s'affiche pour chaque paramètre. Pour effacer une valeur existante, appuyez sur la touche Espace lorsque le paramètre s'affiche.

Procédure

Procédez comme suit pour configurer l'agent Amazon ELB en exécutant un script et en répondant aux invites.

1. Exécutez la commande suivante :

   ```
   rép_install/bin/amazon_elb-agent.sh config nom-instance
   ```

   Où *rép_install* représente le chemin d'installation de l'agent et *nom-instance*, le nom à affecter à l'instance d'agent. N'utilisez que des lettres latines, des chiffres arabes et le caractère moins dans *nom-instance*. Pour plus d'informations, voir *nom_instance* sous «Format de MSN commun pour les agents multi-instance», à la page 172.

   Exemple

   ```
   /opt/ibm/apm/agent/bin/amazon_elb-agent.sh config elb-inst3
   ```

2. Répondez aux invites pour définir les valeurs de configuration de l'agent.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'agent Amazon ELB», à la page 207.

3. Exécutez la commande suivante pour démarrer l'agent :

```
rép_install/bin/amazon_elb-agent.sh start nom-instance
```

Où *rép_install* représente le chemin d'installation de l'agent et *nom-instance*, le nom de l'instance d'agent.

Exemple

```
/opt/ibm/apm/agent/bin/amazon_elb-agent.sh start elb-inst3
```

Exemple

Création d'une instance d'agent nommée `elb-inst3`.

```
# ./amazon_elb-agent.sh config elb-inst3
Configuring Monitoring Agent for Amazon ELB

Edit 'Monitoring Agent for Amazon ELB' settings? [1=Yes,2=No](default is: 1): 1

Subscription Information :
Amazon ELB subscription information

The access ID that is used to authenticate with the specified Amazon Region.
Par exemple, 'AKIAxxxxxxxxxxxxxx'.
Access Key ID (default is: ): AKIAIOSFODNN7EXAMPLE

The secret access key that is used to authenticate with the specified Amazon
Region. Par exemple, 'kK7txxxxxxxxxxxxxxxxxxxxxxxxx'.
Enter Secret Access Key (default is: ): hidden

Re-type : Secret Access Key (default is: ): hidden

The Amazon region where the load balancers are located. Par exemple, 'us-west-2'.
Region (default is: ): us-west-2

Configuration completed successfully.
Automatic start at system initialization has been configured.
Automatic stop at system shutdown has been configured.
```

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration de l'agent. Ce mode de configuration est appelé mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

Procédez comme suit pour configurer l'agent Amazon ELB en mode silencieux.

1. Ouvrez le fichier `amazon_elb_silent_config.txt` qui se trouve dans l'un des chemins ci-après, dans un éditeur de texte.
   - Linux *rép_install*`/samples/amazon_elb_silent_config.txt`

     Par exemple, `/opt/ibm/apm/agent/samples/amazon_elb_silent_config.txt`
   - Windows *rép_install*`\samples\amazon_elb_silent_config.txt`

     Par exemple, `C:\IBM\APM\samples\amazon_elb_silent_config.txt`

Où *rép_install* représente le chemin d'installation de l'agent.

2. Dans le fichier `amazon_elb_silent_config.txt`, spécifiez des valeurs pour tous les paramètres obligatoires et modifiez les valeurs des autres paramètres si nécessaire.

   Voir «Paramètres de configuration de l'agent Amazon ELB», à la page 207 pour obtenir une description de chaque paramètre de configuration.

3. Sauvegardez et fermez le fichier `amazon_elb_silent_config.txt`, puis exécutez la commande suivante :

   - Linux *rép_install*`/bin/amazon_elb-agent.sh config` **nom-instance** *rép_install*`/samples/amazon_elb_silent_config.txt`

     Par exemple, **/opt/ibm/apm/agent/bin/amazon_elb-agent.sh config elb-inst3 /opt/ibm/apm/agent/samples/amazon_elb_silent_config.txt**

   - Windows *rép_install*`\bin\amazon_elb-agent.bat config` **nom-instance** *rép_install*`\samples\amazon_elb_silent_config.txt`

     Par exemple, **C:\IBM\APM\bin\amazon_elb-agent.bat config elb-inst3 C:\IBM\APM\samples\amazon_elb_silent_config.txt**

   Où *rép_install* représente le chemin d'installation de l'agent et *nom-instance*, le nom à affecter à l'instance d'agent. N'utilisez que des lettres latines, des chiffres arabes et le caractère moins dans *nom-instance*. Pour plus d'informations, voir *nom_instance* sous «Format de MSN commun pour les agents multi-instance», à la page 172.

   Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.

4. Exécutez la commande suivante pour démarrer l'agent :

   - Linux *rép_install*`/bin/amazon_elb-agent.sh start` **nom-instance**

     Par exemple, **/opt/ibm/apm/agent/bin/amazon_elb-agent.sh start elb-inst3**

   - Windows *rép_install*`\bin\amazon_elb-agent.bat start` **nom-instance**

     Par exemple, **C:\IBM\APM\bin\amazon_elb-agent.bat start elb-inst3**

   Où *rép_install* représente le chemin d'installation de l'agent et *nom-instance*, le nom de l'instance d'agent.

Exemple

Fichier `amazon_elb_silent_config.txt` édité.

```
#
# Ce fichier est un exemple de fichier de réponses de configuration pour l'agent Amazon ELB.
#
# Il contient une entrée pour chaque propriété de configuration.
# Les entrées des propriétés facultatives qui n'ont pas de valeur par défaut sont incluses
# dans les commentaires.
# Vérifiez que toutes les propriétés non mises en commentaires ont une valeur avant de
configurer
# l'agent.
#

# ID de clé d'accès : ID d'accès servant à l'authentification auprès
# de la région Amazon spécifiée. Par exemple, 'AKIAxxxxxxxxxxxxxxx'.
KAL_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

# Clé d'accès secrète : clé d'accès secrète servant à l'authentification auprès
# de la région Amazon spécifiée. Par exemple, 'kK7txxxxxxxxxxxxxxxxxxxxxxxxxx'.
KAL_SECRET_ACCESS_KEY_PASSWORD=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

# Région : région Amazon où se trouvent les équilibreurs de charge. Par
# exemple, 'us-west-2'.
KAL_REGION=us-west-2
```

Paramètres de configuration de l'agent Amazon ELB

Les paramètres de configuration de l'agent Amazon ELB sont regroupés dans un tableau.

1. Tableau 15, à la page 207 - Données d'identification requises pour accéder à l'abonnement Amazon qui contient les équilibreurs de charge élastiques AWS à surveiller.

Tableau 15. Informations sur l'abonnement

Nom de paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
ID clé d'accès	ID d'accès servant à l'authentification auprès de la région Amazon spécifiée. Par exemple, 'AKIAxxxxxxxxxxxxxxx'.	**KAL_ACCESS_KEY_ID**
Clé d'accès secrète	Clé d'accès secrète servant à l'authentification auprès de la région Amazon spécifiée. Par exemple, 'kK7txxxxxxxxxxxxxxxxxxxxxxxxx'.	**KAL_SECRET_ACCESS_KEY_PASSWORD**
Région	Région Amazon où se trouvent les équilibreurs de charge. Par exemple, "us-west-2".	**KAL_REGION**

Configuration de la surveillance Azure Compute

L'Agent Azure Compute permet de surveiller de manière centralisée la santé, la disponibilité et les performances de vos instances Azure Compute. L'agent affiche un ensemble complet de mesures qui vous aident à prendre des décisions avisées concernant votre environnement Azure Compute. Ces mesures incluent l'utilisation de l'UC, l'utilisation du réseau et les performances du disque.

Avant de commencer

- Lisez l'intégralité de la rubrique «Configuration de la surveillance Azure Compute», à la page 207 pour déterminer les éléments nécessaires à l'achèvement de la configuration.
- Les instructions figurant dans cette rubrique concernent l'édition la plus récente de l'agent, sauf indication contraire.
- Assurez-vous que votre environnement possède la configuration système requise pour l'Agent Azure Compute. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent Azure Compute.
- Vérifiez que les informations suivantes sont disponibles :
  - Les données d'identification d'abonnement Azure avec le droit d'accéder aux instances Azure Compute à surveiller. Voir «Informations de configuration d'Azure Compute», à la page 208 pour plus de détails.

Pourquoi et quand exécuter cette tâche

L'Agent Azure Compute est à la fois un agent à plusieurs instances et un agent de sous-noeud. Chaque sous-noeud de l'Agent Azure Compute surveille un regroupement de machines virtuelles Azure Compute en fonction du filtre que vous définissez. Vous pouvez créer une instance d'agent à plusieurs sous-noeuds (un pour chaque regroupement de machines virtuelles) ou une instance d'agent pour chaque regroupement de machines virtuelles avec un sous-noeud pour ce regroupement . Vous pouvez également créer une combinaison de chaque type de configuration. Après avoir configuré les instances d'agent, démarrez chacune d'elles manuellement. Il est conseillé de ne pas avoir plus de 50 ressources par regroupement de machines virtuelles Azure Compute. Chaque nom de sous-noeud de l'agent Azure Compute doit être unique dans votre environnement.

Procédure

1. Configurez l'agent sur des systèmes Windows avec la fenêtre **IBM Performance Management** ou le fichier de réponses silencieux.
   - «Configuration de l'agent sur des systèmes Windows», à la page 209.
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 213.
2. Configurez l'agent sur des systèmes Linux avec le script qui génère des invites pour les réponses ou le fichier de réponses silencieux.
   - «Configuration de l'agent en répondant à des invites», à la page 211.
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 213.

Que faire ensuite

Dans la console Cloud APM, accédez à votre Tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Pour identifier et résoudre les incidents, reportez-vous au forum Cloud Application Performance Management.

Informations de configuration d'Azure Compute

L'Agent Azure Compute requiert des étapes de configuration supplémentaires dans l'environnement Azure Compute.

Pourquoi et quand exécuter cette tâche

Pour exécuter ces étapes, vous devez vous connecter à la console Microsoft Azure.

Procédure

1. ID abonnement
   - Dans le panneau de gauche, sélectionnez "Subscriptions" et choisissez l'abonnement à utiliser pour cet agent.
   - Sélectionnez "Overview", puis copiez l'ID d'abonnement. Ce dernier sera utilisé en tant que paramètre de configuration de l'agent.
2. ID titulaire
   - Accédez à "Azure Active Directory".
   - Sélectionnez "Properties", puis copiez l'ID titulaire.
3. Enregistrer une application
   - Accédez à "All services" et recherchez "App registrations".
   - Cliquez sur "New Application Registration".
   - Indiquez un nom, sélectionnez le type d'application "Web App/API" et une URL de connexion (n'importe laquelle puisqu'elle ne sera pas utilisée).
   - Cliquez sur "Create".
   - Copiez l'ID d'application - il sera utilisé dans la zone "Client ID" de l'agent.
4. Créer la clé d'application

- Cliquez sur l'appli que vous venez de créer, puis accédez à "Settings" suivi de "Keys".
- Entrez une description ("IBM Key" par exemple) et une durée ("Never Expires" par exemple), puis cliquez sur "Save".
- Copiez la clé secrète et stockez-la dans un lieu sûr - vous ne verrez cette clé qu'une seule fois et devrez en générer une nouvelle si vous la perdez.

5. Attribuer des autorisations d'application
   - Accédez à "Subscriptions" et sélectionnez l'abonnement à surveiller.
   - Accédez à "Access Control (IAM) et cliquez sur "Add".
   - Sélectionnez le rôle "Reader" ou un rôle supérieur à surveiller.
   - Sous "Select", recherchez l'appli que vous venez d'enregistrer et sélectionnez-la, puis cliquez sur "Save".

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'Agent Azure Compute sur les systèmes d'exploitation Windows dans la fenêtre IBM Cloud Application Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur le modèle **Monitoring Agent for Azure Compute**, puis cliquez sur **Configure agent**.

   A faire : Après avoir configuré une instance d'agent pour la première fois, l'option **Configure agent** est désactivée. Pour reconfigurer l'instance d'agent, cliquez dessus avec le bouton droit de la souris et sélectionnez **Reconfigure**.
3. Entrez un nom d'instance unique, puis cliquez sur **OK**. N'utilisez que des lettres latines, des chiffres arabes, le caractère de soulignement et le caractère moins dans le nom de l'instance. Par exemple, `azc-inst3`. Pour plus d'informations, voir *nom_instance* sous «Format de MSN commun pour les agents multi-instance», à la page 172.

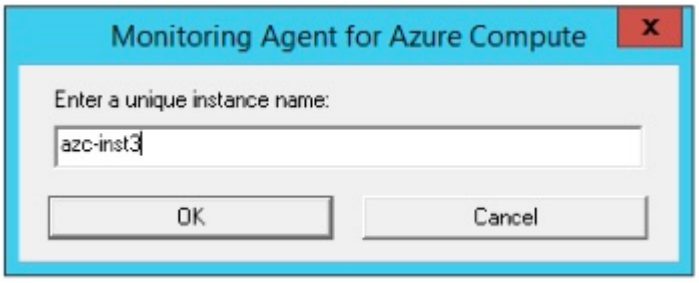


Figure 9. Fenêtre de saisie d'un nom d'instance d'agent unique.

4. Entrez les **données d'identification d'abonnement Azure**, puis cliquez sur **Suivant**.

   Pour obtenir une description de chaque paramètre de configuration, voir Tableau 16, à la page 215.

   Important : Windows Si votre **`clé secrète/mot de passe`** contient le signe égal (=), vous devez la/le saisir à nouveau chaque fois que vous reconfigurez l'agent.

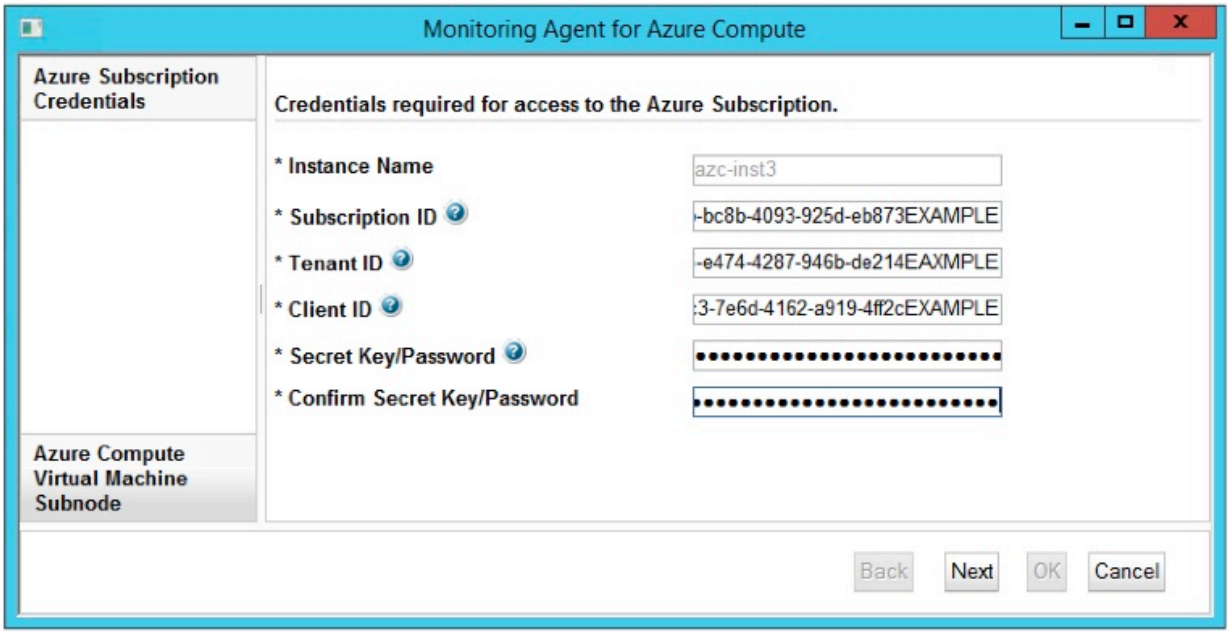


Figure 10. Fenêtre des données d'identification d'abonnement Azure.

5. Entrez les paramètres du modèle de **sous-noeud de machine virtuelle Azure Compute**.

   Pour obtenir une description de chaque paramètre de configuration, voir Tableau 17, à la page 216.

   Remarque : Cette section ne permet pas de configurer l'instance du sous-noeud de machine virtuelle Azure Compute. Il s'agit d'un modèle de section qui permet de définir les valeurs par défaut utilisées lorsque vous ajoutez les configurations réelles de l'instance du sous-noeud de machine virtuelle Azure Compute à l'étape 6.

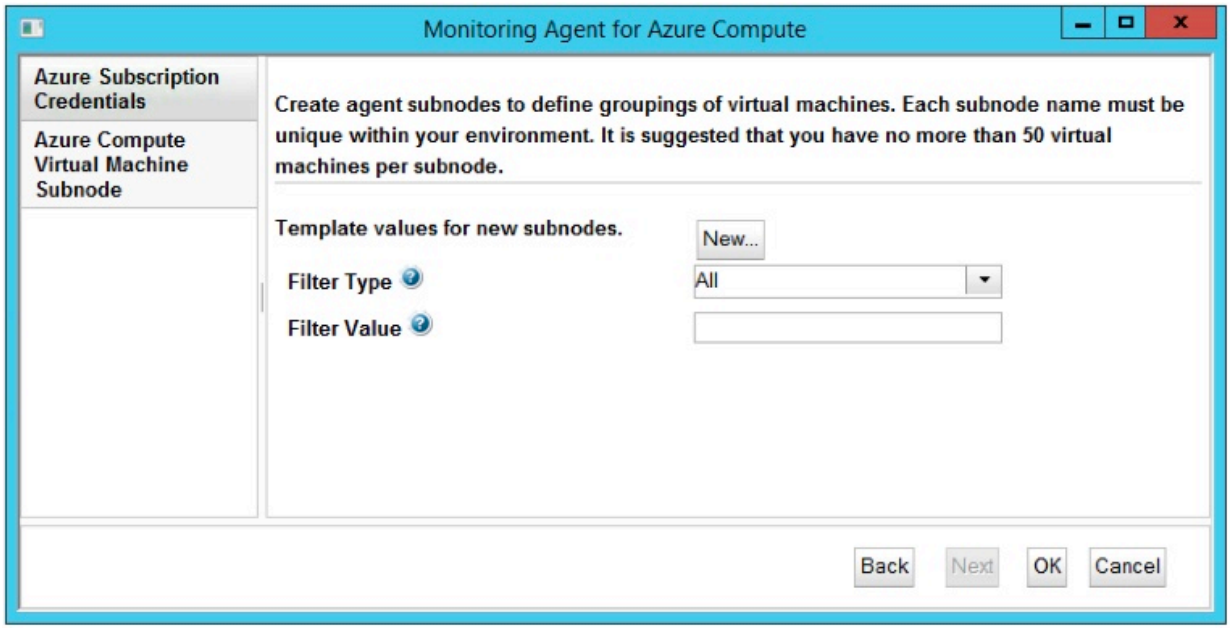


Figure 11. Fenêtre de spécification des paramètres de modèle de sous-noeud de machine virtuelle Azure Compute.

6. Cliquez sur **Nouveau** et entrez les paramètres de l'instance du **sous-noeud de machine virtuelle Azure Compute**, puis cliquez sur **Suivant**.

   Pour obtenir une description de chaque paramètre de configuration, voir Tableau 17, à la page 216.

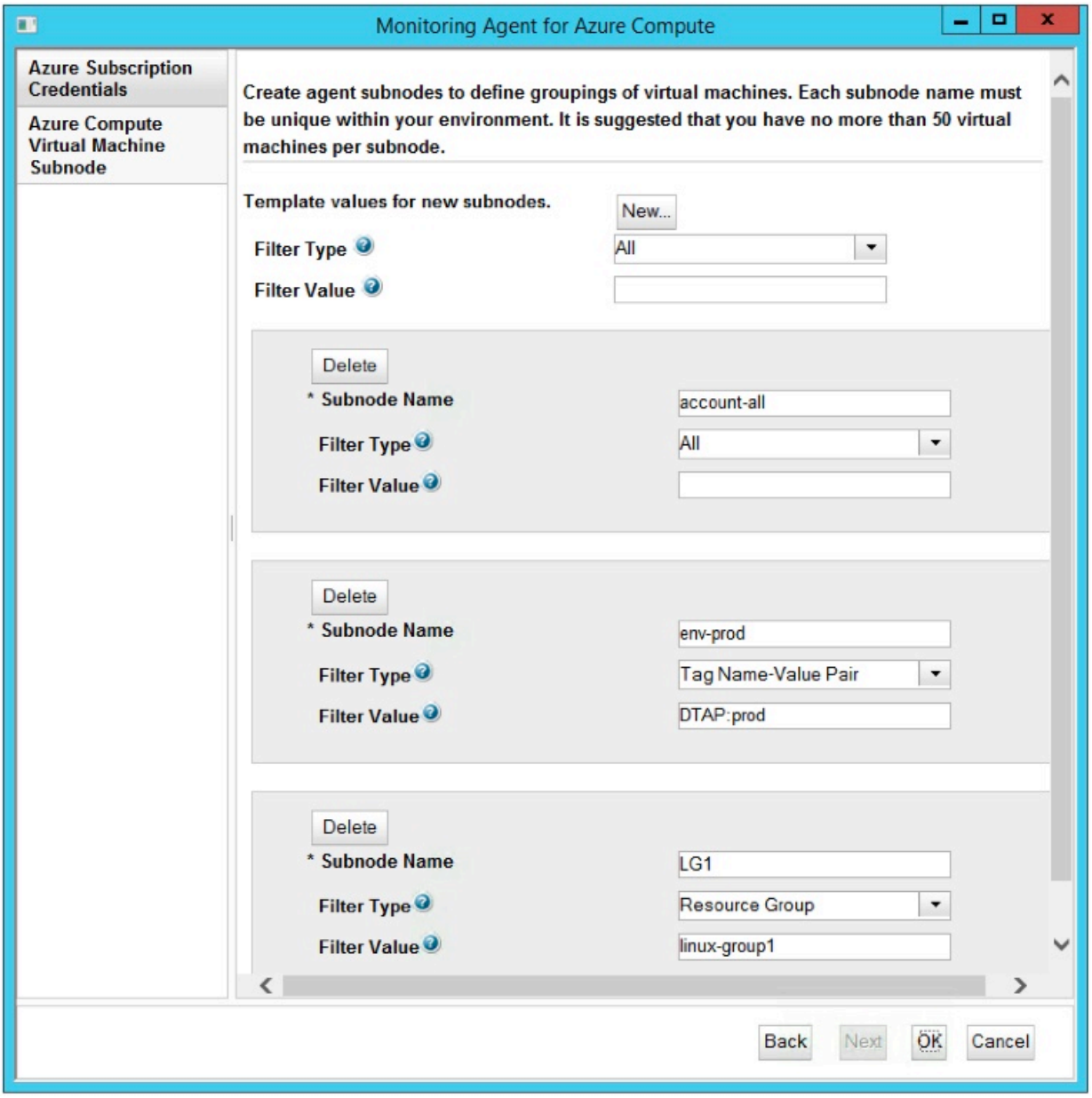


Figure 12. Fenêtre de spécification des paramètres de l'instance du sous-noeud de machine virtuelle Azure Compute.

7. Cliquez sur **OK** pour terminer la configuration.
8. Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur l'instance que vous avez configurée, puis cliquez sur **Démarrer**.

Configuration de l'agent en répondant à des invites

Après avoir installé l'Agent Azure Compute, vous devez le configurer pour pouvoir le démarrer. Si l'Agent Azure Compute est installé sur un ordinateur Linux, vous pouvez suivre ces instructions pour le configurer de manière interactive en suivant des invites de ligne de commande.

Pourquoi et quand exécuter cette tâche

A faire : Si vous reconfigurez une instance d'agent configurée, la valeur définie dans la dernière configuration s'affiche pour chaque paramètre. Pour effacer une valeur existante, appuyez sur la touche Espace lorsque le paramètre s'affiche.

Procédure

Procédez comme suit pour configurer l'Agent Azure Compute en exécutant un script et en répondant aux invites.

1. Exécutez la commande suivante :

   ```
   rép_install/bin/azure_compute-agent.sh config nom-instance
   ```

   Où *rép_install* représente le chemin d'installation de l'agent et *nom-instance*, le nom à affecter à l'instance d'agent. N'utilisez que des lettres latines, des chiffres arabes et le caractère moins dans *nom-instance*. Pour plus d'informations, voir *nom_instance* sous «Format de MSN commun pour les agents multi-instance», à la page 172.

   Exemple

   ```
   /opt/ibm/apm/agent/bin/azure_compute-agent.sh config azc-inst3
   ```

2. Répondez aux invites pour définir les valeurs de configuration de l'agent.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'Agent Azure Compute», à la page 215.

   A faire : Lorsque vous configurez une instance d'agent pour la première fois, vous devez ajouter au moins un sous-noeud lorsque vous êtes invité à modifier les paramètres du sous-noeud de machine virtuelle Azure Compute (**Edit 'Azure Compute Virtual Machine Subnode' settings**).

3. Exécutez la commande suivante pour démarrer l'agent :

   ```
   rép_install/bin/azure_compute-agent.sh start nom-instance
   ```

   Où *rép_install* représente le chemin d'installation de l'agent et *nom-instance*, le nom de l'instance d'agent.

   Exemple

   ```
   /opt/ibm/apm/agent/bin/azure_compute-agent.sh start azc-inst3
   ```

Exemple

Création d'une instance d'agent nommée `azc-inst3` et dotée d'une instance de sous-noeud nommée `azc1`.

```
# ./azure_compute-agent.sh config azc-inst3
Configuring Monitoring Agent for Azure Compute

Edit 'Monitoring Agent for Azure Compute' settings? [1=Yes,2=No](default is: 1): 1

Azure Subscription Credentials :
Credentials required for access to the Azure Subscription.

The ID assigned by Azure for the Subscription that is monitored.
Subscription ID (default is: ): 09x73b6b-bcxb-40x3-92xd-ebx7-EXAMPLE

The tenant ID that is assigned by Azure. Used to log in to the Azure service API.
Tenant ID (default is: ): 75x2e745-e4x4-42x7-94xb-dex1-EXAMPLE

The client ID that is assigned by Azure to identify this agent as an external
application that monitors the Azure compute services.
Client ID (default is: ): 79x2e6c3-7exd-41x2-a9x9-4fx2-EXAMPLE

The secret access key or password that is created by Azure for the client application.
Enter Secret Key/Password (default is: ): hidden

Re-type : Secret Key/Password (default is: ): hidden

Azure Compute Virtual Machine Subnode :

Create agent subnodes to define groupings of virtual machines. Each subnode name
must be unique within your environment. It is suggested that you have no more
than 50 virtual machines per subnode.
```

```
No 'Azure Compute Virtual Machine Subnode' settings available.
Edit 'Azure Compute Virtual Machine Subnode' settings, [1=Add, 2=Edit, 3=Del,
4=Next, 5=Exit] (default is: 5): 1
Subnode Name (default is: ): azc1
The type of filter to be applied.
Filter Type [ 1=All, 2=Tag Name-Value Pair, 3=Resource Group ] (default is: 1): 2
The filter value corresponding to the selected Filter Type. This value can be a
Resource Group or Tag Name-Value Pair, for example Environment\:Production.
A backslash might appear in the example, do not enter a backslash in the value
you provide.
Filter Value (default is: ): Environment:Production



Azure Compute Virtual Machine Subnode settings: Subnode Name=azc1
Edit 'Azure Compute Virtual Machine Subnode' settings, [1=Add, 2=Edit, 3=Del,
4=Next, 5=Exit] (default is: 5): 5
Configuration completed successfully.
Automatic start at system initialization has been configured.
Automatic stop at system shutdown has been configured.
You have new mail in /var/spool/mail/root
```

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration de l'agent. Ce mode de configuration est appelé mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

Procédez comme suit pour configurer l'Agent Azure Compute en mode silencieux.

1. Ouvrez le fichier `azure_compute_silent_config.txt` qui se trouve dans l'un des chemins ci-après, dans un éditeur de texte.
   - Linux *rép_install*`/samples/azure_compute_silent_config.txt`

     Par exemple, `/opt/ibm/apm/agent/samples/azure_compute_silent_config.txt`
   - Windows *rép_install*`\samples\azure_compute_silent_config.txt`

     Par exemple, `C:\IBM\APM\samples\azure_compute_silent_config.txt`

   Où *rép_install* représente le chemin d'installation de l'agent.
2. Dans le fichier `azure_compute_silent_config.txt`, spécifiez des valeurs pour tous les paramètres obligatoires et modifiez les valeurs des autres paramètres si nécessaire.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'Agent Azure Compute», à la page 215.

   Important : Vous devez activer et spécifier les paramètres Filter Type et Filter Value pour au moins un nom de sous-noeud.
3. Sauvegardez et fermez le fichier `azure_compute_silent_config.txt` et exécutez la commande suivante :
   - Linux *rép_install*`/bin/azure_compute-agent.sh config` **nom-instance** *rép_install*`/samples/azure_compute_silent_config.txt`

Par exemple, **/opt/ibm/apm/agent/bin/azure_compute-agent.sh config azc-inst3 /opt/ibm/apm/agent/samples/azure_compute_silent_config.txt**

- Windows *rép_install*\bin\azure_compute-agent.bat config **nom-instance** *rép_install*\samples\azure_compute_silent_config.txt

  Par exemple, **C:\IBM\APM\bin\azure_compute-agent.bat config azc-inst3 C:\IBM\APM\samples\azure_compute_silent_config.txt**

Où *rép_install* représente le chemin d'installation de l'agent et *nom-instance*, le nom à affecter à l'instance d'agent. N'utilisez que des lettres latines, des chiffres arabes et le caractère moins dans *nom-instance*. Pour plus d'informations, voir *nom_instance* sous «Format de MSN commun pour les agents multi-instance», à la page 172.

Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.

4. Exécutez la commande suivante pour démarrer l'agent :

   - Linux *rép_install*/bin/azure_compute-agent.sh start **nom-instance**

     Par exemple, **/opt/ibm/apm/agent/bin/azure_compute-agent.sh start azc-inst3**

   - Windows *rép_install*\bin\azure_compute-agent.bat start **nom-instance**

     Par exemple, **C:\IBM\APM\bin\azure_compute-agent.bat start azc-inst3**

   Où *rép_install* représente le chemin d'installation de l'agent et *nom-instance*, le nom de l'instance d'agent.

Exemple

Fichier azure_compute_silent_config.txt édité avec trois sous-noeuds nommés account-all, env-prod et LG1.

```
#
# Ce fichier est un exemple de fichier de réponses de configuration pour l'agent Azure Compute.
#
# Il contient une entrée pour chaque propriété de configuration.
# Les entrées des propriétés facultatives qui n'ont pas de valeur par défaut sont incluses
# dans les commentaires.
# Les entrées du sous-noeud AVM se voient attribuer l'exemple de nom d'instance de sous-noeud
avm1.
# Vérifiez que toutes les propriétés non mises en commentaires ont une valeur avant de
configurer
# l'agent.
#

# ID abonnement : ID attribué par Azure à l'abonnement
# surveillé.
KAK_SUBSCRIPTION_ID=09x73b6b-bcxb-40x3-92xd-ebx7-EXAMPLE
# ID titulaire : ID titulaire attribué par Azure. Permet de se connecter à
# l'API du service Azure.
KAK_TENANT_ID=75x2e745-e4x4-42x7-94xb-dex1-EXAMPLE
# ID client : ID client attribué par Azure pour identifier cet agent
# en tant qu'application externe
# qui surveille les services Azure Compute.
KAK_CLIENT_ID=79x2e6c3-7exd-41x2-a9x9-4fx2-EXAMPLE
# Clé secrète/Mot de passe : clé d'accès secrète ou mot de passe créé(e) par
# Azure pour l'application client.
KAK_SECRET_PASSWORD=hZxWPq/IOxlnvg/wdxLwTf2Fs3x2sWQV/sCE-EXAMPLE

# Type de filtre : type de filtre à appliquer.
# Valeurs valides : ALL (All), TAG_NAME_VALUE (paire nom-valeur de balise),
# RESOURCE_GROUP (groupe de ressources)
#KAK_FILTER_TYPE.avm1=ALL
# Valeur de filtre : valeur de filtre correspondant au type de filtre sélectionné.
# Cette valeur peut être un Groupe de ressources ou une paire Nom-valeur de balise, par exemple
# Environment:Production. Une barre oblique inversée peut apparaître dans l'exemple.
# Ne saisissez pas de barre oblique inversée dans la valeur que vous entrez.
#KAK_FILTER_VALUE.avm1=

# Type de filtre : type de filtre à appliquer.
# Valeurs valides : ALL (All), TAG_NAME_VALUE (paire nom-valeur de balise),
# RESOURCE_GROUP (groupe de ressources)
```

```
KAK_FILTER_TYPE.account-all=ALL
# Valeur de filtre : valeur de filtre correspondant au type de filtre sélectionné.
# Cette valeur peut être un Groupe de ressources ou une paire Nom-valeur de balise, par exemple
# Environment:Production. Une barre oblique inversée peut apparaître dans l'exemple.
# Ne saisissez pas de barre oblique inversée dans la valeur que vous entrez.
KAK_FILTER_VALUE.account-all=

# Type de filtre : type de filtre à appliquer.
# Valeurs valides : ALL (All), TAG_NAME_VALUE (paire nom-valeur de balise),
# RESOURCE_GROUP (groupe de ressources)
KAK_FILTER_TYPE.env-prod=TAG_NAME_VALUE
# Valeur de filtre : valeur de filtre correspondant au type de filtre sélectionné.
# Cette valeur peut être un Groupe de ressources ou une paire Nom-valeur de balise, par exemple
# Environment:Production. Une barre oblique inversée peut apparaître dans l'exemple.
# Ne saisissez pas de barre oblique inversée dans la valeur que vous entrez.
KAK_FILTER_VALUE.env-prod=DTAP:prod

# Type de filtre : type de filtre à appliquer.
# Valeurs valides : ALL (All), TAG_NAME_VALUE (paire nom-valeur de balise),
# RESOURCE_GROUP (groupe de ressources)
KAK_FILTER_TYPE.LG1=RESOURCE_GROUP
# Valeur de filtre : valeur de filtre correspondant au type de filtre sélectionné.
# Cette valeur peut être un Groupe de ressources ou une paire Nom-valeur de balise, par exemple
# Environment:Production. Une barre oblique inversée peut apparaître dans l'exemple.
# Ne saisissez pas de barre oblique inversée dans la valeur que vous entrez.
KAK_FILTER_VALUE.LG1=linux-group1
```

Paramètres de configuration de l'Agent Azure Compute

Les paramètres de configuration de l'Agent Azure Compute sont affichés dans des tableaux qui les regroupent par sections.

1. Tableau 16, à la page 215 - Données d'identification requises pour accéder à l'abonnement Azure qui contient les ressources Azure Compute à surveiller.
2. Tableau 17, à la page 216 - Créez des sous-noeuds d'agent pour définir des regroupements de machines virtuelles. Chaque nom du sous-noeud doit être unique dans votre environnement. Il est conseillé de ne pas avoir plus de 50 machines virtuelles par sous-noeud.

Tableau 16. Données d'identification pour l'abonnement Azure

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
ID abonnement	ID attribué par Azure pour l'abonnement surveillé.	**KAK_SUBSCRIPTION_ID**
ID titulaire	ID titulaire affecté par Azure. Utilisé pour la connexion à l'API de service Azure.	**KAK_TENANT_ID**
ID client	ID client affecté par Azure pour identifier cet agent en tant qu'application externe qui surveille les services Azure Compute.	**KAK_CLIENT_ID**
Clé secrète/Mot de passe	Clé d'accès secrète ou mot de passe créé(e) par Azure pour l'application client. **Important :** Windows Si votre **clé secrète/mot de passe** contient le signe égal (=), vous devez la/le saisir à nouveau chaque fois que vous reconfigurez l'agent.	**KAK_SECRET_PASSWORD**

Tableau 17. Sous-noeud de machine virtuelle Azure Compute		
Nom du paramètre	**Description**	**Nom du paramètre de fichier de configuration en mode silencieux**
Nom du sous-noeud	Nom du sous-noeud Azure Compute utilisé pour la collecte de données. Par exemple, *azc1*. Le nom du sous-noeud doit être unique dans votre environnement. Cet alias fait partie du nom de système géré (MSN) et permet d'identifier visuellement l'environnement surveillé dans la console Cloud APM. **Remarque :** Cet alias représente l'instance du sous-noeud Azure Compute avec les restrictions suivantes. Vous pouvez utiliser des lettres de l'alphabet latin (a-z, A-Z), des chiffres arabes (0-9), le trait d'union/ signe moins (-) et le caractère de soulignement (_) pour créer des noms d'instances de sous-noeud d'agent. La longueur maximale d'un nom de sous-noeud Azure Compute est de 25 caractères.	Chacun des paramètres suivants doit contenir un point (.) suivi du **nom de sous-noeud** d'agent comme suffixe. Le **nom du sous-noeud** doit être identique pour chaque paramètre de sous-noeud. Les nouvelles instances de sous-noeud d'agent doivent utiliser un **nom de sous-noeud** unique pour son ensemble de paramètres. Par exemple, une instance de sous-noeud d'agent peut utiliser *.azc1*, tandis qu'une autre peut utiliser *.azc2* en lieu et place de *.nom_sous_noeud* dans les noms de paramètres qui suivent.
Type de filtre	Type de filtre à appliquer.	**KAK_FILTER_TYPE.nom_sous_noeud** Les valeurs possibles sont les suivantes : **ALL** Tous **TAG_NAME_VALUE** Paire Nom-valeur de balise **RESOURCE_GROUP** Groupe de ressources

Tableau 17. Sous-noeud de machine virtuelle Azure Compute (suite)		
Nom du paramètre	**Description**	**Nom du paramètre de fichier de configuration en mode silencieux**
Valeur de filtre	Valeur de filtre correspondant au **type de filtre** sélectionné. Cette valeur peut être un **Groupe de ressources** ou une **paire Nom-valeur de balise**. Ne la renseignez pas si le **type de filtre** est défini sur **All**. Pour la configuration sur ligne de commande, une barre oblique inversée peut apparaître dans l'exemple affiché. Ne saisissez pas de barre oblique inversée dans la valeur que vous entrez. Exemples de paires type de filtre/valeur de filtre : • Le sous-noeud Azure Compute surveille toutes les machines virtuelles. Ne renseignez pas la valeur de filtre. Elle n'est pas nécessaire et est ignorée pour le type de filtre **All**. – Type de filtre : **All** – Valeur de filtre : • Le sous-noeud Azure Compute surveille toutes les machines virtuelles dont le nom de balise est DTAP et dotées d'une valeur de balise correspondant à la chaîne `prod`. – Type de filtre : **Paire Nom-valeur de balise** – Valeur de filtre : `DTAP:prod` • Le sous-noeud Azure Compute surveille toutes les machines virtuelles dotées d'une propriété Groupe de ressources correspondant à la chaîne `linux-group1`. – Type de filtre : **Groupe de ressources** – Valeur de filtre : `linux-group1`	**KAK_FILTER_VALUE.nom_sous_noeud**

Configuration de la surveillance de Cassandra

Vous devez configurer l'agent Cassandra pour qu'il puisse collecter les données issues des noeuds au sein du cluster afin de surveiller l'état de santé de la base de données Cassandra.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel en consultant Software Product Compatibility Reports for Cassandra agent

Pourquoi et quand exécuter cette tâche

L'agent Cassandra est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

- Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser la fenêtre IBM Cloud Application Performance Management ou le fichier de réponses silencieux.
- Pour configurer l'agent sur les systèmes Linux, vous pouvez exécuter le script et répondre aux invites, ou utiliser le fichier de réponses silencieux.

Configuration de l'agent sur des systèmes Windows

Pour pouvez utiliser la fenêtre IBM Cloud Application Performance Management pour configurer l'agent sur des systèmes Windows.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Modèle** dans la colonne **Tâche/sous-système**, puis sélectionnez **Configurer avec les valeurs par défaut**.

   La fenêtre **Monitoring Agent for Cassandra** s'ouvre.
3. Dans la zone **Enter a unique instance name**, entrez le nom d'instance de l'agent et cliquez sur **OK**.
4. Dans la fenêtre **Monitoring Agent for Cassandra**, indiquez des valeurs pour les paramètres de configuration et cliquez sur **OK**.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 220.
5. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis cliquez sur **Démarrer**.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console, voir «Démarrage de la console Cloud APM», à la page 1003.

Pour obtenir de l'aide sur le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration de l'agent sur des systèmes Linux

Pour configurer l'agent sur des systèmes d'exploitation Linux, vous pouvez exécuter le script ou répondre à des invites.

Procédure

1. Dans la ligne de commande, modifiez le chemin d'accès au répertoire d'installation de l'agent. Exemple : `/opt/ibm/apm/agent/bin`
2. Exécutez la commande suivante, où nom_instance est le nom que vous souhaitez donner à l'instance :

   `./cassandra-agent.sh config` *`nom_instance`*
3. Lorsque la ligne de commande affiche le message suivant, entrez 1 et entrez :

   `Edit 'Monitoring Agent for Cassandra' setting? [1=Yes, 2=No]`
4. A l'invite, indiquez les valeurs des paramètres de configuration.

Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 220.

5. Exécutez la commande suivante pour démarrer l'agent :

   ```
   ./cassandra-agent.sh start nom_instance
   ```

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Pour obtenir de l'aide sur le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'agent Cassandra sur les systèmes Linux and Windows. Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

1. Dans un éditeur de texte, ouvrez le fichier de configuration en mode silencieux qui est disponible à l'emplacement suivant et indiquez des valeurs pour tous les paramètres :

   Windows `rép_install\samples\cassandra_silent_config_windows.txt`
   Linux `rép_install\samples\cassandra_silent_config_UNIX.txt`

   Windows `C:\IBM\APM\samples`

   Linux `/opt/ibm/apm/agent/samples`

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 220.
2. Sur la ligne de commande, changez le chemin d'accès au `rép_install \casier`.
3. Exécutez la commande suivante :

   Windows `cassandra-agent.bat config nom_instance rép_install\samples \cassandra_silent_config_windows.txt`
   Linux `cassandra-agent.sh config nom_instance rép_install\samples \cassandra_silent_config_UNIX.txt`
4. Démarrez l'agent.

   Windows Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis sur **Démarrer**.
   Linux Exécutez la commande suivante : `./cassandra-agent.sh start nom_instance`

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Pour obtenir de l'aide sur le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Paramètres de configuration de l'agent

Lorsque vous configurez l'agent Cassandra, vous pouvez modifier la valeur par défaut des paramètres, comme Adresse IP et JMX_PORT.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de l'agent Cassandra.

Tableau 18. Noms et descriptions des paramètres de configuration

Nom du paramètre	Description	Zone obligatoire
Nom d'instance	La valeur par défaut de cette zone est identique à celle que vous indiquez dans la zone **Enter a unique instance name**.	Oui
Adresse IP	Adresse IP de n'importe quel noeud dans le cluster.	Oui
JMX_PORT	Numéro de port JMX permettant d'activer la surveillance. **Important :** Veillez à spécifier le Port JMX, le Nom d'utilisateur JMX et le mot de passe JMX dans l'ensemble du cluster. Si le noeud qui connecte l'agent au cluster ne fonctionne pas, l'agent peut collecter des données par le biais d'un autre noeud dans le cluster en utilisant les mêmes paramètres.	Oui
JMX_Username	Nom d'utilisateur permettant d'accéder à JMX.	Non
JMX_Password	Mot de passe permettant d'accéder à JMX.	Non

Configuration de la surveillance de Cisco UCS

Monitoring Agent for Cisco UCS surveille l'infrastructure virtuelle Cisco UCS en se connectant à Cisco UCSM. Vous devez configurer l'agent Cisco UCS de sorte qu'il puisse collecter les données Cisco UCS.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Cisco UCS.
- Vérifiez que l'utilisateur, qui se connecte à l'infrastructure Cisco UCS, dispose des privilèges aaa ou d'administrateur. Utilisez un utilisateur existant disposant des privilèges aaa ou d'administrateur, ou créez un nouvel ID utilisateur.
- Si l'agent Cisco UCS est configuré pour communiquer avec ses sources de données Cisco UCS qui utilisent l'agent SSL, ajoutez le certificat SSL de chaque source de données au magasin de clés de confiance de certificats de l'agent. Pour plus d'informations sur l'activation de la communication SSL avec les sources de données Cisco UCS, voir «Activation de la communication SSL avec les sources de données Cisco UCS», à la page 225.

Pourquoi et quand exécuter cette tâche

L'agent Cisco UCS est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau ci-après.

Tableau 19. Versions d'agent et documentation	
Version de l'agent Cisco UCS	**Documentation**
7.2.0.4, 7.2.0.3	IBM Cloud Application Performance Management **Remarque :** Le lien permet d'ouvrir une rubrique Knowledge Center sur site.
7.2.0.2	IBM Performance Management 8.1.3 **Remarque :** Le lien permet d'ouvrir une rubrique Knowledge Center sur site.
7.2.0.1	IBM Performance Management 8.1.2 **Remarque :** Le lien permet d'ouvrir une rubrique Knowledge Center sur site.

Les attributs de configuration définissent l'infrastructure Cisco UCS qui est surveillée. Les attributs définissent une connexion à Cisco UCSM 1.4 ou ultérieure. Vous pouvez configurer plusieurs instances de l'agent de surveillance sur un système hôte de surveillance distant. Vous pouvez également créer des instances distinctes pour surveiller une infrastructure Cisco UCS spécifique.

Une fois l'agent Cisco UCS installé, vous pouvez le démarrer. Vous devez cependant le configurer manuellement pour afficher les données de tous les attributs d'agent.

- Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser la fenêtre **IBM Performance Management** ou le fichier de réponses silencieux.
- Pour configurer l'agent sur les systèmes Linux, vous pouvez exécuter le script et répondre aux invites, ou utiliser le fichier de réponses silencieux.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent sur les systèmes d'exploitation Windows à l'aide de la fenêtre **IBM Performance Management**. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Pourquoi et quand exécuter cette tâche

L'agent Cisco UCS fournit des valeurs par défaut pour certains paramètres. Vous pouvez spécifier différentes valeurs pour ces paramètres.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **Agents IBM Monitoring** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Monitoring Agent for Cisco UCS**, puis sur **Configuration de l'agent**.

   A faire : Après avoir configuré l'agent pour la première fois, l'option **Configuration de l'agent** est désactivée. Pour reconfigurer l'agent, cliquez sur **Reconfigurer**.
3. Dans la fenêtre Monitoring Agent for Cisco UCS, procédez comme suit :
   a) Entrez un nom unique pour l'instance d'agent Cisco UCS et cliquez sur **OK**.
   b) Dans l'onglet **CONFIG**, spécifiez les valeurs des paramètres de configuration et cliquez sur **Suivant**.
   c) Dans l'onglet **LOG_CONFIG**, spécifiez les valeurs des paramètres de configuration et cliquez sur **Suivant**.

   Pour plus d'informations sur les paramètres de configuration dans chaque onglet de la fenêtre Monitoring Agent for Cisco UCS, consultez les rubriques suivantes :

- «Paramètres de configuration de l'agent», à la page 224
- «Paramètres de configuration pour le fournisseur de données», à la page 225

4. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Monitoring Agent for Cisco UCS**, puis sur **Démarrer**.

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

  Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.
- Si vous surveillez un environnement Cisco UCS de grande taille, vous devrez sans doute augmenter la taille du segment de mémoire pour le fournisseur de données Java. Pour plus d'informations, voir «Augmentation de la taille de segment de mémoire Java», à la page 226.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration de l'agent. Ce mode de configuration est appelé mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

- Pour configurer l'agent Cisco UCS en mode silencieux, procédez comme suit :
  a) Dans un éditeur de texte, ouvrez le fichier `cisco_ucs_silent_config.txt` disponible à l'emplacement suivant :
     – Linux *rép_install*`/samples/cisco_ucs_silent_config.txt`

       Exemple : `/opt/ibm/apm/agent/samples/cisco_ucs_silent_config.txt`
     – Windows *rép_install*`\samples\cisco_ucs_silent_config.txt`

       Exemple : `C:\IBM\APM\samples\cisco_ucs_silent_config.txt`
  b) Dans le fichier `cisco_ucs_silent_config.txt`, spécifiez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.

     Pour plus d'informations sur les paramètres de configuration, voir les rubriques suivantes :
     – «Paramètres de configuration de l'agent», à la page 224
     – «Paramètres de configuration pour le fournisseur de données», à la page 225
  c) Sauvegardez et fermez le fichier `cisco_ucs_silent_config.txt` et exécutez la commande suivante :
     – Linux *rép_install*`/bin/cisco_ucs-agent.sh config` *nom_instance* *rép_install*`/samples/cisco_ucs_silent_config.txt`

       Exemple : **`/opt/ibm/apm/agent/bin/cisco_ucs-agent.sh config nom_instance /opt/ibm/apm/agent/samples/cisco_ucs_silent_config.txt`**

– Windows *rép_install*\bin\cisco_ucs-agent.bat config *nom_instance* *rép_install*\samples\cisco_ucs_silent_config.txt

Exemple : **C:\IBM\APM\bin\cisco_ucs-agent.bat config nom_instance C:\IBM\APM\samples\cisco_ucs_silent_config.txt**

Où

nom_instance
Nom à attribuer à l'instance.

rép_install
Chemin d'installation de l'agent.

Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.

d) Exécutez la commande suivante pour démarrer l'agent :

– Linux *rép_install*/bin/cisco_ucs-agent.sh start *nom_instance*

Exemple : **/opt/ibm/apm/agent/bin/cisco_ucs-agent.sh start nom_instance**

– Windows *rép_install*\bin\cisco_ucs-agent.bat start *nom_instance*

Exemple : **C:\IBM\APM\bin\cisco_ucs-agent.bat start nom_instance**

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

  Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.
- Si vous surveillez un environnement Cisco UCS de grande taille, vous devrez sans doute augmenter la taille du segment de mémoire pour le fournisseur de données Java. Pour plus d'informations, voir «Augmentation de la taille de segment de mémoire Java», à la page 226.

Configuration de l'agent en répondant aux invites

Pour configurer l'agent sur des systèmes d'exploitation Linux, vous pouvez exécuter le script ou répondre à des invites.

Procédure

- Pour configurer l'agent en exécutant le script et en répondant aux invites, procédez comme suit :

  a) Sur la ligne de commande, entrez la commande suivante :

  rép_install/bin/cisco_ucs-agent.sh config *nom_instance*

  Exemple : **/opt/ibm/apm/agent/bin/cisco_ucs-agent.sh config nom_instance**

  Où

  nom_instance
  Nom à attribuer à l'instance.

  rép_install
  Chemin d'installation de l'agent.

  b) Répondez aux invites en vous référant aux rubriques suivantes :

  – «Paramètres de configuration de l'agent», à la page 224
  – «Paramètres de configuration pour le fournisseur de données», à la page 225

  c) Exécutez la commande suivante pour démarrer l'agent :

rép_install/bin/cisco_ucs-agent.sh start *nom_instance*

Exemple : **/opt/ibm/apm/agent/bin/cisco_ucs-agent.sh start nom_instance**

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

  Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.
- Si vous surveillez un environnement Cisco UCS de grande taille, vous devrez sans doute augmenter la taille du segment de mémoire pour le fournisseur de données Java. Pour plus d'informations, voir «Augmentation de la taille de segment de mémoire Java», à la page 226.

Paramètres de configuration de l'agent

Lorsque vous configurez l'agent Cisco UCS, vous pouvez modifier les valeurs par défaut des paramètres, comme le nom de l'instance et les certificats de validation SSL.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de l'agent Cisco UCS.

Tableau 20. Noms et descriptions des paramètres de configuration pour l'agent Cisco UCS

Nom du paramètre	Description	Zone obligatoire
Nom d'instance	Nom de l'instance. **Restriction :** La zone **Nom d'instance** contient le nom de l'instance que vous spécifiez lorsque vous configurez l'agent pour la première fois. Lorsque vous reconfigurez l'agent, vous ne pouvez pas modifier le nom d'instance de l'agent.	Oui
URL	Adresse URL du gestionnaire Cisco UCS. Pour définir l'adresse URL du gestionnaire Cisco UCS, entrez l'URL au format http://adresse_ip/nuova.	Oui
Nom d'utilisateur	Nom d'utilisateur administrateur du gestionnaire Cisco UCS.	Oui
Mot de passe	Mot de passe administrateur du gestionnaire Cisco UCS.	Oui
Confirmer le mot de passe	Mot de passe que vous avez entré dans la zone **Password**.	Oui
SSL truststore filepath	Chemin d'accès au fichier de clés certifiées SSL. Pour que l'agent valide les certificats SSL lors de l'utilisation de SSL pour communiquer à travers le réseau, spécifiez l'emplacement du fichier de clés certifiées SSL.	Oui

Tableau 20. Noms et descriptions des paramètres de configuration pour l'agent Cisco UCS (suite)		
Nom du paramètre	**Description**	**Zone obligatoire**
Valider les certificats SSL	Valeur booléenne qui indique si l'agent valide les certificats SSL lorsque l'agent utilise SSL pour communiquer à travers le réseau. Définissez la valeur sur Yes pour que l'agent valide les certificats SSL lorsqu'il utilise SSL pour communiquer à travers le réseau. Définissez la valeur sur No pour empêcher l'agent de valider les certificats SSL. **Conseil :** Pour plus d'informations sur l'activation de la communication SSL avec les sources de données Cisco UCS, voir «Activation de la communication SSL avec les sources de données Cisco UCS», à la page 225.	Oui

Paramètres de configuration pour le fournisseur de données

Lorsque vous configurez l'agent Cisco UCS, vous pouvez modifier les valeurs par défaut des paramètres pour le fournisseur de données, comme le nombre maximal de fichiers journaux du fournisseur de données, la taille maximale du fichier journal et le niveau de détail inclus dans le fichier journal.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration du fournisseur de données.

Tableau 21. Noms et descriptions des paramètres de configuration pour le fournisseur de données		
Nom du paramètre	**Description**	**Zone obligatoire**
Maximum number of Data Provider Log Files	Nombre maximal de fichiers journaux créés par le fournisseur de données avant qu'il remplace les anciens fichiers journaux. La valeur par défaut est 10.	Oui
Taille maximale (en ko) de chaque journal de fournisseur de données	Taille maximale en ko qu'un fichier journal de fournisseur de données doit atteindre avant que le fournisseur de données ne crée un autre fichier journal. La valeur par défaut est 5190 ko.	Oui
Niveau de détail dans le journal du fournisseur de données	Niveau de détail qui peut être inclus dans le fichier journal que le fournisseur de données crée. La valeur par défaut est INFO. Les valeurs admises sont les suivantes : OFF, SEVERE, WARNING, INFO, FINE, FINER, FINEST et ALL.	Oui

Activation de la communication SSL avec les sources de données Cisco UCS

L'agent Cisco UCS peut être configuré pour communiquer de manière sécurisée avec ses sources de données Cisco UCS via SSL. Dans cette configuration, vous devez ajouter un certificat SSL de source de données dans le magasin de clés de confiance de l'agent.

Pourquoi et quand exécuter cette tâche

Important : Les informations ci-dessous ne s'appliquent que si l'agent est configuré de manière à valider les certificats SSL.

Si la validation de certificat SSL est désactivée, l'agent Cisco UCS se connecte aux sources de données Cisco UCS même si leurs certificats SSL ont expiré, ne sont pas dignes de confiance ou ne sont pas valides. Cependant, la désactivation de la validation des certificats SSL peut poser des problèmes de sécurité et doit être effectuée avec précaution.

Si une source de données Cisco UCS utilise un certificat SSL signé par une autorité de certification commune (par exemple Verisign, Entrust ou Thawte), il n'est pas nécessaire d'ajouter des certificats au

magasin de clés de confiance de certificats de l'agent Cisco UCS. En revanche, si la source de données utilise un certificat qui n'est pas signé par une autorité de certification courante, comme c'est le cas par défaut, le certificat doit être ajouté au magasin de clés de confiance pour permettre à l'agent de se connecter et de collecter des données.

Procédure

1. Copiez le fichier de certificat de votre source de données vers l'ordinateur de l'agent.
2. Sur l'ordinateur de l'agent, placez le fichier de certificat dans le répertoire de votre choix. Evitez tout écrasement des fichiers de certificat. Utilisez pour chaque certificat ajouté un nom de fichier et un libellé uniques.
3. Utilisez la commande `keytool` pour ajouter le certificat de source de données au magasin de clés de confiance de l'agent :

   ```
   keytool -import -noprompt -trustcacerts -alias CertificateAlias -file
   CertificateFile -keystore Truststore -storepass TruststorePassword
   ```

   Où

   CertificateAlias

   Référence unique pour chaque certificat ajouté au magasin de clés de confiance de l'agent ; par exemple, *datasource* est un alias approprié pour le certificat provenant de *datasource.example.com*.

   CertificateFile
   Nom et chemin d'accès complet au fichier de certificat de source de données Cisco UCS à ajouter au magasin de clés de confiance.

   Truststore

   Nom et chemin d'accès complet au fichier de la base de données de certificats de l'agent Cisco UCS. Utilisez le chemin et le nom de fichier suivants :

   - Windows (64 bits) *rép_install*`\tmaitm6_x64\kv6.truststore`
   - Linux (64 bits) : `rép_install/lx8266/vm/etc/kv6.truststore`

   TruststorePassword

   ITMFORVE est le mot de passe par défaut du magasin de clés de confiance de l'agent Cisco UCS. Pour modifier ce mot de passe, reportez-vous à la documentation relative à l'environnement d'exécution Java pour plus d'informations sur les outils à utiliser.

   Important : Pour utiliser la commande `keytool`, le répertoire bin de l'environnement d'exécution Java doit être indiqué dans le chemin. Utilisez les commandes suivantes :

   - Windows (64 bits) : `set PATH=%PATH%;rép_install\java\java70_x64\jre\bin`
   - Linux (64 bits) : `PATH="$PATH":/opt/ibm/apm/agent/JRE/lx8266/bin`
4. Après avoir ajouté tous les certificats de source de données, démarrez l'agent de surveillance.

Augmentation de la taille de segment de mémoire Java

Après avoir configuré l'agent Cisco UCS, si vous surveillez un environnement Cisco UCS de grande taille, vous devrez sans doute augmenter la taille du segment de mémoire pour le fournisseur de données Java.

Pourquoi et quand exécuter cette tâche

La taille de segment de mémoire par défaut du fournisseur de données Java est de 256 mégaoctets. Dans les environnements Cisco de grande taille, si les problèmes suivants surviennent, il peut s'avérer nécessaire d'augmenter la taille de segment de mémoire :

- Le fournisseur de données Java s'arrête en raison d'un problème `javacore` et crée un fichier nommé `javacore.`*`date.heure.numéro`*`.txt` dans le répertoire `CANDLEHOME\tmaitm6_x64`.

- Le fichier `javacore.date.heure.numéro.txt` contient la chaîne `java/lang/OutOfMemoryError`.

Procédure

- Windows

  Pour attribuer une valeur de 1 Go à la taille de segment de mémoire, procédez comme suit :

  1. Ouvrez le fichier `%CANDLE_HOME%\TMAITM6_x64\kv6_data_provider.bat`.
  2. Ajoutez la ligne suivante avant la ligne commençant par `KV6_JVM_ARGS="$KV6_CUSTOM_JVM_ARGS...` :

     ```
     SET KV6_CUSTOM_JVM_ARGS=-Xmx1024m
     ```

  3. Redémarrez l'agent.

- Linux

  Pour attribuer une valeur de 1 Go à la taille de segment de mémoire, procédez comme suit :

  1. Ouvrez le fichier `$CANDLEHOME/lx8266/vm/bin/kv6_data_provider.sh`.
  2. Ajoutez la ligne suivante avant la ligne commençant par `KV6_JVM_ARGS="$KV6_CUSTOM_JVM_ARGS...` :

     ```
     KV6_CUSTOM_JVM_ARGS=-Xmx1024m
     ```

  3. Redémarrez l'agent.

Configuration de la surveillance de Citrix Virtual Desktop Infrastructure

L'agent Citrix VDI permet de surveiller de manière centralisée vos ressources Citrix XenDesktop ou XenApp, y compris les groupes de distribution, les catalogues, les applications, les bureaux, les utilisateurs et les sessions. Avant de pouvoir utiliser l'agent, vous devez le configurer afin de collecter les données par le biais du contrôleur de distribution.

Avant de commencer

- Les instructions figurant dans cette rubrique concernent l'édition la plus récente de l'agent, sauf indication contraire.
- Assurez-vous que votre environnement possède la configuration système requise pour l'agent Citrix VDI. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Citrix VDI.
- Vérifiez que les informations suivantes sont disponibles :
  - Nom d'hôte du contrôleur de distribution auquel vous prévoyez de vous connecter.
  - Nom d'utilisateur, mot de passe et domaine OData.
  - Nom d'utilisateur PowerShell, mot de passe, domaine, port PowerShell, type de vérification SSL et mécanisme d'authentification si vous activez l'extraction des événements du journal des événements Windows et de la métrique PowerShell.
- Assurez-vous qu'un compte utilisateur d'opérateur d'agent dispose au moins des privilèges d'administrateur en lecture seule de Citrix. Voir la rubrique sur l'activation des privilèges d'administrateur en lecture seule de Citrix.
- La fonctionnalité d'extraction du journal des événements Windows est désormais disponible depuis la version 8.1.3.1 de l'agent Citrix VDI. Pour en bénéficier depuis l'ensemble des machines Desktop Delivery Controller (DDC) et Virtual Delivery Agent (VDA), vous devez activer l'accès PowerShell à distance pour le compte utilisateur qui a été spécifié lors de la configuration de l'instance de l'agent. Pour être sûr que l'agent pourra effectuer cette fonction, procédez comme suit :

1. Connectez-vous à un ordinateur Windows en tant qu'utilisateur spécifié dans la configuration de l'instance d'agent.
2. Exécutez la commande PowerShell suivante, où *vda_system* représente le nom d'une machine VDA sous tension :
   ```
   Get-WinEvent -FilterHashtable
   @{ProviderName='Citrix*';LogName='Citrix*';StartTime=((Get-
   Date).AddDays(-10))} -ComputerName système_vda
   ```

- Assurez-vous que les stratégies d'équilibrage de charge suivantes sont activées pour l'environnement surveillé :
  - Utilisation de l'UC
  - Utilisation du disque
  - Utilisation de la mémoire

  Vous pouvez configurer ces stratégies par le biais de l'application Citrix Studio.

Pourquoi et quand exécuter cette tâche

L'agent Citrix VDI est un agent multi-instance. Vous devez créer au moins une instance et démarrer l'instance d'agent manuellement.

La configuration des serveurs XenApp est identique à celle des serveurs XenDesktop. Si un nom ou une description de paramètre de configuration ne mentionne que "XenDesktop", il s'applique également à XenApp.

Procédure

1. Configurez l'agent sur des systèmes Windows avec la fenêtre **IBM Performance Management** ou le fichier de réponses silencieux.
   - «Configuration de l'agent sur des systèmes Windows», à la page 229.
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 233.
2. Configurez l'agent sur des systèmes Linux avec le script qui génère des invites pour les réponses ou le fichier de réponses silencieux.
   - «Configuration de l'agent en répondant à des invites», à la page 232.
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 233.

Que faire ensuite

Dans la console Cloud APM, accédez à votre Tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Pour identifier et résoudre les incidents, reportez-vous au forum Cloud Application Performance Management.

Activation des privilèges d'administrateur en lecture seule de Citrix

L'agent Citrix VDI requiert que le compte utilisateur d'opérateur d'agent dispose au moins des privilèges d'administrateur en lecture seule de Citrix.

Pourquoi et quand exécuter cette tâche

Pour effectuer ces étapes à distance depuis un ordinateur sur lequel le composant logiciel enfichable Citrix Delegated Admin PowerShell est installé, utilisez le paramètre `AdminAddress`. Par exemple, la commande à l'étape 2 deviendrait :
`New-AdminAdministrator -Name "YOURDOMAIN\NewAdmin" -AdminAddress "controller1.YOURDOMAIN.com"`. Où *YOURDOMAIN* représente le nom du domaine réseau, *NewAdmin*, le compte utilisateur auquel les droits d'administration Citrix sont octroyés et *controller1.YOURDOMAIN.com*, le nom de domaine complet du serveur du site Citrix.

Procédure

1. Démarrez une session PowerShell avec un compte administrateur Citrix existant.
2. Chargez le composant logiciel enfichable Delegated Admin PowerShell pour gérer le site Citrix XenApp ou XenDesktop.

   `(Add-PSSnapin Citrix.DelegatedAdmin.Admin.V1)`
3. Ajoutez le compte utilisateur d'opérateur d'agent comme administrateur de site Citrix.

   `New-AdminAdministrator -Name "YOURDOMAIN\NewAdmin"`

   Où *YOURDOMAIN* représente le nom du domaine réseau et *NewAdmin*, le compte utilisateur auquel les droits d'administration Citrix sont octroyés.
4. Déterminez les rôles et portées disponibles à affecter à *NewAdmin*.

   ```
   Get-AdminRole
   Get-AdminScope
   ```
5. Affectez les rôles au compte utilisateur d'opérateur d'agent, notamment les droits d'administrateur en lecture seule.

   `Add-AdminRight -Administrator "YOURDOMAIN\NewAdmin" -Role "Read Only Administrator" -Scope "All"`

   Où

   - *YOURDOMAIN* représente le nom du domaine réseau.
   - *NewAdmin* représente le compte utilisateur auquel les droits d'administration Citrix sont octroyés.
   - *Read Only Administrator* représente le rôle d'administrateur de site Citrix que vous affectez.
   - *All* représente la portée d'administrateur de site Citrix que vous affectez.
6. Confirmez l'ajout et les modifications de l'administrateur.

   `Get-AdminAdministrator -Name "YOURDOMAIN\NewAdmin"`

   Où *YOURDOMAIN* représente le nom du domaine réseau et *NewAdmin*, le compte utilisateur auquel les droits d'administration Citrix sont octroyés.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent Citrix VDI sur les systèmes d'exploitation Windows dans la fenêtre IBM Cloud Application Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.

2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur le modèle **Monitoring Agent for Citrix Virtual Desktop Infrastructure**, puis cliquez sur **Configure agent**.

   A faire : Après avoir configuré une instance d'agent pour la première fois, l'option **Configure agent** est désactivée. Pour reconfigurer l'instance d'agent, cliquez dessus avec le bouton droit de la souris et sélectionnez **Reconfigure**.
3. Entrez un nom d'instance unique, puis cliquez sur **OK**. N'utilisez que des lettres, des chiffres arabes, le caractère de soulignement et le caractère moins dans le nom de l'instance. Par exemple, `vdi_inst2`.

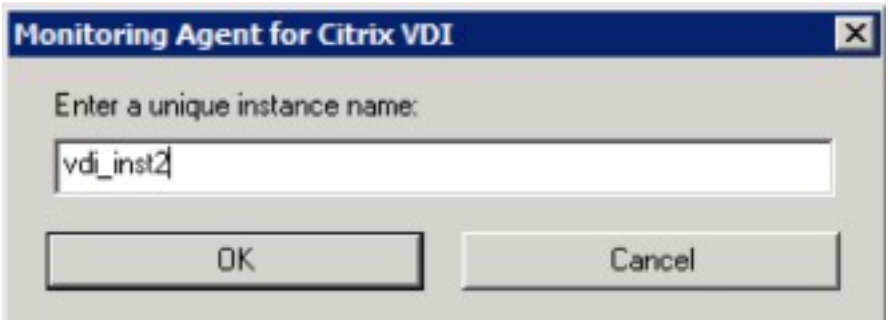


Figure 13. Fenêtre de saisie d'un nom d'instance unique.

4. Cliquez sur **Suivant** dans la fenêtre du nom d'instance de l'agent.

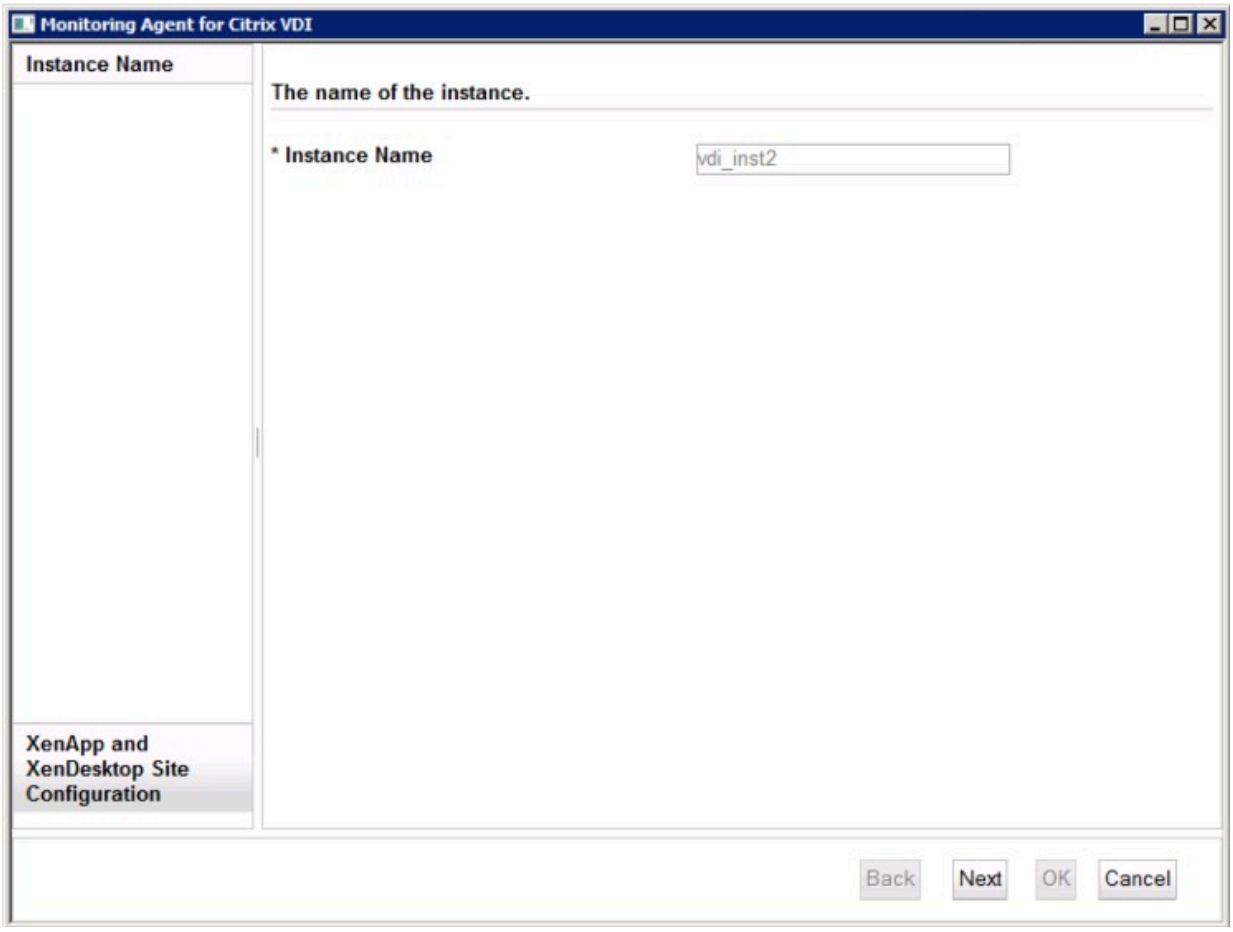


Figure 14. Fenêtre du nom d'instance de l'agent.

5. Entrez les paramètres du modèle d'instance **Configuration de site XenApp et XenDesktop**.

   Remarque : Cette section ne décrit pas la configuration de l'instance de site XenApp ou XenDesktop. Il s'agit d'un modèle de section qui permet de définir les valeurs par défaut lorsque vous ajoutez les véritables configurations d'instance de site XenApp ou XenDesktop à l'étape 6.

Pour obtenir une description de chaque paramètre de configuration, voir Tableau 22, à la page 235.

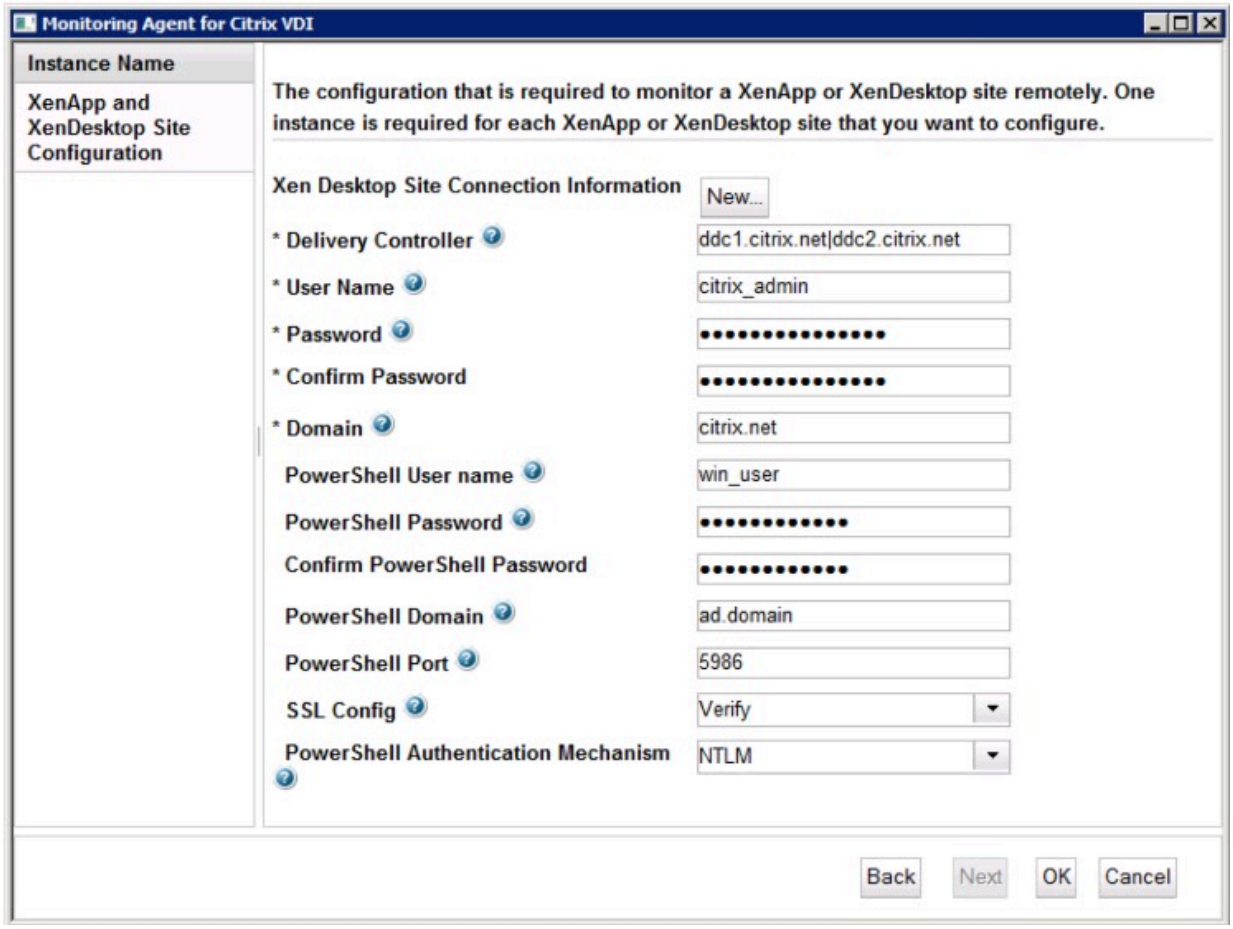


Figure 15. Fenêtre de spécification des paramètres du modèle d'instance de site XenApp ou XenDesktop

6. Appuyez sur **Nouveau** et entrez les paramètres d'instance de site XenApp ou XenDesktop, puis cliquez sur **Suivant**.

   Pour obtenir une description de chaque paramètre de configuration, voir Tableau 22, à la page 235.

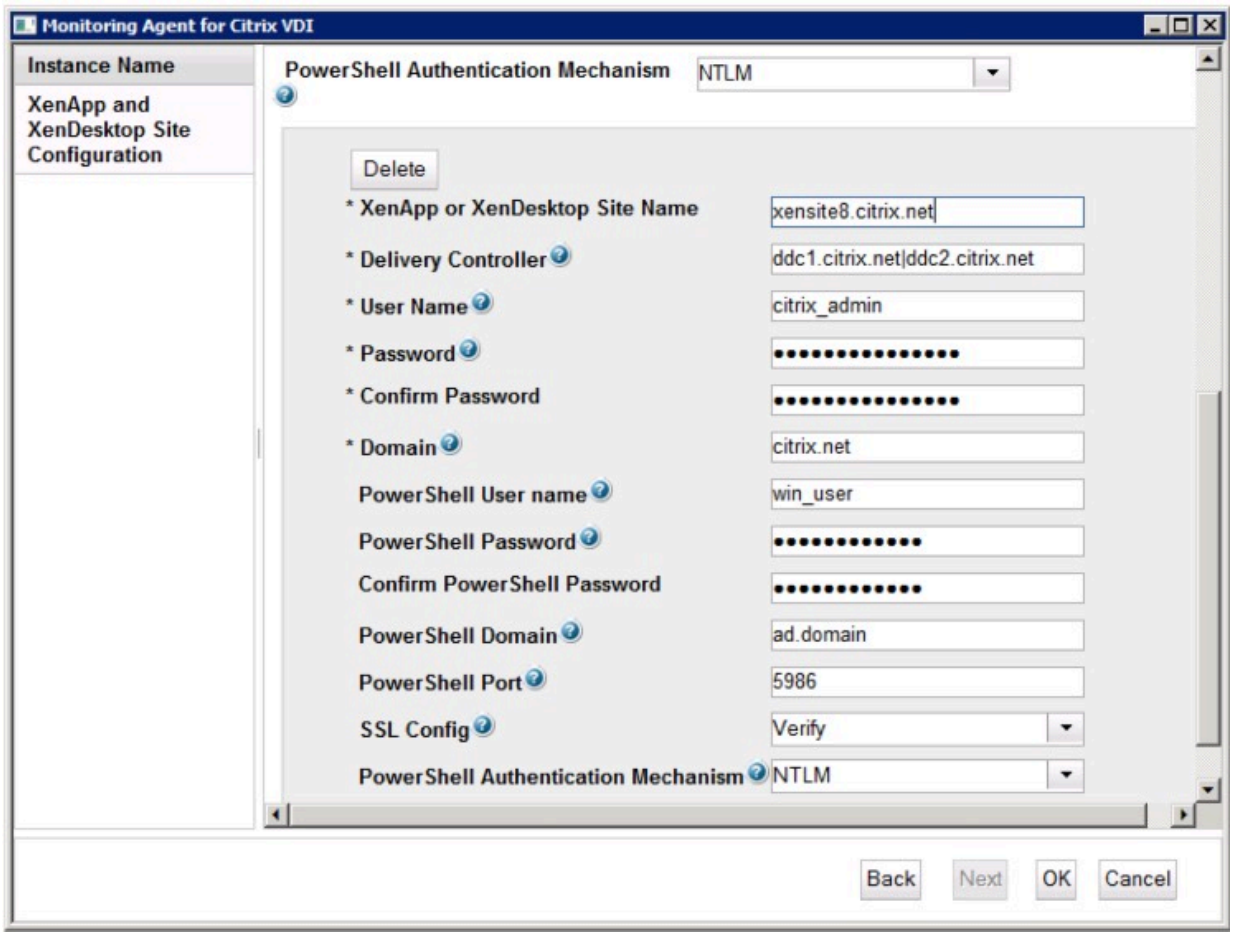


Figure 16. Fenêtre de spécification des paramètres d'instance de site XenApp ou XenDesktop

Remarque : Le paramètre **`Nom d'utilisateur PowerShell`** et tous les paramètres PowerShell ci-après ne sont requis que lors de l'«Activation de la surveillance des événements Windows et des mesures PowerShell», à la page 236. Ces variables d'environnement avancées sont désactivées par défaut en raison de la charge importante qu'elles imposent au système surveillé.

Remarque : Vérifiez que les paramètres de **`configuration SSL`** et du **`mécanisme d'authentification PowerShell`** sont définis correctement pour chaque nouvelle instance de site XenApp ou XenDesktop. Un incident entraîne la définition des valeurs par défaut et non des valeurs de modèle.

7. Cliquez sur **OK** pour terminer la configuration.
8. Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur l'instance que vous avez configurée, puis cliquez sur **Démarrer**.

Configuration de l'agent en répondant à des invites

Après avoir installé l'agent Citrix VDI, vous devez le configurer pour pouvoir le démarrer. Si l'agent Citrix VDI est installé sur une machine Linux, vous pouvez suivre ces instructions pour le configurer de manière interactive en suivant des invites de ligne de commande.

Pourquoi et quand exécuter cette tâche

A faire : Si vous reconfigurez une instance d'agent configurée, la valeur définie dans la dernière configuration s'affiche pour chaque paramètre. Pour effacer une valeur existante, appuyez sur la touche Espace lorsque le paramètre s'affiche.

Procédure

Procédez comme suit pour configurer l'agent Citrix VDI en exécutant un script et en répondant aux invites.

1. Exécutez la commande suivante :

   ```
   rép_install/bin/citrixvdi-agent.sh
   config nom_instance
   ```

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent.

   Exemple

   ```
   /opt/ibm/apm/agent/bin/citrixvdi-agent.sh config vdi_inst01
   ```

2. Répondez aux invites pour définir les valeurs de configuration de l'agent.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'agent Citrix VDI», à la page 234.

   Remarque : Le paramètre **Nom d'utilisateur PowerShell** et tous les paramètres PowerShell ci-après ne sont requis que lors de l'«Activation de la surveillance des événements Windows et des mesures PowerShell», à la page 236. Ces variables d'environnement avancées sont désactivées par défaut en raison de la charge importante qu'elles imposent au système surveillé.

3. Exécutez la commande suivante pour démarrer l'agent :

   ```
   rép_install/bin/citrixvdi-agent.sh
   start nom_instance
   ```

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

   Exemple

   ```
   /opt/ibm/apm/agent/bin/citrixvdi-agent.sh start vdi_inst01
   ```

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

- Configurez l'agent Citrix VDI en mode silencieux :
  a) Ouvrez le fichier `citrixvdi_silent_config.txt` qui se trouve dans l'un des chemins ci-après, dans un éditeur de texte.
  - Linux *rép_install*`/samples/citrixvdi_silent_config.txt`

    Par exemple, `/opt/ibm/apm/agent/samples/citrixvdi_silent_config.txt`
  - Windows *rép_install*`\samples\citrixvdi_silent_config.txt`

Par exemple, `C:\IBM\APM\samples\citrixvdi_silent_config.txt`

où *rép_install* représente le chemin d'installation de l'agent.

b) Dans le fichier `citrixvdi_silent_config.txt`, spécifiez des valeurs pour tous les paramètres obligatoires et modifiez les valeurs des autres paramètres si nécessaire.

Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'agent Citrix VDI», à la page 234.

Remarque : Le paramètre **Nom d'utilisateur PowerShell** et tous les paramètres PowerShell ci-après ne sont requis que lors de l'«Activation de la surveillance des événements Windows et des mesures PowerShell», à la page 236. Ces variables d'environnement avancées sont désactivées par défaut en raison de la charge importante qu'elles imposent au système surveillé.

c) Sauvegardez et fermez le fichier `citrixvdi_silent_config.txt`, puis exécutez la commande suivante :

– Linux *rép_install*`/bin/citrixvdi-agent.sh config` **nom_instance** *rép_install*`/samples/citrixvdi_silent_config.txt`

Par exemple, **/opt/ibm/apm/agent/bin/citrixvdi-agent.sh config vdi_inst01 /opt/ibm/apm/agent/samples/citrixvdi_silent_config.txt**

– Windows *rép_install*`\bin\citrixvdi-agent.bat config` **nom_instance** *rép_install*`\samples\citrixvdi_silent_config.txt`

Par exemple, **C:\IBM\APM\bin\citrixvdi-agent.bat config vdi_inst01 C:\IBM\APM\samples\citrixvdi_silent_config.txt**

où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent.

Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.

d) Exécutez la commande suivante pour démarrer l'agent :

– Linux *rép_install*`/bin/citrixvdi-agent.sh start` **nom_instance**

Par exemple, **/opt/ibm/apm/agent/bin/citrixvdi-agent.sh start vdi_inst01**

– Windows *rép_install*`\bin\citrixvdi-agent.bat start` **nom_instance**

Par exemple, **C:\IBM\APM\bin\citrixvdi-agent.bat start vdi_inst01**

où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

Paramètres de configuration de l'agent Citrix VDI

Les paramètres de configuration de l'agent Citrix VDI sont regroupés dans un tableau.

1. Paramètres de l'agent Citrix VDI - Paramètres d'environnement de l'agent Citrix VDI.

Tableau 22. Paramètres de l'agent Citrix VDI

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Nom du site XenApp ou XenDesktop	Indiquez un nom pour identifier l'instance d'agent du site XenApp ou XenDesktop. Par exemple, *vdi_inst2* **Remarque :** cet alias vous permet de représenter l'instance de l'agent du serveur WebLogic avec les restrictions suivantes. Seuls les lettres, les chiffres arabes, le caractère souligné et le caractère moins peuvent être utilisés dans le nom de connexion. La longueur maximale d'un nom de connexion est de 25 caractères.	Chacun des paramètres suivants doit avoir un suffixe de nom d'instance qui est le même pour chaque paramètre d'une instance d'agent. Les nouvelles instances d'agent doivent utiliser un nom d'instance unique pour son jeu de paramètres. Par exemple, une instance d'agent peut utiliser *.vdi1* et une autre instance d'agent peut utiliser *.vdi2* à la place de *.nom_instance* dans les noms de paramètres ci-après.
Contrôleur de distribution	Nom d'hôte ou adresse IP du contrôleur de distribution. Si plusieurs DDC sont configurés dans un cluster, une liste de contrôleurs de distribution séparés par un caractère '|' peut être fournie.	**KVD_XDS_DELIVERY_CONTROLLER.instance_name**
Nom d'utilisateur	Nom d'utilisateur utilisé pour s'authentifier avec l'API OData sur le contrôleur de distribution XenApp ou XenDesktop spécifié.	**KVD_XDS_ODATA_USERNAME.instance_name**
Mot de passe	Mot de passe utilisé pour s'authentifier avec l'API OData sur le contrôleur de distribution XenApp ou XenDesktop spécifié.	**KVD_XDS_ODATA_PASSWORD.instance_name**
Domaine	Domaine utilisé pour s'authentifier avec l'API OData sur le contrôleur de distribution XenApp ou XenDesktop spécifié.	**KVD_XDS_ODATA_DOMAIN.instance_name**
Nom d'utilisateur PowerShell	Nom d'utilisateur utilisé pour s'authentifier pour les appels PowerShell aux machines VDA et DDC distantes. **Remarque :** ce paramètre et tous les paramètres PowerShell ci-après ne sont requis que lors de l'«Activation de la surveillance des événements Windows et des mesures PowerShell», à la page 236. Ces variables d'environnement avancées sont désactivées par défaut en raison de la charge importante qu'elles imposent au système surveillé.	**KVD_XDS_POWERSHELL_USERNAME.instance_name**
Mot de passe PowerShell	Mot de passe associé au nom d'utilisateur PowerShell fourni.	**KVD_XDS_POWERSHELL_PASSWORD.instance_name**
Domaine PowerShell	Domaine associé au nom d'utilisateur PowerShell fourni.	**KVD_XDS_POWERSHELL_DOMAIN.instance_name**

Tableau 22. Paramètres de l'agent Citrix VDI (suite)

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Port PowerShell	Pour SSL ouvert pour être utilisé par WinRm. Les ports de connexion distants par défaut de PowerShell sont 5985 pour HTTP et 5986 pour HTTPS.	**KVD_XDS_POWERSHELL_PORT.instance_name**
Exigence SSL	Choisissez l'option SSL requise pour votre environnement.	**KVD_XDS_SSL_CONFIG.instance_name** Les valeurs possibles sont les suivantes : **KVD_XDS_SSL_CONFIG_VERIFY** Vérification **KVD_XDS_SSL_CONFIG_NOVERIFY** Pas de vérification **KVD_XDS_SSL_CONFIG_NOSSL** Pas de couche SSL
Mécanisme d'authentification PowerShell	Définit le type d'authentification utilisé pour créer des données d'identification afin d'extraire les informations de systèmes distants avec PowerShell.	**KVD_XDS_POWERSHELL_AUTH_MECH.instance_name** Les valeurs possibles sont les suivantes : **KVD_XDS_POWERSHELL_BASIC** De base **KVD_XDS_POWERSHELL_CREDSSP** CredSSP **KVD_XDS_POWERSHELL_NTLM** NTLM **KVD_XDS_POWERSHELL_DEFAULT** Valeur par défaut **KVD_XDS_POWERSHELL_DIGEST** Prétraitement **KVD_XDS_POWERSHELL_KERBEROS** Kerberos **KVD_XDS_POWERSHELL_NEGOTIATE** Négociation

Activation de la surveillance des événements Windows et des mesures PowerShell

Activez la surveillance des événements Windows et des mesures PowerShell à l'aide de cette procédure. La surveillance de ces données peut avoir un impact considérable sur les performances du système géré.

Avant de commencer

Vérifiez que les paramètres de configuration PowerShell de l'agent sont définis.

Pourquoi et quand exécuter cette tâche

Une ou plusieurs des variables d'environnement avancées ci-après doivent être activées pour que l'agent puisse surveiller les événements Windows et les mesures PowerShell.

GET_SESSION_LATENCY
Indique si le temps d'attente de la session et la durée de la boucle sont extraits à distance de la machine VDA connectée de PowerShell.

GET_VDA_MACHINE_METRICS_REMOTELY
Indique si les mesures de la machine VDA sont extraites à distance de PowerShell.

RETRIEVE_WINDOWS_EVENTS
Indique si les événements du journal des événements Windows sont extraits de PowerShell à partir des machines VDA et DDC Windows.

Procédure

1. Accédez au répertoire d'installation de l'agent Citrix VDI :
   - Linux *rép_install*/config
   - Windows *rép_install*\TMAITM6_x64

   où *rép_install* représente le chemin d'installation de l'agent.
2. Editez le fichier de configuration de l'agent Citrix VDI pour définir une ou plusieurs des variables *GET_SESSION_LATENCY*, *GET_VDA_MACHINE_METRICS_REMOTELY* et *RETRIEVE_WINDOWS_EVENTS* sur `true`.
   - Linux `vd.environment`
   - Windows KVDENV_*nom_instance*

   où *nom_instance* représente le nom de l'instance d'agent.
3. Redémarrez l'agent.

   Important : Pour que ces paramètres soient définis par défaut pour toutes les nouvelles instances d'agent, définissez-les sur `true` dans les fichiers du modèle de configuration :
   - Linux Ce paramètre a déjà été défini par défaut pour les nouvelles instances d'agent en éditant `vd.environment` à l'étape 2.
   - Windows KVDENV

Exemple

```
GET_SESSION_LATENCY=true
GET_VDA_MACHINE_METRICS_REMOTELY=true
RETRIEVE_WINDOWS_EVENTS=true
```

Configuration de la surveillance DataPower

Pour surveiller les dispositifs DataPower, vous devez effectuer certaines tâches de configuration sur vos dispositifs, puis configurer Monitoring Agent for DataPower.

Conseil : Cliquez sur APM v8: Configuring DataPower monitoring in IBM APM pour regarder une vidéo concernant le processus de configuration de base de la surveillance DataPower.

Configuration des dispositifs DataPower

Pour pouvoir configurer Monitoring Agent for DataPower, vous devez effectuer certaines tâches de configuration sur vos dispositifs.

Conseil : Pour plus d'informations sur les dispositifs DataPower pris en charge, consultez l'onglet Prerequisites sur la page des rapports de compatibilité des produits logiciels.

Vous pouvez surveiller les dispositifs DataPower à trois niveaux différents. Configurez les trois niveaux en fonction de vos besoins sur chaque dispositif DataPower que vous voulez surveiller pour afficher les données de dispositif DataPower dans la console Cloud APM.

1. Surveillance des ressources

   Pour définir des données de surveillance, telles que l'utilisation des ressources, le débit et les statistiques de connexion, activez la surveillance des ressources. Pour plus d'informations, voir «Surveillance des ressources», à la page 238.

2. Suivi des transactions de middleware

   Pour afficher des données de surveillance pour des transactions, telles que les informations détaillées, le volume et les dépendances des transactions, activez le suivi de transaction de middleware. Pour plus d'informations, voir «Suivi des transactions de middleware», à la page 239.

3. Suivi des transactions de niveau instance du dispositif DataPower

   Pour afficher les données de surveillance pour des transactions dans les topologies des instances, configurez le suivi des transactions de niveau instance du dispositif DataPower. Pour plus d'informations, voir «Suivi des transactions de niveau instance du dispositif DataPower», à la page 241.

Important : Assurez-vous que l'ID utilisateur possède les droits appropriés pour configurer le dispositif DataPower. Vous pouvez entrer `*/*/*?Access=r` dans la zone **Access profile** pour l'ID utilisateur utilisé pour configurer le dispositif DataPower. Utilisez ensuite cet ID utilisateur pour configurer le dispositif DataPower.

Exportation du certificat public
Si le profil de proxy SSL est activé sur l'interface de gestion XML du dispositif DataPower, vous devez exporter le certificat public utilisé par l'interface de gestion XML du dispositif DataPower sur la machine qui exécute l'agent DataPower.

Procédure

1. Pour télécharger le certificat cryptographique utilisé par l'interface de gestion XML du dispositif DataPower, par exemple `pubcert:///mycert.pem`, cliquez sur **Administration** > **Main** > **File Management** et enregistrez le certificat sur la machine qui exécute l'agent DataPower.
2. Lorsque vous configurez l'agent DataPower, vous avez la possibilité de spécifier la zone **SSL Proxy Profile**. Entrez le chemin d'accès absolu au certificat public.

   Remarque : Lorsque plusieurs passerelles multiprotocole sont ajoutées, vous devez répéter ces étapes.

Surveillance des ressources
Le premier niveau de surveillance disponible sur un dispositif DataPower est d'activer le contrôle des ressources, telles que la gestion SOAP, les statistiques et les taux de transaction.

L'opération dans l'interface utilisateur de DataPower Gateway décrite dans les tâches de configuration suivantes s'applique à DataPower Gateway Version 7.5.1 et antérieure. Si la version de DataPower Gateway que vous utilisez est postérieure à 7.5.1, vous pouvez cliquer sur le point d'interrogation situé dans le coin supérieur droit de l'interface utilisateur et sélectionner **WebGUI** pour revenir à la version antérieure de l'interface utilisateur. Suivez ensuite les instructions pour exécuter les tâches de configuration du dispositif DataPower.

Activation de la gestion SOAP
Si vous souhaitez que l'agent DataPower collecte des données des dispositifs DataPower, vous devez configurer l'interface de gestion XML et activer la gestion de SOAP.

Procédure

Pour activer SOAP :

1. Connectez-vous à l'interface Web du dispositif DataPower que vous souhaitez surveiller.
2. Cliquez sur **Objects** > **Device Management** > **XML Management Interface**.

   Remarque : Vérifiez que l'état administratif est activé.

3. Pour **Port Number**, indiquez le numéro de port sur lequel l'agent DataPower écoute les rapports de notification. Le numéro de port par défaut est 5550.
4. Pour **Enabled Services**, vérifiez que **SOAP Management** est sélectionné.

Activation des statistiques
Si vous souhaitez que l'agent DataPower collecte des données à partir des dispositifs DataPower, les statistiques doivent être activées.

Procédure

Pour activer les statistiques, procédez comme suit :

1. Connectez-vous à l'interface Web du dispositif DataPower que vous souhaitez surveiller.
2. Cliquez sur **Administration** > **Device** > **Statistics Settings**.
3. Activez **Statistics Settings** et cliquez sur **Apply**.

Activation du débit de transaction
Si vous souhaitez que l'agent DataPower collecte des données à partir des dispositifs DataPower, le débit de transaction doit être activé.

Procédure

Pour activer le débit de transaction, procédez comme suit :

1. Connectez-vous à l'interface Web du dispositif DataPower que vous souhaitez surveiller.
2. Sélectionnez le domaine `default`.
3. Cliquez sur **Status** > **Connection** > **Transaction Rate**.
4. Si le message **Statistics is currently disabled** s'affiche, cliquez sur **disabled** et définissez **Administrative state** sur **enabled** dans les paramètres des statistiques.
5. Si vous disposez de plusieurs domaines, cliquez sur **Show All Domains** et répétez les étapes 3-4 pour activer le débit de transaction pour tous les domaines applicables.
6. Cliquez sur **Apply**.

Suivi des transactions de middleware
Le deuxième niveau de surveillance disponible pour un dispositif DataPower consiste à afficher le suivi des transactions de middleware dans les espaces de travail.

L'opération dans l'interface utilisateur de DataPower Gateway décrite dans les tâches de configuration suivantes s'applique à DataPower Gateway Version 7.5.1 et antérieure. Si la version de DataPower Gateway que vous utilisez est postérieure à 7.5.1, vous pouvez cliquer sur le point d'interrogation situé dans le coin supérieur droit de l'interface utilisateur et sélectionner **WebGUI** pour revenir à la version antérieure de l'interface utilisateur. Suivez ensuite les instructions pour exécuter les tâches de configuration du dispositif DataPower.

Le suivi des transactions des trafics SOAP et REST par l'intermédiaire du dispositif DataPower est pris en charge. Le suivi des transactions DataPower prend en charge SOAP à l'aide des fichiers `store:///soapreq.xsl`, `store:///soaprsp.xsl` et `store:///soaperror.xsl`. Ces fichiers XSL instrumentent le proxy de service Web pour ajouter et générer des rapports sur `kd4:KD4SoapHeaderV2` dans l'enveloppe SOAP.

Outre les fichiers `soap*.xsl`, le suivi des transactions DataPower inclut également les fichiers `apm_req.xsl`, `apm_rsp.xsl` et `apm_error.xsl`, qui prennent en charge les demandes HTTP entrantes contenant `ARM_CORRELATOR: HTTP Header`, ou une enveloppe SOAP contenant `ITCAMCorrelator` ou `kd4:KD4SoapHeaderV2`. Le proxy de service Web met à jour ou définit la demande sortante de sorte à contenir `ARM_CORRELATOR: HTTP Header` et supprime les corrélateurs SOAP.

Remarque : Si des dispositifs DataPower sont ajoutés à une application métier et que le dispositif transporte le trafic pour plusieurs applications, lorsque le suivi des transactions est activé, la topologie

d'application affichée pour ces applications métier comprend les chemins vers les noeuds pour toutes les applications.

Configuration de Web Service Management
Procédez comme suit pour chaque dispositif DataPower dont vous souhaitez afficher les données de suivi.

1. Connectez-vous à l'interface Web du dispositif DataPower que vous souhaitez surveiller.
2. Sélectionnez le domaine `default`.
3. Recherchez `XML Management Interface`. Définissez les valeurs suivantes et cliquez sur **Apply**.
   - Dans l'onglet **Main**, section **Enabled services**, activez **WS-Management endpoint**
4. Recherchez `Web Services Management Agent`. Définissez les valeurs suivantes et cliquez sur **Apply**.
   - Définissez **Administrative state** sur **enabled**
   - Définissez **Capture Mode** sur **None**
   - Définissez **Buffering Mode (deprecated)** sur **Discard**
5. Configurez le proxy de service Web ou la passerelle multiprotocole comme décrit dans les rubriques suivantes.

Configuration du proxy de service Web
Procédez comme suit pour chaque proxy de service Web dont vous souhaitez afficher les données de suivi.

Procédure

1. Sélectionnez le domaine dont fait partie le proxy de service Web.
2. Dans l'onglet **Proxy Settings**, définissez les valeurs suivantes et cliquez sur **Apply** :
   - Définissez **Monitor via Web Services Management Agent** sur **on**
3. Pour signaler les fautes SOAP, désactivez le traitement d'erreur et activez la génération de rapports d'erreurs dans la console Cloud APM : dans l'onglet **Advanced Proxy Settings**, définissez **Process HTTP Errors** sur `off` et cliquez sur **Apply**.

Configuration de la passerelle multiprotocole
Procédez comme suit pour chaque passerelle multiprotocole dont vous souhaitez afficher les données de suivi des transactions.

Procédure

1. Sélectionnez le domaine dont fait partie la passerelle multiprotocole.
2. Dans l'onglet **Advanced** de la passerelle multiprotocole, définissez les valeurs suivantes et cliquez sur **Apply** :
   - Définissez **Monitor via Web Services Management Agent** sur **on**
   - Si le serveur Web utilise des redirections, définissez **Follow Redirects** sur **off**. Définissez ensuite **Rewrite Location URL** sur **on**.
3. Si vous surveillez une passerelle multiprotocole avec un type de réponse ou un type de demande défini sur `Non-XML`, vous devez définir une stratégie de passerelle multiprotocole dont les règles couvrent à la fois la direction Client to Server et Server to Client. Si la stratégie d'une passerelle multiprotocole non XML ne possède aucune règle, aucun trafic n'est capturé par l'agent Web Services Management ou par une sonde de débogage DataPower (si activée).
4. Pour propager le Code de réponse HTTP du serveur d'arrière-plan et signaler les fautes SOAP, sous l'onglet **Advanced Settings**, définissez **Process Backend Errors** sur `off` et cliquez sur **Apply**.

Suivi des transactions de niveau instance du dispositif DataPower
Le troisième niveau de surveillance disponible pour un dispositif DataPower consiste à afficher ses données dans des topologies d'instance.

L'opération dans l'interface utilisateur de DataPower Gateway décrite dans les tâches de configuration suivantes s'applique à DataPower Gateway Version 7.5.1 et antérieure. Si la version de DataPower Gateway que vous utilisez est postérieure à 7.5.1, vous pouvez cliquer sur le point d'interrogation situé dans le coin supérieur droit de l'interface utilisateur et sélectionner **WebGUI** pour revenir à la version antérieure de l'interface utilisateur. Suivez ensuite les instructions pour exécuter les tâches de configuration du dispositif DataPower.

Configuration des transformations
Procédez comme suit sur chaque dispositif DataPower que vous voulez afficher dans les topologies d'instance.

Pourquoi et quand exécuter cette tâche

Pour IBM Performance Management V8.1.2 Fix Pack 1, le suivi des transactions du trafic SOAP par l'intermédiaire du dispositif DataPower est pris en charge. Le suivi des transactions DataPower prend en charge SOAP à l'aide des fichiers `store:///soapreq.xsl`, `store:///soaprsp.xsl` et `store:///soaperror.xsl`. Ces fichiers XSL instrumentent le proxy de service Web pour ajouter et générer des rapports sur `kd4:KD4SoapHeaderV2` dans l'enveloppe SOAP.

Pour IBM Performance Management V8.1.3 et ultérieure, le suivi des transactions du trafic REST par l'intermédiaire du dispositif DataPower est également pris en charge. Outre les fichiers `soap*.xsl`, le suivi des transactions DataPower inclut également les fichiers `apm_req.xsl`, `apm_rsp.xsl` et `apm_error.xsl`, qui prennent en charge les demandes HTTP entrantes contenant `ARM_CORRELATOR: HTTP Header`, ou une enveloppe SOAP contenant `ITCAMCorrelator` ou `kd4:KD4SoapHeaderV2`. Le proxy de service Web met à jour ou définit la demande sortante de sorte à contenir `ARM_CORRELATOR: HTTP Header` et supprime les corrélateurs SOAP.

L'agent DataPower prend en charge le suivi des transactions pour le trafic SOAP via le dispositif DataPower, le trafic REST via le dispositif DataPower et le trafic entre DataPower et WebSphere MQ.

- Pour activer le suivi des transactions pour le trafic SOAP et REST via le dispositif DataPower, appliquez `apm_req.xsl`, `apm_rsp.xsl` et `apm_error.xsl`, qui prennent en charge les demandes HTTP entrantes contenant `ARM_CORRELATOR: HTTP Header`, ou une enveloppe SOAP contenant `ITCAMCorrelator` ou `kd4:KD4SoapHeaderV2`. Le proxy de service Web met à jour ou définit la demande sortante de sorte à contenir `ARM_CORRELATOR: HTTP Header` et supprime les corrélateurs SOAP.
- Pour activer le suivi des transactions entre DataPower et WebSphere MQ, en plus du trafic SOAP et REST via le dispositif DataPower, appliquez les fichiers `apm_req_MQ.xsl`, `apm_rsp_MQ.xsl` et `apm_error_MQ.xsl`. Le suivi des transactions pour le trafic SOAP et REST est également activé automatiquement après avoir appliqué ces fichiers.

Procédure

Pour suivre le trafic REST et activer le suivi des transactions entre DataPower et WebSphere MQ, procédez comme suit :

1. Téléchargez les fichiers à partir de l'emplacement suivant :
   - Pour les systèmes Linux, `/opt/ibm/apm/agent/`*`lx8266`*`/bn/bin`
   - Pour les systèmes AIX, `/opt/ibm/apm/agent/`*`aix536`*`/bn/bin`
2. Transférez les fichiers XSL vers chaque dispositif DataPower que vous voulez surveiller dans le cadre de la Pile d'intégration IBM.
3. Configurez le proxy de service Web ou la passerelle multiprotocole comme décrit dans les rubriques suivantes.
4. Configurez chaque domaine que vous voulez surveiller comme suit :
   a) Sélectionnez le domaine dans la liste déroulante de l'en-tête DataPower Gateway.

b) Dans le navigateur du panneau de configuration, sélectionnez **Objects** > **Device Management** > **Web Services Management Agent**.

c) Définissez **Buffering Mode (deprecated)** sur `Discard`.

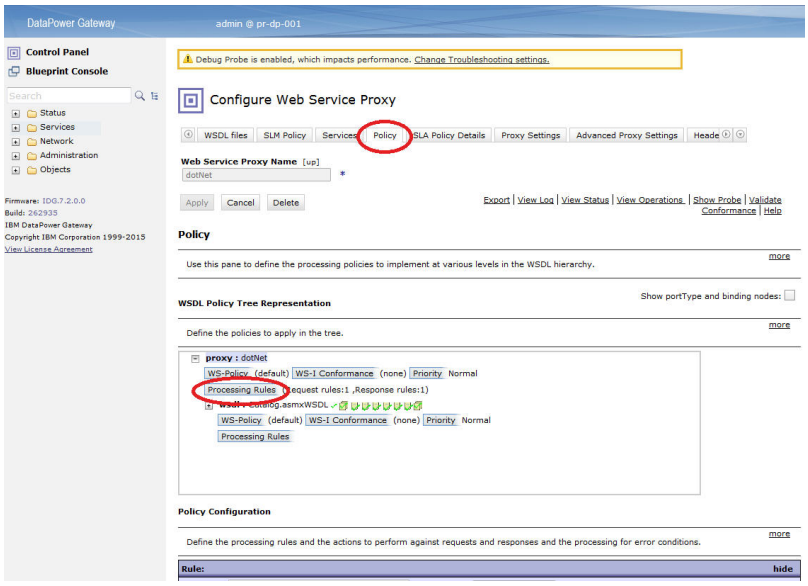
d) Cliquez sur **Appliquer**.

Configuration du proxy de service Web
Procédez comme suit sur chaque proxy de service Web que vous voulez afficher dans les topologies d'instance.

Procédure

Dans l'interface graphique Web, procédez comme suit pour chaque proxy de service Web que vous voulez surveiller :

1. Sur la page **Configure Web Service Proxy**, sélectionnez le nom du proxy de service Web à configurer.
2. Dans l'onglet **Policy**, développez **proxy : *domaine*** et cliquez sur **Processing Rules**.



3. Dans la section **Policy Configuration**, sélectionnez une règle `Client to Server` existante ou cliquez sur **New Rule** pour en créer une.

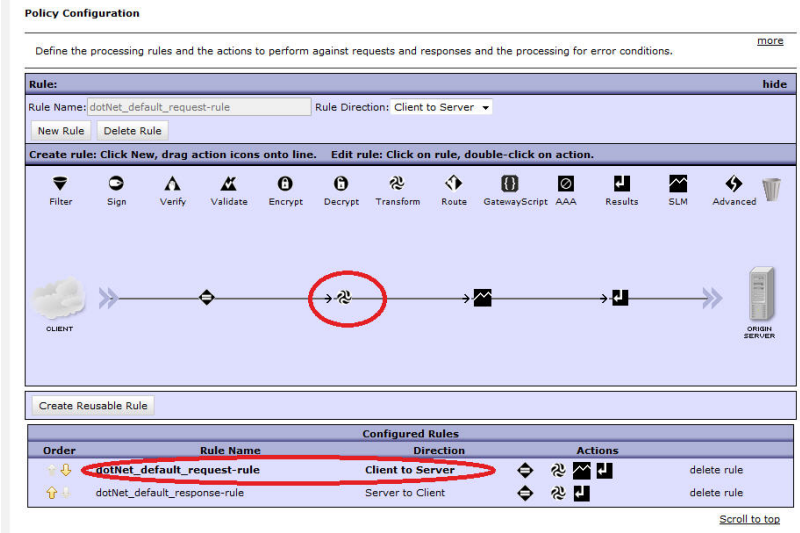
   a. Faites glisser une transformation vers le diagramme.

   Remarque :

   1) Si une règle `Client to Server` existe déjà, ajoutez-y le noeud de transformation.

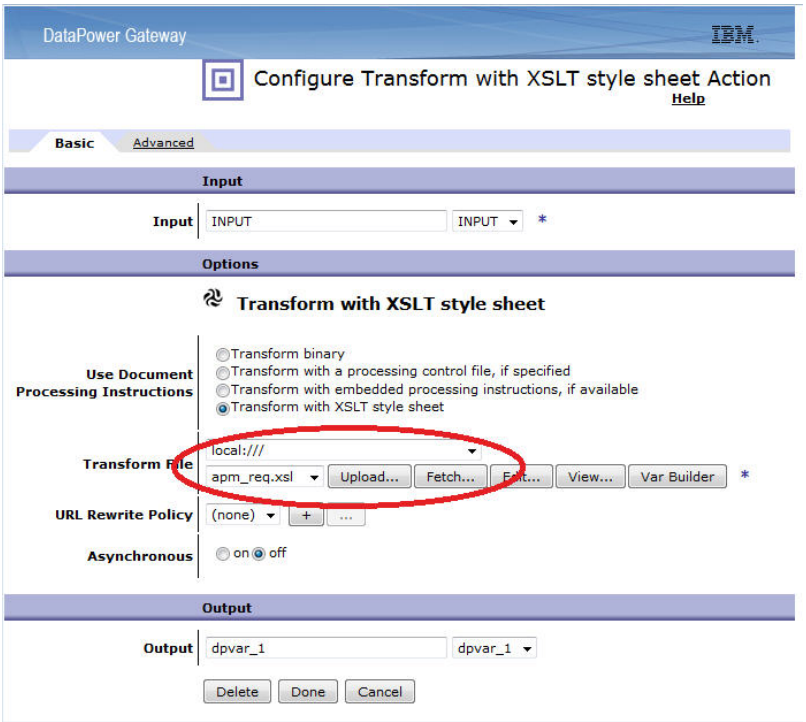
   2) Si la règle `Client to Server` a un noeud Authentification, Autorisation et Audit (AAA), veillez à ce que le noeud de transformation qui inclut le fichier xslt de l'agent DataPower précède le noeud AAA.

   b. Cliquez deux fois sur la transformation pour l'éditer.



c. Dans la fenêtre **Configure Transform with XSLT style sheet Action**, en regard du fichier de transformation, sélectionnez `apm_req.xsl` dans le magasin de données vers lequel vous l'avez transféré. Par exemple, `local:///`

Si le fichier n'existe pas, cliquez sur **Upload** pour le transférer à partir de l'emplacement installé.



Conseil : Outre la surveillance du trafic SOAP et REST via le dispositif DataPower, appliquez le fichier `apm_req_MQ.xsl` au lieu du fichier `apm_req.xsl` dans cette étape si vous souhaitez configurer une règle `Client to Server` pour surveiller le trafic entre DataPower et WebSphere MQ.

d. Cliquez sur **Terminé**.

4. Dans la section **Policy Configuration**, répétez l'étape 3 pour configurer une règle `Server to Client` ou cliquez sur **New Rule** pour en créer une.

a. Faites glisser une transformation vers le diagramme.

b. Cliquez deux fois sur la transformation pour l'éditer.

c. Dans la fenêtre **Configure Transform with XSLT style sheet Action**, en regard du fichier de transformation, sélectionnez `apm_rsp.xsl` dans le magasin de données vers lequel vous l'avez transféré. Par exemple, `local:///`

   Si le fichier n'existe pas, cliquez sur **Upload** pour le transférer à partir de l'emplacement installé.

   Conseil : Pour configurer une règle `Server to Client` afin de surveiller le trafic entre DataPower et WebSphere MQ, en plus du trafic SOAP et REST via le dispositif DataPower, appliquez le fichier `apm_rsp_MQ.xsl` à la place du fichier `apm_rsp.xsl` au cours de cette étape.

d. Cliquez sur **Terminé**.

5. Dans la section **Policy Configuration**, répétez l'étape 3 pour configurer une règle `Error` ou cliquez sur **New Rule** pour en créer une.

   a. Faites glisser une transformation vers le diagramme.

   b. Cliquez deux fois sur la règle de transformation pour l'éditer.

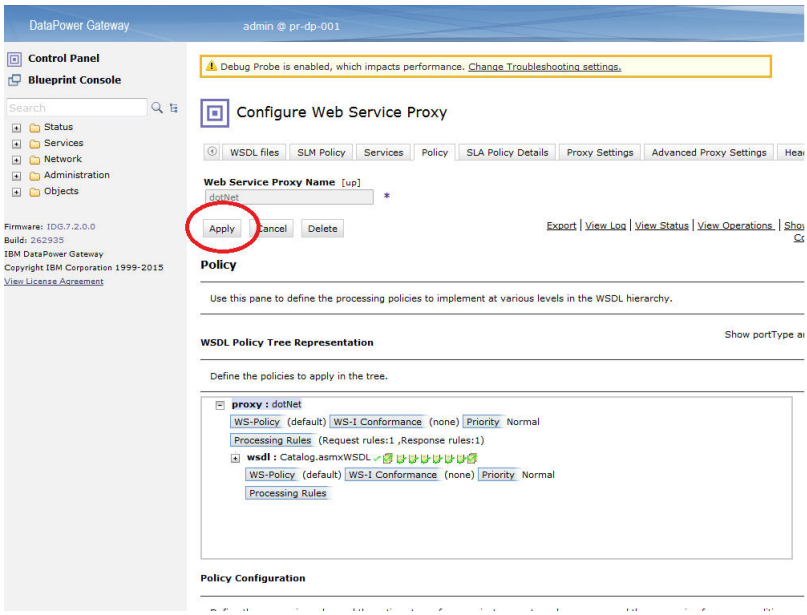
   c. Dans la fenêtre **Configure Transform with XSLT style sheet Action**, en regard du fichier de transformation, sélectionnez `apm_error.xsl` dans le magasin de données vers lequel vous l'avez transféré. Par exemple, `local:///`

   Si le fichier n'existe pas, cliquez sur **Upload** pour le transférer à partir de l'emplacement installé.

   Conseil : Pour configurer une règle `error` afin de surveiller le trafic entre DataPower et WebSphere MQ, en plus du trafic SOAP et REST via le dispositif DataPower, appliquez le fichier `apm_error_mq.xsl` à la place du fichier `apm_error.xsl` au cours de cette étape.

   d. Cliquez sur **Done**.

6. Sur la page **Configure Web Service Proxy**, cliquez sur **Appliquer**.



Configuration de la passerelle multiprotocole

Procédez comme suit sur chaque passerelle multiprotocole que vous voulez afficher dans les topologies d'instance.

Procédure

Dans l'interface graphique Web, procédez comme suit pour chaque passerelle multiprotocole que vous voulez surveiller.

1. Sur la page **Configure Multi-Protocol Gateway**, cliquez sur le nom de la passerelle multiprotocole que vous voulez configurer.
2. Sur la page **Multi-Protocol Gateway Policy**, configurez la règle. Cliquez sur **...**.

3. Sur la page **Configure Multi-Protocol Gateway Style Policy**, sélectionnez une règle `Client to Server` existante ou cliquez sur **New Rule** pour en créer une.
   a. Faites glisser une transformation vers le diagramme.

      Remarque :

      1) Si une règle `Client to Server` existe déjà, ajoutez-y le noeud de transformation.
      2) Si la règle `Client to Server` a un noeud Authentification, Autorisation et Audit (AAA), veillez à ce que le noeud de transformation qui inclut le fichier xslt de l'agent DataPower précède le noeud AAA.

   b. Cliquez deux fois sur la règle de transformation pour l'éditer.
   c. Dans la fenêtre **Configure Transform with XSLT style sheet Action**, en regard du fichier de transformation, sélectionnez `apm_req.xsl` dans le magasin de données vers lequel vous l'avez transféré. Par exemple, `local:///`

      Si le fichier n'existe pas, cliquez sur **Upload** pour le transférer à partir de l'emplacement installé.

      Conseil : Pour configurer une règle `Client to Server` afin de surveiller le trafic entre DataPower et WebSphere MQ, en plus du trafic SOAP et REST via le dispositif DataPower, appliquez le fichier `apm_req_MQ.xsl` à la place du fichier `apm_req.xsl` au cours de cette étape.
   d. Cliquez sur **Terminé**.
4. Sur la page **Configure Multi-Protocol Gateway Style Policy**, sélectionnez une règle `Server to Client` existante ou cliquez sur **New Rule** pour en créer une.
   a. Faites glisser une transformation vers le diagramme.
   b. Cliquez deux fois sur la règle de transformation pour l'éditer.
   c. Dans la fenêtre **Configure Transform with XSLT style sheet Action**, en regard du fichier de transformation, sélectionnez `apm_rsp.xsl` dans le magasin de données vers lequel vous l'avez transféré. Par exemple, `local:///`

      Si le fichier n'existe pas, cliquez sur **Upload** pour le transférer à partir de l'emplacement installé.

      Conseil : Pour configurer une règle `Server to Client` afin de surveiller le trafic entre DataPower et WebSphere MQ, en plus du trafic SOAP et REST via le dispositif DataPower, appliquez le fichier `apm_rsp_MQ.xsl` à la place du fichier `apm_rsp.xsl` au cours de cette étape.
   d. Cliquez sur **Terminé**.
5. Sur la page **Configure Multi-Protocol Gateway Style Policy**, sélectionnez une règle `Error` existante ou cliquez sur **New Rule** pour en créer une.
   a. Faites glisser une transformation vers le diagramme.
   b. Cliquez deux fois sur la règle de transformation pour l'éditer.
   c. Dans la fenêtre **Configure Transform with XSLT style sheet Action**, en regard du fichier de transformation, sélectionnez `apm_error.xsl` dans le magasin de données vers lequel vous l'avez transféré. Par exemple, `local:///`

      Si le fichier n'existe pas, cliquez sur **Upload** pour le transférer à partir de l'emplacement installé.

      Conseil : Pour configurer une règle `error` afin de surveiller le trafic entre DataPower et WebSphere MQ, en plus du trafic SOAP et REST via le dispositif DataPower, appliquez le fichier `apm_error_mq.xsl` à la place du fichier `apm_error.xsl` au cours de cette étape.
   d. Cliquez sur **Terminé**.
6. Sur la page **Configure Multi-Protocol Gateway Style Policy**, dans l'onglet **Advanced**, définissez **Monitor via Web Services Management Agent** sur **on** et cliquez sur **Apply**.
7. Cliquez sur **Apply**.

Que faire ensuite

Dans certains cas, l'ajout de transformations au Suivi des transactions amène DataPower à modifier la valeur des en-têtes Content-Type HTTP. De ce fait, vous pouvez voir des pages Web avec des images qui ne se chargent pas ou des fichiers binaires qui s'affichent avec du texte HTML déformé.

Le comportement de DataPower change lorsqu'il compare une règle ne comportant pas de transformations XSL à une règle comportant une ou plusieurs transformations XSL. Si le service traite des messages codés en MIME, MTOM, XOP ou autre, ce comportement peut être souhaité. Sinon, modifiez votre configuration DataPower en conséquence afin d'éviter ce comportement.

Pour empêcher DataPower de modifier l'en-tête Content-Type HTTP, définissez la variable dans chaque règle affectée (var://service/mpgw/proxy-content-type):

1. Faites glisser un objet avancé vers la règle.
2. Cliquez deux fois sur l'objet avancé pour l'éditer.
3. Sélectionnez **Définir variable** et cliquez sur **Suivant**.
4. Entrez le nom de variable `service/mpgw/proxy-content-type` et la valeur de variable `1`, puis cliquez sur **Terminé**.
5. Appliquez les modifications apportées à la configuration de service et de règle.
6. Répétez les étapes 1 à 5 pour chaque règle affectée.

Configuration de l'agent DataPower

Monitoring Agent for DataPower permet de surveiller de manière centralisée les dispositifs DataPower dans votre environnement d'entreprise. Il permet d'identifier et de recevoir des notifications sur les problèmes courants liés aux dispositifs. L'agent fournit également des informations sur les performances, les ressources et la charge de travail des dispositifs.

Pourquoi et quand exécuter cette tâche

L'agent DataPower est un agent à plusieurs instances ; vous devez créer la première et lancer l'agent manuellement. Le nom de système géré inclut le nom d'instance que vous spécifiez, *nom_instance*`:`*nom_hôte*`:`*pc* par exemple, où *cp* est le code produit à deux caractères. Il est limité à 32 caractères.

Le nom d'instance que vous entrez est limité à 28 caractères, moins la longueur de votre nom d'hôte. Par exemple, si vous spécifiez `DataPower` comme nom d'instance, votre nom de système géré est `DataPower:hostname:BN`.

Important : Si vous indiquez un nom d'instance long, le nom du système géré est tronqué et le code d'agent ne s'affiche pas correctement.

Remarque : Le langage XSLT de l'agent DataPower n'analyse pas les caractères BLOB utilisés pour les applications.

Pour chaque dispositif DataPower de production, configurez une instance. Si vos dispositifs DataPower ne sont pas utilisés en production ou qu'ils sont petits, vous ne pouvez configurer qu'une instance d'agent pour les surveiller. Vous pouvez exécuter plusieurs instances sur la même machine. Vous pouvez exécuter le script de configuration pour créer une instance et modifier n'importe quels paramètres de configuration. Vous pouvez éditer le fichier de réponses silencieux de l'agent avant d'exécuter le script afin d'éviter les invites et les réponses qui sont requises.

Procédure

- Pour configurer l'agent DataPower, suivez l'une des procédures ci-dessous :
  - Linux AIX Pour configurer l'agent en répondant à des invites, procédez comme suit :
    1. Accédez au répertoire *rép_install*`/bin`, où *rép_install* correspond au répertoire d'installation de l'agent DataPower.
    2. Exécutez la commande `./datapower-agent.sh config` *nom_instance*.

Sélectionnez un *nom_instance* unique sur le serveur.

3. A l'invite d'édiction des paramètres de l'agent DataPower, entrez 1 pour continuer.
4. A l'invite d'édition des **informations sur le système géré**, entrez l'une des options suivantes :

   - 1=Add
   - 2=Edit
   - 3=Del
   - 4=Next
   - 5=Exit

   Si vous configurez une instance d'agent DataPower pour la première fois sur votre système, le message `No 'DataPower Appliances' settings available` s'affiche. Entrez 1 pour ajouter un paramètre DataPower Appliances. L'option par défaut est `5=Exit`.
5. Entrez les propriétés du dispositif DataPower :

   Nom du système géré
   Entrez le nom du système géré de l'agent dans **Nom du système géré**.

   Sélectionnez un **Nom de système géré** unique pour toutes les instances de l'agent et permettant d'identifier facilement un dispositif. Ce nom ne doit contenir que des caractères alphanumériques, par exemple, le nom d'hôte du dispositif DataPower.

   Hôte de périphérique
   Dans la zone **Hôte de périphérique**, entrez l'adresse IP du dispositif DataPower surveillé. L'adresse IP par défaut est *9.123.109.139*.

   Port d'interface de gestion XML
   Pour **Port d'interface de gestion XML**, entrez le numéro de port de l'interface de gestion XML. Le numéro par défaut est 5550.

   ID utilisateur
   Pour **ID utilisateur**, entrez l'ID utilisateur de connexion au dispositif DataPower surveillé. La valeur par défaut est admin.

   Mot de passe
   Pour **Mot de passe**, entrez le mot de passe de connexion au dispositif DataPower surveillé, puis confirmez le mot de passe.

   Profil de proxy SSL
   Pour **Profil de proxy SSL**, entrez le chemin d'accès absolu du certificat public de votre profil de proxy SSL si l'interface de gestion XML du périphérique est configurée pour utiliser le profil. Par exemple,

   ```
   l'emplacement du fichier .pem exporté à partir des dispositifs Datapower/mycert.pem
   ```

   où *l'emplacement du fichier .pem exporté à partir des dispositifs Datapower* correspond au chemin d'accès absolu du certificat public. Pour exporter le certificat public, voir Exportation du certificat public.

   Option de proxy SSL
   Définissez l'**option de proxy SSL** sur `Yes` si l'interface de gestion XML du dispositif surveillé est configurée pour utiliser un profil de proxy SSL personnalisé. Sinon, définissez-la sur `No`.
6. Pour surveiller plusieurs dispositifs DataPower, répétez les étapes «4», à la page 247 et «5», à la page 247 pour configurer une instance d'agent pour chaque dispositif DataPower. Sinon, tapez 5 et appuyez sur **Entrée** pour terminer la configuration.
7. Exécutez la commande suivante pour démarrer l'agent :

   ```
   ./datapower-agent.sh start nom_instance
   ```

- Configuration en mode silencieux

  1. Pour configurer l'agent en éditant le fichier de réponses silencieux et en exécutant le script sans intervenir, procédez comme suit :

     - Linux AIX Ouvrez *rép_install*/samples/datapower_silent_config.txt dans un éditeur de texte.
     - Windows Ouvrez *rép_install*/samples/datapower_silent_config.txt dans un éditeur de texte.

  2. Pour configurer l'agent DataPower de sorte qu'il surveille un dispositif, entrez les propriétés suivantes :

     Hôte de périphérique
     Entrez le nom d'hôte ou l'adresse IP du périphérique. Par exemple, **SOAP_HOST.ManageSystemName=** *datapower01*.

     Port d'interface de gestion XML
     Entrez le numéro de port de l'interface de gestion XML. Valeur par défaut : 5550. Par exemple, **DP_PORT.ManageSystemName=** *5550*.

     ID utilisateur
     Entrez l'ID utilisateur de connexion au périphérique. La valeur par défaut est admin. Par exemple, **DP_UID.ManageSystemName=** *admin*.

     Mot de passe
     Entrez le mot de passe de l'ID utilisateur. Par exemple, **DP_PASSWORD.ManageSystemName=** *mot de passe*.

     Profil de proxy SSL
     Entrez le chemin d'accès absolu du certificat public de votre profil de proxy SSL si l'interface de gestion XML du périphérique est configurée pour utiliser le profil. Par exemple,

     ```
     l'emplacement du fichier .pem exporté à partir des dispositifs Datapower/mycert.pem
     ```

     où *l'emplacement du fichier .pem exporté à partir des dispositifs Datapower* correspond au chemin d'accès absolu du certificat public. Pour exporter le certificat public, voir Exportation du certificat public.

     Option de proxy SSL
     Définissez l'**option de proxy SSL** sur Yes si l'interface de gestion XML du dispositif surveillé est configurée pour utiliser un profil de proxy SSL personnalisé. Sinon, configurez-la sur No. Par exemple : **DP_SSL_OPTION.ManageSystemName1=** Yes.

     Important : ManageSystemName est unique. Vous devez le remplacer par votre propre nom de système dans toutes les entrées. Pour surveiller plusieurs dispositifs, copiez et répétez les étapes affichées pour surveiller un dispositif. Veillez à définir les paramètres appropriés pour les dispositifs ManageSystemName et DataPower.

  3. Accédez au répertoire d'installation de l'agent et exécutez la commande suivante pour démarrer l'agent :

     ```
     ./datapower-agent.sh start nom_instance
     ```

Que faire ensuite

- Pour vérifier les noms et les paramètres des instances d'agent configurées, lancez la commande **./cinfo -s bn**.
- Vous pouvez vérifier que les données de l'agent DataPower sont affichées dans la console Cloud APM. Pour obtenir des instructions de démarrage de la console Cloud APM, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.

- Pour afficher les données de suivi des transactions dans la console Cloud APM, configurez le suivi des transactions pour l'agent DataPower. Pour plus d'informations, voir Configuration du suivi des transactions pour l'agent DataPower.
- Pour afficher la surveillance à différents niveaux, configurez le dispositif DataPower en conséquence. Pour les instructions, voir Surveillance des ressources, Suivi des transactions de middleware et Suivi des transactions de niveau instance des dispositifs DataPower.

Configuration du suivi des transactions pour l'agent DataPower
Pour afficher les données de suivi des transactions pour les dispositifs DataPower dans les tableaux de bord de topologie et du middleware, vous devez activer le suivi des transactions pour l'agent DataPower.

Avant de commencer

- Installez l'agent DataPower et configurez-le pour qu'il se connecte au dispositif DataPower.
- Activez la surveillance pour SOAP ou ARM sur le dispositif DataPower.

Procédure

Pour activer le suivi des transactions pour l'agent DataPower, procédez comme suit :

1. Dans la barre de navigation, cliquez sur **Configuration système** > **Configuration d'agent**.
2. Dans l'onglet **DataPower**, sélectionnez les instances d'agent pour lesquelles vous voulez activer le suivi des transactions.
3. Sélectionnez **Actions** > **Set Transaction Tracking** > **Enabled** pour activer le suivi des transactions. Le statut de l'agent dans la colonne **Transaction Tracking** est mis à jour sur **Enabled**.

Résultats
Vous venez d'activer le suivi des transactions pour les instances d'agent sélectionnées.

Que faire ensuite
Pour afficher les données d'un dispositif DataPower dans les tableaux de bord du middleware et de la topologie, vous devez à présent ajouter les dispositifs à surveiller au tableau de bord d'Application Performance. Pour plus d'informations sur l'ajout d'un dispositif DataPower au Tableau de bord d'Application Performance , voir «Ajout d'applications middleware au Tableau de bord d'Application Performance », à la page 100.

Remarque : Si vous utilisez Integration Services et souhaitez surveiller les données transmises entre IBM Integration Bus et DataPower, des étapes de configuration supplémentaires sont requises pour pouvoir afficher un widget Agréger une topologie de transaction exact. L'agent IBM Integration Bus ne peut pas inclure la prise en charge de la corrélation pour les messages SOAP sans enveloppe SOAP. Les noeuds `SOAPRequest`, `SOAPAsyncRequest` et `SOAPReply` peuvent accepter des messages sans enveloppe SOAP sous la forme de messages d'entrée. Pour ces noeuds, la vue de topologie n'affiche aucune relation de la médiation vers la médiation aval ou le serveur d'applications. Pour éviter ce problème, insérez un noeud `SOAPEnvelope` immédiatement avant les noeuds `SOAPRequest`, `SOAPAsyncRequest` ou `SOAPReply` dans votre flux de messages IBM Integration Bus et sélectionnez l'option **Create new envelope** pour le noeud `SOAPEnvelope` pour ajouter une enveloppe SOAP pour le message SOAP.

Configuration de la surveillance de Db2

Monitoring Agent for Db2 surveille la disponibilité et les performances du serveur Db2. Vous pouvez surveiller plusieurs serveurs à partir de la console Cloud APM ; chaque serveur est surveillé par une instance agent Db2. La surveillance à distance est également prise en charge par l'agent Db2.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Db2.

Pourquoi et quand exécuter cette tâche

L'agent Db2 est un agent à instances multiples. Vous devez commencer par créer l'instance, puis démarrer l'agent manuellement.

Le nom de système géré inclut le nom d'instance d'agent que vous spécifiez, par exemple, *nom_instance*:*nom_hôte*:*cp*.

Où :

- *pc* désigne le code produit à deux caractères.
- *nom_instance* est le nom d'instance d'agent, et doit être identique au nom d'instance Db2 à surveiller.

Le nom de système géré peut contenir jusqu'à 32 caractères. Le nom d'instance d'agent que vous entrez admet jusqu'à 8 caractères, sans compter la longueur de votre nom d'hôte. Par exemple, si vous indiquez `DB2inst1` comme nom d'instance d'agent, le nom du système géré est `DB2inst1:hostname:ud`.

Important : Si vous indiquez un nom d'instance d'agent long, le nom du système géré est tronqué et le code d'agent ne s'affiche pas complètement.

Afin d'éviter tout problème de droits lorsque vous configurez l'agent, veillez à utiliser le même ID d'utilisateur superutilisateur ou non superutilisateur que celui utilisé pour installer l'agent. Si vous avez installé votre agent en tant qu'un utilisateur sélectionné et que vous souhaitez configurer l'agent en tant qu'un autre utilisateur, consultez «Configuration des agents en tant qu'utilisateur non superutilisateur», à la page 188. Si vous avez installé et configuré votre agent en tant qu'utilisateur sélectionné et que vous voulez démarrer l'agent en tant qu'un autre utilisateur, voir «Démarrage des agents en tant qu'utilisateur non superutilisateur», à la page 1042.

Exécutez le script de configuration pour créer une instance et changer les paramètres de configuration. Vous pouvez éditer le fichier de réponses silencieux Db2 avant d'exécuter le script de configuration afin d'éviter l'affichage des invites et la saisie des réponses qui sont normalement nécessaires.

Après avoir configuré l'agent Db2, veillez à démarrer l'agent avec un ID utilisateur doté du droit Db2 SYSADM sur l'instance surveillée. L'agent doit disposer des droits d'accès SYSADM pour activer tous les inverseurs logiques du moniteur. Par conséquent, il est nécessaire que l'agent soit démarré par un agent disposant des droits d'accès SYSADM. Utilisez l'utilisateur propriétaire de l'instance, qui détient les droits d'accès SYSADM, pour démarrer l'agent.

Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Procédure

Pour configurer l'agent avec les paramètres par défaut, procédez comme suit :

1. Exécutez la commande suivante, où *nom_instance* correspond au nom que vous souhaitez attribuer à l'instance :

   ```
   rép_install/bin/db2-agent.sh config nom_instance
    rép_install/samples/db2_silent_config.txt
   ```

   Le nom d'instance d'agent *nom_instance* est toujours identique au nom d'instance Db2 surveillé. Pour plus de détails sur les instances d'agent existantes, voir «Page Configuration d'agent», à la page 187
2. Exécutez la commande suivante pour démarrer l'agent Db2 :

   ```
   rép_install/bin/db2-agent.sh start nom_instance
   ```

Que faire ensuite

- Accordez à l'utilisateur Db2 les privilèges lui permettant d'afficher les données relatives à certains attributs de Db2. Pour plus d'informations sur l'octroi de ces privilèges, voir «Octroi de privilèges pour l'affichage des mesures Db2», à la page 255.
- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de l'agent sur des systèmes Windows

Vous pouvez utiliser la fenêtre IBM Cloud Application Performance Management pour configurer l'agent sur des systèmes Windows.

Avant de commencer

Avant de commencer à configurer l'agent Db2 pour la surveillance en local et à distance, veillez à réaliser la tâche suivante pour la surveillance à distance.

- Configuration de l'environnement client/serveur pour la surveillance à distance ; voir «Prérequis pour la surveillance à distance», à la page 259.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur **Monitoring Agent for DB2**, puis cliquez sur **Configuration de l'agent**.
3. Dans la zone **Enter a unique instance name**, entrez le nom d'instance de l'agent et cliquez sur **OK**.

   Important : Pour la surveillance en local, le nom de l'instance d'agent doit être celui de l'instance Db2 actuellement surveillée.

   Pour la surveillance à distance, le nom de l'instance d'agent doit être le nom unique du noeud catalogue.
4. Dans la fenêtre **Monitoring Agent for DB2**, procédez comme suit :
   a) Dans la zone **Username**, entrez le nom d'utilisateur de l'instance Db2.

      Pour Db2 en local, entrez le nom du propriétaire d'instance Db2.

      Pour Db2 à distance, entrez le nom réel du propriétaire d'instance Db2 sur la machine Db2 distante.

      Important : Ce paramètre est obligatoire pour la surveillance de l'instance Db2 distante.

   b) Dans la zone **Password**, entrez le mot de passe de l'instance Db2.

      Pour Db2 en local, entrez le mot de passe du propriétaire d'instance Db2.

      Pour Db2 à distance, entrez le mot de passe réel du propriétaire d'instance Db2 sur la machine Db2 distante.

      Important : Ce paramètre est obligatoire pour la surveillance de l'instance Db2 distante.

   c) Dans la zone **DB2Customized SQL Definition File**, entrez le chemin de fichier complet du fichier de définition SQL. Si le fichier de définition SQL se trouve le répertoire par défaut, laissez cette zone vide. Sinon, entrez le chemin complet du fichier. Le nom de fichier par défaut avec le chemin d'accès est le suivant :

      Linux AIX `CANDLEHOME/config/kudcussql.properties`

      Windows `CANDLEHOME\TMAITM6_x64\kudcussql.properties`

   d) Dans la zone **db2diag Log File Path**, entrez le chemin de répertoire du fichier journal db2diag. Si le fichier journal db2diag se trouve le répertoire par défaut, laissez cette zone vide. Sinon, indiquez le chemin d'accès du répertoire. Le chemin du répertoire par défaut est le suivant :

Linux AIX /home/*rép_base_propriétaireDB2*/sqllib/db2dump

Windows C:\ProgramData\IBM\DB2\DB2COPY*NOMINSTANCEDB2*

Remarque : Ce paramètre n'est pas applicable à la surveillance à distance.

e) Dans la zone **MSGID Filter in Regular Expression**, entrez *MSGID* pour filtrer le journal de diagnostic. MSGID est une combinaison du type de message, du numéro de message et du niveau de gravité. Utilisez une expression régulière pour filtrer le journal en fonction du type de message, du numéro de message, ou du niveau de gravité, par exemple, `ADM1\d*1E|ADM222\d2W`.

f) Dans la liste **Enable Monitoring for Partitions in Remote Hosts**, sélectionnez `Yes` pour indiquer que l'agent Db2 peut surveiller des partitions sur des hôtes distants.

g) Dans la liste **Enable Monitoring All Databases**, sélectionnez `Yes` pour indiquer que l'agent Db2 peut surveiller toutes les bases de données.

h) Cliquez sur **OK**.

L'instance de l'agent est affichée dans la fenêtre IBM Cloud Application Performance Management.

5. Procédez comme suit pour configurer la surveillance à distance.
   a) Ouvrez *rép_install*`\TMAITM6_x64\KUDENV_<nom_instance>`.
   b) Définissez *KUD_DB2_CLIENT_INST* sur le nom de l'instance client Db2 sous lequel l'instance du serveur Db2 distante est cataloguée.
6. Cliquez avec le bouton droit de la souris sur l'instance **Monitoring Agent for DB2**, puis cliquez sur **Démarrer**.

Que faire ensuite

- Accordez à l'utilisateur Db2 les privilèges lui permettant d'afficher les données relatives à certains attributs de l'agent Db2. Pour plus d'informations sur l'octroi de ces privilèges, voir «Octroi de privilèges pour l'affichage des mesures Db2», à la page 255.
- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de l'agent sur des systèmes Linux ou UNIX

Exécutez le script de configuration pour configurer l'agent sur les systèmes Linux.

Avant de commencer

Avant de commencer à configurer l'agent Db2 pour la surveillance en local et à distance, veillez à réaliser la tâche suivante pour la surveillance à distance.

- Configuration de l'environnement client/serveur pour la surveillance à distance ; voir «Prérequis pour la surveillance à distance», à la page 259.

Procédure

1. Exécutez la commande *rép_install*`/bin/db2-agent.sh config` *nom_instance*

   Où *nom_instance* est le nom à attribuer à l'instance :

   Important : Pour la surveillance en local, le nom de l'instance d'agent doit être celui de l'instance Db2 actuellement surveillée.

   Pour la surveillance à distance, il s'agit du noeud catalogué local de l'instance du serveur Db2 distante à surveiller.
2. Lorsque vous êtes invité à saisir une valeur pour les paramètres suivants, appuyez sur Entrée pour accepter la valeur par défaut ou spécifiez une valeur et appuyez sur Entrée :
   - Username
   - Password

- DB2 SQL path
- Diaglog path
- Diaglog message ID filter
- Monitor remote partitions
- Monitor all databases

3. Exécutez la commande suivante pour démarrer l'agent :

   Pour la surveillance en local, exécutez *rép_install*/bin/db2-agent.sh start *nom_instance* en tant que propriétaire de l'instance Db2.

   Pour la surveillance à distance, exécutez *rép_install*/bin/db2-agent.sh start *nom_noeud* en tant que propriétaire de l'instance client Db2 sous lequel l'instance du serveur Db2 distante est cataloguée.

Que faire ensuite

- Accordez à l'utilisateur Db2 les privilèges lui permettant d'afficher les données relatives à certains attributs de l'agent Db2. Pour plus d'informations sur l'octroi de ces privilèges, voir «Octroi de privilèges pour l'affichage des mesures Db2», à la page 255.
- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Utilisez le fichier de réponses silencieux pour configurer l'agent sans répondre aux invites quand vous exécutez le script de configuration. Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'agent sur les systèmes Windows et Linux.

Avant de commencer

Avant de commencer à configurer l'agent Db2 pour la surveillance en local et à distance, veillez à réaliser la tâche suivante pour la surveillance à distance.

- Configuration de l'environnement client/serveur pour la surveillance à distance ; voir «Prérequis pour la surveillance à distance», à la page 259.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration. Vous éditez les valeurs de paramètre dans le fichier de réponses, et exécutez le script de configuration pour créer une instance d'agent et mettre à jour les valeurs de configuration.

Procédure

1. Dans un éditeur de texte, ouvrez le fichier db2_silent_config.txt disponible à l'emplacement suivant :

   Linux AIX *rép_install*/samples/db2_silent_config.txt

   Windows *rép_install*\tmaitm6_x64\samples\db2_silent_config.txt

2. Dans le fichier de réponses, indiquez une valeur pour les paramètres suivants :

   - Dans la zone **Username**, entrez le nom d'utilisateur de l'instance Db2.

     Pour Db2 en local, entrez le nom du propriétaire d'instance Db2.

     Pour Db2 à distance, entrez le nom réel du propriétaire d'instance Db2 sur la machine Db2 distante.

     Important : Ce paramètre est obligatoire pour la surveillance de l'instance Db2 distante.
   - Dans la zone **Password**, entrez le mot de passe de l'instance Db2.

Pour Db2 en local, entrez le mot de passe du propriétaire d'instance Db2.

Pour Db2 à distance, entrez le mot de passe réel du propriétaire d'instance Db2 sur la machine Db2 distante.

Important : Ce paramètre est obligatoire pour la surveillance de l'instance Db2 distante.

- Pour le paramètre **DB2 SQL path**, laissez à blanc cette zone si le fichier de définition SQL est disponible dans le répertoire par défaut. Sinon, entrez le chemin de répertoire correct. Le fichier de définition SQL est disponible au chemin d'accès par défaut suivant :

  Linux AIX `CANDLEHOME/config/kudcussql.properties` Par exemple, **KUD_DB2_SQL_PATH=** `/opt/ibm/apm/agent/config/kudcussql.properties`

  Windows `CANDLEHOME\TMAITM6_x64\kudcussql.properties` Par exemple, **KUD_DB2_SQL_PATH=** `C:\IBM\ITM\TMAITM6_x64\kudcussql.properties`

- Pour le paramètre **dialog path**, laissez à blanc cette zone si le fichier journal db2diag est disponible dans le répertoire par défaut. Sinon, entrez le chemin de répertoire correct. Le fichier journal est disponible au chemin d'accès par défaut suivant :

  Linux AIX `/home/rép_base_propriétaireDB2/sqllib/db2dump`
  Par exemple, **KUD_DIAGLOG_PATH=** `/home/db2inst1/sqllib/db2dump`.

  Windows `unité_installation_Windows:\ProgramData\IBM\DB2\DB2COPY \DB2INSTANCENAME`
  Par exemple, **KUD_DIAGLOG_PATH=** `C:\ProgramData\IBM\DB2\DB2COPY1\DB2`

  Remarque : Ce paramètre n'est pas applicable à la surveillance à distance.

- Pour le paramètre **dialog message ID filter**, indiquez *MSGID* pour filtrer le journal de diagnostic. MSGID est une combinaison du type de message, du numéro de message et du niveau de gravité. Vous pouvez également utiliser une expression régulière, par exemple **KUD_DIAGLOG_MSGID_FILTER=** `ADM1\d*1E|ADM222\d2W`.
- Pour le paramètre **monitor remote partitions**, entrez Yes pour indiquer que l'agent Db2 surveille des partitions sur des hôtes distants. Par exemple, **KUD_MONITOR_REMOTE_PARTITIONS=** *Yes*.
- Pour le paramètre **monitor all databases**, entrez Yes pour indiquer que vous souhaitez que l'agent Db2 surveille toutes les bases de données. Par exemple, **KUD_MONITOR_ALL_DATABASES=** *Yes*.

3. Sauvegardez et fermez le fichier db2_silent_config.txt et exécutez la commande suivante :

   Linux AIX *rép_install*`/bin/db2-agent.sh config` *nom_instance* *rép_install*`/samples/ db2_silent_config.txt`

   Windows *rép_install*`\bin\db2-agent.bat config`*nom_instance* `\tmaitm6_x64\samples\db2_silent_config.txt`

   <nom_instance> est

   - Pour la surveillance en local du serveur Db2 : le nom de l'instance du serveur Db2 que vous voulez surveiller.
   - Pour la surveillance à distance du serveur Db2 : le nom du noeud catalogue de l'instance du serveur Db2 distante.

   Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.

4. Pour Windows, ouvrez le fichier CANDLEHOME\TMAITM6_x64\KUDENV_<nom_instance> et éditez la ligne KUD_DB2_CLIENT_INST comme suit : KUD_DB2_CLIENT_INST=<nom de l'instance client sous lequel l'instance du serveur Db2 distant est cataloguée>
5. Exécutez la commande suivante pour démarrer l'agent :

   Linux AIX *rép_install*`/bin/db2-agent.sh start` *nom_instance*

Windows *rép_install*\bin\db2-agent.bat start nom_instance

A faire : Lors de la surveillance de l'instance du serveur Db2 distante sous UNIX ou Linux, la commande doit être exécutée en tant que propriétaire de l'instance client sous lequel l'instance du serveur distant est cataloguée.

Que faire ensuite

- Accordez à l'utilisateur Db2 les privilèges lui permettant d'afficher les données relatives à certains attributs de l'agent Db2. Pour plus d'informations sur l'octroi de ces privilèges, voir «Octroi de privilèges pour l'affichage des mesures Db2», à la page 255.
- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Octroi de privilèges pour l'affichage des mesures Db2

Pour surveiller les ressources Db2, un utilisateur Db2 doit disposer des droits Db2 SYSADM, SYSCTRL, SYSMAINT et SYSMON pour l'instance surveillée afin de visualiser les données pour certains attributs de l'agent Db2.

Pourquoi et quand exécuter cette tâche

Pour afficher les données de surveillance que l'agent collecte pour tous les attributs du tableau de bord, l'utilisateur Db2 doit disposer de privilèges spécifiques. Pour affecter ces privilèges à l'utilisateur Db2, exécutez le fichier de script qui se trouve à l'emplacement suivant :

Linux AIX *rép_install*/config/KudGrantUserPermissions.sh

Windows *rép_install*\TMAITM6_x64\KudGrantUserPermissions.bat

Un utilisateur Db2 disposant du droit d'accès SYSADM peut exécuter le script permettant d'octroyer des privilèges à lui-même ou à n'importe quel autre utilisateur Db2. Pour une instance Db2, utilisez le propriétaire d'instance, qui dispose déjà du droit d'accès SYSADM, pour exécuter le script qui lui permet d'octroyer d'autres droits à lui-même ou l'ensemble des droits à tout autre utilisateur Db2.

Procédure

1. Pour la surveillance en local, procédez comme suit.
   a) Sur le système où l'agent Db2 est installé, ouvrez l'interface de ligne de commande Db2.
   b) Exécutez la commande suivante, où *nom_instance* est le nom de l'instance Db2 et *nom_utilisateur* est le nom de l'utilisateur Db2 :

      Linux AIX *rép_install*/config/KudGrantUserPermissions.sh *nom_instance nom_utilisateur*

      Windows *rép_install*\TMAITM6_x64\KudGrantUserPermissions.bat *nom_instance nom_utilisateur*

      Remarque : Pour les systèmes Windows, *nom_utilisateur* est facultatif dans la commande. Si aucun nom d'utilisateur n'est spécifié dans la commande, les privilèges sont affectés à l'utilisateur par défaut (système).
2. Pour la surveillance à distance, procédez comme suit.
   a) Copiez le fichier KudGrantUserPermissions.sh pour Unix ou Linux et le fichier KudGrantUserPermissions.bat pour Windows, figurant dans le répertoire *rép_install*/TMAITM6_x64/ du poste de travail d'agent, sur la machine du serveur Db2.
   b) Exécutez la commande suivante en tant que propriétaire de l'instance Db2, où *nom_instance* est le nom de l'instance Db2 et *nom_utilisateur* est le nom de l'utilisateur Db2 :

Linux AIX `./KudGrantUserPermissions.sh nom_instance nom_utilisateur`

Windows `KudGrantUserPermissions.bat nom_instance nom_utilisateur`

A faire : Pour la surveillance à distance de Db2 sous Windows, *nom_utilisateur* doit correspondre au nom d'utilisateur fourni pendant la configuration de l'agent Db2 sur le poste de travail client.

Configuration des variables d'environnement local

Vous pouvez configurer les variables d'environnement local pour modifier le comportement de agent Db2.

Procédure

1. Sur les systèmes Windows, cliquez sur **Démarrer** > **Tous les programmes** > **Agents IBM Monitoring** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, dans le menu **Actions**, cliquez sur **Advanced > Edit ENV File**.
3. Sur les systèmes Linux ou AIX, accédez à la ligne de commande et éditez le fichier ud.environment à partir du répertoire rép_install/config, rép_install représentant le répertoire d'installation de l'agent.

   Remarque : Le fichier ud.environment est un fichier caché.
4. Dans le fichier des variables d'environnement, entrez des valeurs pour les variables d'environnement.

   Pour plus d'informations sur les variables d'environnement que vous pouvez configurer, voir «Variables d'environnement local», à la page 256.

Variables d'environnement local

Vous pouvez changer le comportement de agent Db2 en définissant les variables d'environnement local.

Variables permettant de définir la méthode de collecte des données pour le jeu de données de l'espace table

Pour définir la méthode de collecte de données pour le jeu de données de l'espace table, utilisez les variables d'environnement suivantes :

- **KUD_T1_BY_SQL** : utilisez cette variable pour définir la méthode de collecte de données pour le jeu de données de l'espace table à l'aide de requêtes SQL. Pour activer la collecte de données à l'aide de requêtes SQL, définissez la valeur de cette variable sur Y. Pour collecter des données pour le jeu de données de l'espace table à l'aide de la méthode d'image instantanée, définissez la valeur de cette variable sur N. La valeur par défaut de cette variable est N.

  Important : Pour collecter des données à l'aide de requêtes SQL, la version de Db2 doit être 9.7 ou supérieure. En outre, l'utilisateur qui démarre l'agent Db2 doit disposer du droit d'accès SYSADM pour l'ensemble des bases de données.
- **KUD_T1_DISABLE** : utilisez cette variable pour désactiver la collecte de données pour le jeu de données de l'espace table. Pour activer la collecte de données pour le jeu de données de l'espace table, définissez la valeur de cette variable sur N. Pour désactiver la collecte de données pour le jeu de données de l'espace table, définissez la valeur de cette variable sur Y. La valeur par défaut de cette variable est N.

Variable permettant d'exclure les noeuds CF (Caching Facility) de la collection de données

Pour exclure les noeuds CF (Caching Facility) de l'algorithme de collecte de données dans l'environnement pureScale, utilisez la variable **DB2_CF_PARTITION_NUMS**. Dans le fichier d'environnement de l'agent, définissez la variable **DB2_CF_PARTITION_NUMS** sur DB2_CF_PARTITION_NUMS=<nombre de noeuds CF>. Par exemple, DB2_CF_PARTITION_NUMS=1. Pour plusieurs noeuds CF, spécifiez pour la variable **DB2_CF_PARTITION_NUMS** une liste qui utilise l'un des caractères spéciaux # . : , ; | @ comme délimiteur. Par exemple, DB2_CF_PARTITION_NUMS=12,13,23,34. Aucune valeur par défaut n'est définie pour cette variable.

Variable permettant de limiter la collecte de données pour le jeu de données de tables Db2

Pour définir le nombre maximal de lignes que l'agent Db2 doit renvoyer, tout en collectant des données pour le jeu de données de tables Db2, utilisez la variable d'environnement **KUD_TABLE_NUMBER**. La valeur par défaut est 10000.

Variable permettant de définir l'intervalle de rechargement du fichier de propriétés SQL personnalisé

Pour définir l'intervalle de temps de rechargement (en secondes) pour le fichier de propriétés SQL personnalisé, utilisez la variable **KUD_CUS_SQL_INTERVAL**. La valeur par défaut est 20 secondes.

Variable permettant de limiter les lignes dans la collecte de données pour le jeu de données Evénement de l'agent

Pour définir le nombre de lignes pour la collecte de données du jeu de données Evénement de l'agent, utilisez la variable **KUD_AGENT_EVENT_CACHE**. Le jeu de données Evénement de l'agent fournit des informations détaillées sur les événements prédéfinis et déclenchés et détermine les problèmes de santé de la base de données surveillée. La valeur par défaut est 50.

Variable permettant de limiter les lignes dans la collecte de données pour le jeu de données Enregistrement du journal Db2

Pour définir le nombre de lignes pour la collecte de données du jeu de données Enregistrement du journal Db2, utilisez la variable **KUD_DBHISTORY_MAXROW**. Le jeu de données Enregistrement du journal Db2 fournit des informations historiques sur le journal d'archivage de Db2. La valeur par défaut est 500.

Variables permettant de définir la collecte des données pour le jeu de données Journal de diagnostic Db2

Pour définir la méthode de collecte de données pour le jeu de données Journal de diagnostic Db2, utilisez les variables d'environnement suivantes :

- **KUD_DIAGLOG_BY_TABLE** : utilisez cette variable pour définir la méthode de collecte de données pour le jeu de données Journal de diagnostic Db2. Si la valeur de cette variable est définie sur Y, alors les données pour le jeu de données Journal de diagnostic Db2 sont collectées à l'aide des requêtes SQL. Si la valeur de cette variable est définie sur N, alors les données pour le jeu de données Journal de diagnostic Db2 sont collectées par analyse du fichier db2diag.log. La valeur par défaut de cette variable est Y.

  Important : Pour collecter des données à l'aide de requêtes SQL, la version de Db2 doit être 10 ou supérieure.
- **KUD_DIAGLOG_TAILCOUNT** : utilisez cette variable pour définir le nombre de lignes du fichier db2diag.log que l'agent Db2 analyse pour collecter des données pour le jeu de données Journal de diagnostic DB2. Cette variable limite le traitement du fichier journal par l'agent Db2 de façon à ce que seuls les événements et les messages les plus récents soient surveillés. La valeur par défaut de cette variable est 1000.
- **KUD_DIAGLOG_CACHE** : utilisez cette variable pour limiter le nombre d'enregistrements de journal qui s'affichent sur le tableau de bord pour le jeu de données Journal de diagnostic Db2. La valeur par défaut de cette variable est 20.
- **KUD_DIAGLOG_INTERVAL** : utilisez cette variable pour définir l'intervalle de temps de rechargement (en secondes) du fichier db2diag.log pour collecter des données pour le jeu de données Journal de diagnostic Db2. La valeur par défaut de cette variable est 30 secondes.
- **KUD_DISABLE_DIAGLOG** : utilisez cette variable pour désactiver la collecte de données pour le jeu de données Journal de diagnostic Db2. Pour activer la collecte de données pour le jeu de données Journal de diagnostic Db2, définissez la valeur de cette variable sur N. Pour désactiver la collecte de données pour le jeu de données Journal de diagnostic Db2, définissez la valeur de cette variable sur Y. La valeur par défaut de cette variable est N.

Variable de définition du délai d'expiration de la requête

Si une requête SQL prend très longtemps pour s'exécuter, cela affecte les performances de l'agent Db2. Pour définir le délai d'expiration de requête pour l'agent Db2, utilisez la variable **KUD_QUERY_TIMEOUT**. Cette variable d'environnement permet de définir le délai maximal (en secondes) pendant lequel l'agent Db2 attend une réponse pour une requête envoyée au serveur Db2. La valeur par défaut de cette variable doit être inférieure à 300 secondes. La valeur par défaut de cette variable est 45 secondes.

Variable permettant de définir la collecte des données pour le jeu de données DB2 Database01 (obsolète)

L'agent ne doit pas déclencher de requêtes ASN pour collecter des données pour le jeu de données DB2 Database01 (obsolète) lorsque les schémas ASN ne sont pas présents. Pour activer l'exécution des requêtes ASN, utilisez la variable **KUD_REPLICATION_ON**. Si la valeur de cette variable est définie sur Y, l'agent Db2 exécute les requêtes ASN même lorsque les schémas ASN ne sont pas présents. Si la valeur de cette variable est définie sur N, l'agent Db2 n'exécute pas les requêtes ASN. La valeur par défaut de cette variable est Y.

Variable permettant de configurer les inverseurs logiques du moniteur lors de la collecte de données à l'aide de la méthode d'image instantanée

Si vous voulez collecter les données de surveillance de l'agent Db2 à l'aide de la méthode d'image instantanée, activez l'inverseur logique du moniteur Db2 pour le jeu de données. Pour activer l'inverseur logique du moniteur Db2, utilisez la variable **KUD_MON_SWITCH_OVERRIDE**. La liste des inverseurs logiques du moniteur Db2 est la suivante :

LOCK
Informations sur les verrous

SORT
Informations sur les tris

STATEMENT
Informations sur les instructions SQL

TABLE
Informations sur les activités de table

TIMESTAMP
Informations sur les horodatages

UOW
Informations sur les unités d'oeuvre.

Si la valeur de cette variable est définie sur Y, l'agent Db2 maintient les paramètres de configuration des inverseurs logiques du moniteur Db2. Si la valeur de cette variable est définie sur N, l'agent Db2 active tous les inverseurs logiques du moniteur pour collecter des données. La valeur par défaut de cette variable est N.

Variable permettant de tracer les données en mémoire tampon d'image instantanée Db2 d'un jeu de données

Pour afficher les données collectées pour un jeu de données à l'aide de la méthode d'image instantanée, utilisez la variable **KUD_SNAPSHOT_DUMPOUT**. Si la valeur de cette variable est définie sur Y, l'agent Db2 vide les données en mémoire tampon d'image instantanée pour les groupes d'attributs dans le fichier journal de l'agent. Si la valeur de cette variable est définie sur N, l'agent Db2 ne vide pas les données en mémoire tampon d'image instantanée dans le fichier journal de l'agent. La valeur par défaut de cette variable est N.

Variable permettant de tracer l'agent Db2 à l'aide des données en mémoire tampon d'image instantanée d'un jeu de données

Pour tracer l'agent Db2 à l'aide des données en mémoire tampon d'image instantanée collectées pour un jeu de données, utilisez la variable **KUD_SNAPSHOT_READIN**. Pour activer le traçage d'un agent Db2,

définissez la valeur de cette variable sur Y. Pour désactiver le traçage d'un agent Db2, définissez la valeur de cette variable sur N.

Variable permettant de définir la méthode de collecte des données pour le jeu de données Conflit de verrouillage

Pour définir la méthode de collecte de données pour le jeu de données Conflit de verrouillage, utilisez la variable **KUD_LOCKCONFLICT_BY_SQL**. Pour collecter des données pour le jeu de données Conflit de verrouillage à l'aide de requêtes SQL, définissez la valeur de cette variable sur Y. Pour collecter des données pour le jeu de données Conflit de verrouillage à l'aide de la méthode d'image instantanée, définissez la valeur de cette variable sur N. La valeur par défaut de cette variable est Y.

Important : Pour collecter des données à l'aide de requêtes SQL, la version de Db2 doit être 9.7 FP1 ou supérieure. En outre, l'utilisateur qui démarre l'agent Db2 doit disposer du droit d'accès SYSADM pour l'ensemble des bases de données.

Variable permettant de surveiller le serveur Db2 distant sous Windows

KUD_DB2_CLIENT_INST : définissez cette variable sur le nom de l'instance client Db2 sous lequel l'instance distante du serveur Db2 est cataloguée. Vous ne devez définir cette variable que si vous utilisez la surveillance à distance où l'agent réside sous Windows.

Prérequis pour la surveillance à distance

Vous pouvez utiliser Monitoring Agent for Db2 pour la surveillance à distance. Consultez la rubrique relative aux prérequis pour la surveillance à distance de Db2.

Pourquoi et quand exécuter cette tâche

Pour la surveillance à distance de Db2, vous devez commencer par la configuration de base de l'environnement client/serveur Db2. Effectuez cette configuration pour Windows et UNIX ou Linux.

L'utilisateur doit disposer des droits d'accès Db2 SYSADM ou SYSCTRL.

A faire : Suivez toutes les étapes sur le poste de travail de l'agent, à l'exception de l'étape 2.

Procédure

1. Sur le poste de travail de l'agent Db2, installez le client Db2. La version de ce client doit être supérieure ou égale à la version de l'instance du serveur Db2 à surveiller.
2. Vérifiez que le protocole de communication de l'instance Db2 est TCPIP.
   a) Pour ce faire, exécutez la commande **db2set** sur la `ligne de commande` Db2.
   b) Si le protocole n'est pas défini sur TCPIP, exécutez **db2set DB2COMM=tcpip** sur la `ligne de commande` Db2.

   Important : Cette étape est réalisée côté serveur.
3. Cataloguez l'instance du serveur distant au niveau du poste de travail de l'agent Db2 en exécutant la commande suivante.

   Important : L'instance du serveur doit être cataloguée sous l'instance client. Vous devez donc exécuter la commande suivante sur l'instance client.

   db2=>CATALOG TCPIP NODE<nom_noeud> REMOTE <nomhôte/adresse_ip> SERVER <nom_service/numéro_port>

   sur Db2, où :

   a. *<nom_noeud>* représente un pseudonyme local de l'instance Db2 sur le composant client.

      Remarque : Pour UNIX ou Linux, *<nom_noeud>* doit être différent de celui de n'importe quel nom d'instance client Db2 ou serveur Db2 disponible sur le même poste de travail.

   b. <nomhôte/adresse_IP> représente le nom ou l'adresse IP du poste de travail du serveur Db2.

c. <nom_service/numéro_port> représente le nom de service ou le numéro de port de configuration du protocole TCPIP Db2.

Pour cataloguer l'instance de serveur Db2 qui s'exécute sur le numéro de port 50000 sur le serveur distant "**myserver**" en tant que noeud "db2node", entrez la commande suivante à partir d'une ligne de commande Db2 :

```
db2 => CATALOG TCPIP NODE db2node REMOTE myserver SERVER 50000
```

Pour plus de détails sur le noeud catalogue, voir https://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.qb.client.doc/doc/t0005621.html

4. Si le poste de travail de l'agent Db2 s'exécute sous UNIX/Linux,
   - Créez un utilisateur dont le nom de noeud est utilisé dans la commande de catalogage.

     Exécutez la commande suivante :

     ```
     useradd -g <groupe> -m -d <rép_base> <utilisateur> -p <mot_de_passe>
     ```

     où

     – **<groupe>** représente un groupe pour les propriétaires d'instance DB2 UDB.
     – **<utilisateur>** représente un **nom d'utilisateur** local sur le poste de travail client. Le **nom d'utilisateur** doit être identique au nom du noeud avec lequel l'instance du serveur a été cataloguée sur la machine agent.
   - Vérifiez le nom de l'instance client Db2 sous lequel l'instance du serveur Db2 distante est catalogué et attribuez les droits en lecture, écriture et exécution du répertoire de base de l'utilisateur que vous venez de créer au propriétaire de cette instance. Cette étape est nécessaire pour rendre l'environnement client Db2 disponible pour effectuer les opérations sur le noeud distant.
   - Exécutez la commande suivante :

     ```
     chmod -R 775 /home/<nom_noeud>
     ```

     où

     – **<nom_noeud>** représente un nom d'utilisateur local de l'instance Db2 sur le composant client
5. Cataloguez toutes les bases de données que vous voulez surveiller sur l'instance client figurant sur le poste de travail de l'agent Db2.

   Exécutez la commande dans l'interpréteur de commandes Db2 pour cataloguer la base de données.

   ```
   CATALOG DATABASE <nom_bdd> AS <alias_bdd> AT NODE <nom_noeud>authentication server
   ```

   a. <nom_bdd> représente le nom de la base de données du serveur.
   b. <alias_bdd> représente l'alias local de la base de données sur le client Db2.
   c. <nom_noeud> représente un pseudonyme local de l'instance Db2 sur le composant client où la base de données est cataloguée.

   Pour cataloguer une base de données nommée "sample" sur le noeud catalogue "db2node" portant l'alias "dbAlias1", entrez la commande suivante à partir d'une invite Db2.

   ```
   db2 => CATALOG DATABASE sample AS dbAlias1 AT NODE db2node authentication server
   ```

Configuration de la surveillance de Hadoop

Vous devez configurer Monitoring Agent for Hadoop pour qu'il puisse collecter les données d'un cluster Hadoop surveillé. L'agent peut surveiller un cluster Hadoop à noeud unique et à plusieurs noeuds.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Hadoop.

Assurez-vous que les hôtes suivants peuvent être résolus à partir de l'ordinateur sur lequel l'agent Hadoop est installé :

- Tous les hôtes Hadoop que vous voulez configurer, comme NameNode, ResourceManager, et ainsi de suite
- Hôtes Hadoop ayant seulement le rôle NodeManager

Par exemple, vous pouvez effectuer les étapes suivantes pour résoudre les hôtes :

- Ajoutez l'adresse IP, le nom d'hôte et le nom de domaine complet de tous les hôtes Hadoop au fichier `hosts` qui est disponible à l'emplacement suivant :
  - Windows `C:\Windows\System32\drivers\etc\hosts`
  - Linux AIX `/etc/hosts`
- Ajoutez l'ordinateur sur lequel l'agent Hadoop est installé dans le même domaine que celui des hôtes Hadoop.

A faire : Pour surveiller un cluster Hadoop sécurisé avec l'authentification basée sur Kerberos SPNEGO, vérifiez que tous les hôtes peuvent être résolus à partir de l'ordinateur sur lequel l'agent Hadoop est installé.

Pourquoi et quand exécuter cette tâche

L'agent Hadoop est un agent à instance unique. Une fois l'agent installé, vous devez le configurer manuellement. L'agent Hadoop peut être configuré sur des systèmes Windows, Linux et AIX.

A faire :

- Pour un cluster Hadoop à noeud unique, le même noeud joue tous les rôles, tels que NameNode, ResourceManager et le rôle NameNode secondaire, en fonction de la configuration du cluster Hadoop. Pour un cluster Hadoop à plusieurs noeuds, ce sont d'autres noeuds Hadoop qui jouent ces rôles.
- Lorsque vous configurez l'agent, ce dernier détecte automatiquement les rôles DataNodes et NodeManagers dans le cluster Hadoop actuellement surveillé.

Lorsque vous effectuez une mise à niveau à partir de l'agent qui utilise des sockets (8.1.2 Fix Pack 2, ou version antérieure) vers l'agent qui utilise l'API (8.1.3, ou version supérieure), effectuez les étapes de configuration indiquées dans les rubriques suivantes. Cependant, assurez-vous d'indiquer les noms d'hôte conformément aux instructions suivantes lorsque vous configurez l'agent.

- Le nom de hôte de divers processus démon (NameNode, ResourceManger, etc.) que vous indiquez doit être identique (casse et mise en forme) que les noms de hôte qui sont configurés pour l'agent qui utilise les sockets.
- Le nom de domaine complet doit être utilisé lorsque vous spécifiez un nom d'hôte. Par exemple, `hos1.ibm.com`. Si la longueur du nom de domaine complet dépasse 25 caractères, indiquez seulement le nom d'hôte abrégé sans le nom de domaine. Par exemple, si le nom de domaine complet d'un hôte est *myhadoopclustersetupnode.ibm.com*, le nom d'hôte abrégé est `myhadoopclustersetupnode`.

Une fois que vous avez configuré l'agent mis à niveau et que vous visualisez des données dans la console Cloud APM, annulez les modifications qui ont été apportées dans le fichier hadoop-

`metrics2.properties` pour l'agent Hadoop. Pour plus d'informations, voir «Mise à niveau de vos agents», à la page 1171.

Sur les systèmes Windows, vous pouvez exécuter l'agent Hadoop en tant qu'utilisateur non-administrateur. Un tel utilisateur nécessite toutefois un droit spécifique pour afficher les données dans les tableaux de bord. Pour plus d'informations sur l'attribution de ce droit, voir «Attribution de droits aux utilisateurs non administrateurs», à la page 270.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent sur des systèmes Windows à l'aide de la fenêtre **IBM Performance Management**.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Monitoring Agent for Hadoop**.
3. Cliquez sur **Configuration de l'agent**.

   Avertissement : Si **Configuration de l'agent** est désactivé, cliquez sur **Reconfigurer**.

   La fenêtre **Configure Monitoring Agent for Hadoop** s'ouvre.
4. Pour surveiller le cluster Hadoop avec l'authentification basée sur Kerberos SPNEGO activée, procédez comme suit :
   a) Sous **L'authentification basée sur Kerberos SPNEGO pour les services Hadoop basés sur HTTP dans le cluster Hadoop est-elle activée**, cliquez sur **Oui**.

      Si vous ne disposez pas de l'authentification basée sur Kerberos SPNEGO pour sécuriser les noeuds finaux REST des services Hadoop basés sur HTTP dans le cluster Hadoop, cliquez sur **No**. Les valeurs des zones **Realm name**, **KDC Hostname**, **SPNEGO principal name** et **SPNEGO keytab file** peuvent alors rester à blanc.

   b) Dans la zone **Nom de domaine**, entrez le nom du domaine Kerberos utilisé pour créer les principaux des services.
   Généralement, le nom de domaine (realm) correspond à votre nom de domaine (domain). Par exemple, si votre ordinateur se trouve dans le domaine (domain) `tivoli.ibm.com`, le nom de domaine (realm) Kerberos est `TIVOLI.IBM.COM`. Ce nom est sensible à la casse.

   c) Dans la zone **Nom d'hôte KDC**, entrez le nom de domaine complet de l'hôte KDC (centre de distribution de clés) pour le domaine spécifié.

      Vous pouvez également indiquer l'adresse IP de l'hôte KDC à la place du nom de domaine complet. Dans le cas d'un centre de distribution de clés Active Directory, le contrôleur de domaine est l'hôte KDC.

   d) Dans la zone **SPNEGO principal name**, entrez le nom du principal Kerberos utilisé pour accéder aux noeuds finaux REST authentifiés par SPNEGO des services HTTP.

      Le nom est sensible à la casse et il est au format HTTP/*nom_hôte_qualifié_complet@domaine_kerberos*

   e) Dans la zone **Fichier de clés SPNEGO**, entrez le nom du fichier de clés du service SPNEGO avec son chemin d'accès complet ou cliquez sur **Parcourir** et sélectionnez-le.

Le fichier de clés contient les noms des principaux et des clés des services Kerberos. Ce fichier fournit un accès direct aux services Hadoop sans nécessiter de mot de passe pour chaque service. Il peut être placé dans le chemin suivant : `etc/security/keytabs/`
Vérifiez que le nom de principal et le fichier de clés SPNEGO appartiennent au même hôte. Par exemple, si le nom de principal est *HTTP/abc.ibm.com@IBM.COM*, le fichier de clés utilisé doit appartenir à l'hôte *abc.ibm.com* host.
Si l'agent est installé sur un ordinateur distant, copiez le fichier de clés ou le principal sur l'ordinateur distant, dans n'importe quel chemin, puis spécifiez ce dernier dans la zone **SPNEGO keytab file**.

f) Cliquez sur **Suivant**.

5. Pour surveiller le cluster Hadoop activé pour HTTPS/SSL, procédez comme suit :
   a) Sous **Is Hadoop Cluster SSL enabled**, cliquez sur **Oui**

      Si vous ne souhaitez pas le cluster Hadoop activé pour SSL, sélectionnez **Non**. Les valeurs des zones **TrustStore file path** et **TrustStore Password** peuvent alors rester à blanc.

   b) Dans **TrustStore file path**, sélectionnez le fichier TrustStore stocké sur votre machine locale.

      Ce fichier peut être copié depuis le cluster Hadoop vers votre machine locale, puis utilisé pour la configuration.

   c) Dans **TrustStore Password**, entrez le mot de passe que vous avez créé lors de la configuration du fichier TrustStore.
6. Pour spécifier les valeurs des paramètres du cluster Hadoop, procédez comme suit :
   a) Dans la zone **Unique Hadoop Cluster Name**, spécifiez le nom unique du cluster Hadoop indiquant la version d'Hadoop. Le nombre maximal de caractères pour cette zone est 12.
   b) Dans la zone **Nom d'hôte du NameNode**, entrez le nom d'hôte du noeud où le processus démon pour NameNode est exécuté.
   c) Dans la zone **Port du NameNode**, entrez le numéro de port associé au processus démon pour NameNode. Le numéro de port par défaut est 50070.
   d) Dans la zone **Nom d'hôte du gestionnaire de ressources**, entrez le nom d'hôte du noeud où le processus démon pour le gestionnaire de ressources est exécuté.
   e) Dans la zone **Port du gestionnaire de ressources**, entrez le numéro de port associé au processus démon pour le gestionnaire de ressources. Le numéro de port par défaut est 8088.
   f) Facultatif : Dans la zone **Nom d'hôte du JobHistoryServer**, entrez le nom d'hôte du noeud où le processus démon du JobHistoryServer est exécuté.
   g) Facultatif : Dans la zone **Port du JobHistoryServer**, entrez le numéro de port associé au processus démon du JobHistoryServer. Le numéro de port par défaut est 19888.
   h) Facultatif : Dans la zone **Nom d'hôte du NameNode supplémentaire**, entrez le nom d'hôte du noeud où le processus démon pour un Namenode secondaire ou de secours est exécuté.
   i) Facultatif : Dans la zone **Port du NameNode supplémentaire**, entrez le numéro de port associé au processus démon pour un Namenode secondaire ou de secours.

      A faire : Si le NameNode supplémentaire est un NameNode de secours, le numéro de port par défaut associé au processus démon pour un NameNode de secours est 50070. Si le NameNode supplémentaire est un NameNode secondaire, le numéro de port par défaut associé au processus démon pour un NameNode secondaire est 50090.

   j) Cliquez sur **Tester la connexion** pour vérifier la connexion aux noms d'hôte et aux ports spécifiés.

      Une fois que vous avez cliqué sur **Tester la connexion**, un message de validation approprié s'affiche lorsque :

      - La connexion aux noms d'hôte et aux ports spécifiés est établie ou a échoué.
      - Une valeur pour un nom d'hôte est restée vide.
      - Une valeur pour un port est restée vide.
      - Une valeur non entière est spécifiée pour un numéro de port.

Mettez à jour les valeurs de configuration comme suggéré dans les messages de validation et vérifiez de nouveau la connexion.

k) Facultatif : Pour ajouter des gestionnaires de ressources de secours dans le cluster Hadoop, cliquez sur **Oui** sous **Gestionnaire(s) de ressource de secours dans le cluster Hadoop**.

Vous êtes invité à ajouter les détails relatifs aux gestionnaires de ressources de secours ultérieurement.

l) Facultatif : Pour surveiller les services Hadoop dans le cluster Hadoop géré par Apache Ambari, cliquez sur **Oui** sous **Surveillance des services Hadoop pour les installations Hadoop basées sur Ambari**, puis sur **Suivant**.

7. Facultatif : Pour spécifier les détails du serveur Ambari pour la surveillance des services Hadoop, procédez comme suit :
   a) Dans la zone **Nom d'hôte du serveur Ambari**, entrez le nom de l'hôte sur lequel s'exécute le serveur Ambari.
   b) Dans la zone **Port serveur Ambari**, entrez le numéro de port associé au serveur Ambari. Le numéro de port par défaut est 8080.
   c) Dans la zone **Nom de l'utilisateur Ambari**, entrez le nom de l'utilisateur Ambari.
   d) Dans la zone **Mot de passe de l'utilisateur Ambari**, entrez le mot de passe de l'utilisateur Ambari.
   e) Cliquez sur **Suivant**.
8. Pour spécifier les valeurs des paramètres Java, procédez comme suit :
   a) Dans la liste **Niveau de trace Java**, sélectionnez une valeur pour le niveau de trace utilisé par les fournisseurs Java.
   b) Facultatif : Dans la zone **Arguments JVM**, spécifiez une liste d'arguments pour la machine virtuelle Java.

      La liste d'arguments doit être compatible avec la version de Java installée avec l'agent.
   c) Cliquez sur **Suivant**.
9. Facultatif : Pour ajouter des gestionnaires de ressources de secours, procédez comme suit :
   a) Cliquez sur **Nouveau**.
   b) Dans la zone **Nom d'hôte du gestionnaire de ressources de secours**, entrez le nom d'hôte du noeud où le processus démon pour le gestionnaire de ressources de secours est exécuté.
   c) Dans la zone **Port du gestionnaire de ressources de secours**, entrez le numéro de port associé au processus démon pour le gestionnaire de ressources de secours. Le numéro de port par défaut est 8088.
   d) Cliquez sur **Tester la connexion** pour valider la connexion au nom d'hôte et au numéro de port spécifiés.

      Une fois que vous avez cliqué sur **Tester la connexion**, un message de validation approprié s'affiche lorsque :

      - La connexion aux noms d'hôte et aux ports spécifiés est établie ou a échoué.
      - Une valeur pour un nom d'hôte est restée vide.
      - Une valeur pour un port est restée vide.
      - Une valeur non entière est spécifiée pour un numéro de port.

      Mettez à jour les valeurs de configuration comme suggéré dans les messages de validation et vérifiez de nouveau la connexion.
   e) Répétez les étapes a, b et c pour ajouter d'autres gestionnaires de ressources de secours.

      Si vous voulez supprimer un des gestionnaires de ressources de secours, cliquer sur le bouton **Supprimer** correspondant au gestionnaire de ressources de secours que vous voulez supprimer.
   f) Cliquez sur **Suivant**.
10. Dans la zone **Chemin d'accès aux classes pour les fichiers JAR**, indiquez le chemin d'accès aux classes des fichiers JAR externes.

Ce chemin d'accès aux classes est ajouté au chemin d'accès aux classes généré par l'agent. Vous pouvez laisser cette zone vide.

11. Cliquez sur **OK**.

    Les paramètres de configuration spécifiés sont sauvegardés.

12. Cliquez avec le bouton droit de la souris sur **Monitoring Agent for Hadoop**, puis cliquez sur **Démarrer**.

Que faire ensuite

1. Activez les événements de sous-noeud pour visualiser les seuils de génération d'événement de l'agent Hadoop. Pour plus d'informations sur l'activation des événements de sous-noeud, voir «Configuration du tableau de bord pour visualiser des événements Hadoop», à la page 269.
2. Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de l'agent sur des systèmes Linux et AIX

Vous exécutez le script de configuration et répondez aux invites pour configurer l'agent sur les systèmes Linux et AIX.

Procédure

1. Sur la ligne de commande, exécutez la commande suivante : *rép_install*`/bin/hadoop-agent.sh config`
   Où *rép_install* est le répertoire d'installation de l'agent Hadoop.

   L'agent est installé dans le répertoire d'installation par défaut suivant : `/opt/ibm/apm/agent`
2. Quand la ligne de commande affiche le message suivant, entrez 1 pour continuer les étapes de configuration et appuyez sur Entrée.
   `Edit "Monitoring Agent for Hadoop" setting? [1= yes, 2= No]`
3. Lorsque la ligne de commande affiche le message suivant, entrez 1 pour spécifier les valeurs de surveillance du cluster Hadoop avec l'authentification basée sur Kerberos SPNEGO activée, puis appuyez sur la touche Entrée. Sinon, entrez 2 et appuyez sur Entrée. Vous pouvez conserver une valeur vide pour les zones **Nom de domaine**, **Nom d'hôte KDC**, **Nom du principal SPNEGO** et **Fichier de clés SPNEGO** :
   `Is Kerberos SPNEGO-based authentication for HTTP based Hadoop services in Hadoop cluster enabled\: [ 1=Yes, 2=No (default is: 2)`
   a) Pour le paramètre **Nom de domaine**, entrez le nom du domaine Kerberos utilisé pour créer les principaux des services.
   Généralement, le nom de domaine (realm) correspond à votre nom de domaine (domain). Par exemple, si votre ordinateur se trouve dans le domaine (domain) `tivoli.ibm.com`, le nom de domaine (realm) Kerberos est `TIVOLI.IBM.COM`. Ce nom est sensible à la casse.

   b) Dans la zone **Nom d'hôte KDC**, entrez le nom de domaine complet de l'hôte KDC (centre de distribution de clés) pour le domaine spécifié. Vous pouvez également indiquer l'adresse IP de l'hôte KDC à la place du nom de domaine complet. Dans le cas d'un centre de distribution de clés Active Directory, le contrôleur de domaine est l'hôte KDC.

   c) Pour le paramètre **Nom du principal SPNEGO**, entrez le nom du principal Kerberos utilisé pour accéder aux noeuds finals REST authentifiés par SPNEGO des services HTTP.

   Le nom est sensible à la casse et il est au format HTTP/*nom_hôte_qualifié_complet*`@`*domaine_kerberos*

   d) Pour le paramètre **Fichier de clés SPNEGO**, entrez le nom du fichier de clés du service SPNEGO avec son chemin d'accès complet.

Le fichier de clés contient les noms des principaux et des clés des services Kerberos. Ce fichier fournit un accès direct aux services Hadoop sans nécessiter de mot de passe pour chaque service. Il peut être placé dans le chemin suivant : `etc/security/keytabs/`
Vérifiez que le nom de principal et le fichier de clés SPNEGO appartiennent au même hôte. Par exemple, si le nom de principal est *HTTP/abc.ibm.com@IBM.COM*, le fichier de clés utilisé doit appartenir à l'hôte *abc.ibm.com* host.
Si l'agent est installé sur un ordinateur distant, copiez le fichier de clés ou le principal sur l'ordinateur distant, dans n'importe quel chemin, puis spécifiez ce dernier pour le paramètre **Fichier de clés SPNEGO**.

4. Lorsque la ligne de commande affiche le message suivant, entrez 1 pour spécifier les valeurs de surveillance du cluster Hadoop activé pour SSL, puis appuyez sur **Entrée**. Sinon, entrez 2 et appuyez sur **Entrée**. Vous pouvez conserver une valeur vide pour les zones **TrustStore file path** et **TrustStore Password** :
   ```
   Is Hadoop Cluster SSL enabled [ 1=Yes, 2=No (default is: 2)
   ```
   a) Dans **TrustStore file path**, indiquez le chemin du fichier TrustStore stocké sur votre machine locale.

   Ce fichier peut être copié depuis le cluster Hadoop vers votre machine locale, puis utilisé pour la configuration.

   b) Dans **TrustStore Password**, indiquez le mot de passe que vous avez créé lors de la configuration du fichier TrustStore.
5. Lorsque vous êtes invité à entrer les détails du cluster Hadoop, spécifiez une valeur appropriée pour chacun des paramètres suivants, puis appuyez sur Entrée :
   a) Dans la zone **Unique Hadoop Cluster Name**, indiquez le nom unique du cluster Hadoop indiquant la version d'Hadoop. Le nombre maximal de caractères pour cette zone est 12.

   b) Pour le paramètre **Nom d'hôte NameNode**, indiquez le nom d'hôte du noeud où le processus démon pour NameNode est exécuté, puis appuyez sur Entrée.

   Avertissement : Si vous appuyez sur Entrée sans indiquer de nom d'hôte, vous êtes invité à en entrer un.

   c) Pour le paramètre **Port NameNode**, indiquez le numéro de port associé au processus démon pour NameNode, puis appuyez sur Entrée. Le numéro de port par défaut est 50070.

   d) Pour le paramètre **Nom d'hôte du gestionnaire de ressources**, indiquez le nom d'hôte du noeud où le processus démon pour le gestionnaire de ressources est exécuté, puis appuyez sur Entrée.

   Avertissement : Si vous appuyez sur Entrée sans indiquer de nom d'hôte, vous êtes invité à en entrer un.

   e) Pour le paramètre **Port du gestionnaire de ressources**, indiquez le numéro de port associé au processus démon pour le gestionnaire de ressources. Le numéro de port par défaut est 8088.
6. Facultatif : Lorsque vous êtes invité à ajouter les détails des paramètres suivants du cluster Hadoop, acceptez la valeur par défaut ou spécifiez une valeur appropriée pour chacun des paramètres suivants, puis appuyez sur Entrée :
   a) Pour le paramètre **Nom d'hôte du JobHistoryServer**, indiquez le nom d'hôte du noeud où le processus démon pour JobHistoryServer est exécuté.

   b) Pour le paramètre **Port du JobHistoryServer**, entrez le numéro de port associé au processus démon pour JobHistoryServer. Le numéro de port par défaut est 19888.

   c) Pour le paramètre **Nom d'hôte du NameNode supplémentaire**, indiquez le nom d'hôte du noeud où le processus démon pour un Namenode secondaire ou de secours est exécuté.

   d) Pour le paramètre **Port du NameNode supplémentaire**, indiquez le numéro de port associé au processus démon pour un Namenode secondaire ou de secours. Le numéro de port par défaut pour un Namenode secondaire est 50090. Pour un NameNode de secours, le numéro de port par défaut est 50070.

7. Facultatif : Lorsque la ligne de commande affiche le message suivant, entrez 1 pour ajouter les détails des gestionnaires de ressources de secours pour le cluster haute disponibilité, puis appuyez sur Entrée.
   `Standby ResourceManager(s) in Hadoop Cluster [ 1=Yes, 2=No ] (default is: 2):`
8. Lorsque la ligne de commande affiche le message suivant, entrez 1 et appuyez ensuite sur la touche Entrée pour surveiller les services Hadoop dans le cluster Hadoop géré par Ambari :
   `Monitoring of Hadoop services for Ambari based Hadoop installations [ 1=Yes, 2=No ] (default is: 2):`
   Sinon, conservez la valeur par défaut 2 et appuyez sur Entrée. Si vous vous activez la surveillance des services Hadoop, spécifiez une valeur pour chacun des paramètres suivants du serveur Ambari, puis appuyez sur Entrée :
   a) Pour le paramètre **Nom d'hôte du serveur Ambari**, entrez le nom de l'hôte sur lequel s'exécute le serveur Ambari.
   b) Pour le paramètre **Port serveur Ambari**, entrez le numéro de port associé au serveur Ambari. Le numéro de port par défaut est 8080.
   c) Pour le paramètre **Nom de l'utilisateur Ambari**, entrez le nom de l'utilisateur Ambari.
   d) Pour le paramètre **Mot de passe de l'utilisateur Ambari**, entrez le mot de passe de l'utilisateur Ambari.
9. Lorsque la ligne de commande affiche le message suivant, sélectionnez le niveau de trace Java approprié et appuyez sur Entrée :
   `This parameter allows you to specify the trace level used by the Java providers Java trace level [ 1=Off, 2=Error, 3=Warning, 4=Information, 5=Minimum Debug, 6=Medium Debug, 7=Maximum Debug, 8=All ] (default is: 2)`
10. Facultatif : Lorsque la ligne de commande affiche le message suivant, spécifiez les arguments pour la machine virtuelle Java et appuyez sur Entrée. La liste d'arguments doit être compatible avec la version de Java installée avec l'agent.
    `This parameter allows you to specify an optional list of arguments to the java virtual machine JVM arguments (default is:)`
11. Facultatif : Lorsque la ligne de commande affiche le message suivant, entrez 1 pour ajouter les détails des gestionnaires de ressources de secours suivants, puis appuyez sur Entrée :
    `Edit "Hadoop High Availability(HA) Cluster with Standby ResourceManagers" settings, [1=Add, 2=Edit, 3=Del, 4=Next, 5=Exit] (default is: 5): 1`
    a) Pour le paramètre **`Nom d'hôte du gestionnaire de ressources de secours`**, entrez le nom d'hôte du noeud où le processus démon pour le gestionnaire de ressources de secours est exécuté.
    b) Pour le paramètre **`Port du gestionnaire de ressources de secours`**, entrez le numéro de port associé au processus démon pour le gestionnaire de ressources de secours. Le numéro de port par défaut est 8088.
    c) Lorsque vous y êtes invité, entrez 1 pour ajouter d'autres gestionnaires de ressources de secours, puis répétez les étapes a et b, ou entrez 5 pour passer à l'étape suivante.

    - Pour éditer les paramètres de configuration d'un gestionnaire de ressources de secours en particulier, tapez 4 et appuyez sur Entrée jusqu'à ce que le nom d'hôte du gestionnaire de ressources de secours nécessaire s'affiche.
    - Pour retirer un gestionnaire de ressources de secours, tapez 3 et appuyez sur Entrée une fois que le nom d'hôte du gestionnaire de ressources de secours que vous voulez retirer est affiché.
12. Lorsque vous y êtes invité, entrez le chemin d'accès aux classes pour les fichiers JAR nécessaires pour le fournisseur de données API Java, puis appuyez sur Entrée.

    Les valeurs de configuration spécifiées sont sauvegardées et un message de confirmation s'affiche.
13. Exécutez la commande suivante pour démarrer l'agent : *`rép_install`*`/bin/hadoop-agent.sh start`

Que faire ensuite

1. Activez les événements de sous-noeud pour visualiser les seuils de génération d'événement de l'agent Hadoop. Pour plus d'informations sur l'activation des événements de sous-noeud, voir «Configuration du tableau de bord pour visualiser des événements Hadoop», à la page 269.
2. Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Pour certains paramètres, les valeurs par défaut sont fournies en commentaire. Vous pouvez spécifier des valeurs différentes pour ces paramètres et supprimer les balises de commentaire qui sont placées au début des paramètres.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'agent Hadoop sur les systèmes Linux, AIX et Windows.

Procédure

1. Ouvrez le fichier de réponses silencieux disponible à l'emplacement suivant : *rép_install* `\samples\hadoop_silent_config.txt`
2. Dans le fichier de réponses, procédez comme suit :
   a) Lorsque vous souhaitez surveiller le cluster Hadoop activé pour l'authentification basée sur Kerberos SPNEGO, spécifiez `yes` et entrez des valeurs pour les paramètres suivants :

   ```
   HADOOP_REALM_NAME
   HADOOP_KDC_HOSTNAME
   HADOOP_PRINCIPAL_NAME
   HADOOP_SPNEGO_KEYTAB
   ```

   b) Lorsque vous souhaitez surveiller le cluster Hadoop activé pour SSL, tapez `oui`, puis entrez des valeurs pour les paramètres suivants :

   ```
   HADOOP_TRUSTSTORE_PATH
   HADOOP_TRUSTSTORE_PASSWORD
   ```

   c) Entrez des valeurs pour les paramètres de cluster suivants des rôles NameNode (NN), ResourceManager (RM) et Job History Server (JHS) :

   ```
   HADOOP_CLUSTER_NAME (facultatif)
   HADOOP_NN_HOSTNAME
   HADOOP_NN_PORT
   HADOOP_RM_HOSTNAME
   HADOOP_RM_PORT
   HADOOP_JHS_HOSTNAME (facultatif)
   HADOOP_JHS_PORT (facultatif)
   ```

   d) Facultatif : Pour le paramètre **HADOOP_ADDITIONAL_NN_HOSTNAME**, spécifiez le nom d'hôte du NameNode de secours ou secondaire.
   e) Facultatif : Pour le paramètre **HADOOP_ADDITIONAL_NN_PORT**, spécifiez le numéro de port du NameNode de secours ou secondaire.

   A faire : Si le NameNode supplémentaire est un NameNode de secours, le numéro de port par défaut qui est associé au processus démon NameNode de secours est 50070. Si le NameNode supplémentaire est un NameNode secondaire, le numéro de port par défaut qui est associé au processus démon NameNode secondaire est 50090.
   f) Facultatif : Pour le paramètre **Hadoop_SRM**, indiquez `Yes` pour ajouter des gestionnaires de ressources (ResourceManager) de secours pour un cluster haute disponibilité, et passez à l'étape g.

g) Facultatif : Pour surveiller les services Hadoop du cluster Hadoop géré par Ambari, entrez les valeurs de chacun des paramètres suivants, puis appuyez sur Entrée :

```
AMBARI_SERVER_HOSTNAME
AMBARI_SERVER_PORT
USERNAME_OF_AMBARI_USER
PASSWORD_OF_AMBARI_USER
```

h) Pour le paramètre **JAVA_TRACE_LEVEL**, indiquez le niveau de trace approprié.

i) Facultatif : Pour le paramètre **JAVA_JVM_ARGS**, indiquez des arguments pour la machine virtuelle Java.

j) Facultatif : Ajoutez le nom d'hôte et le numéro de port d'un ResourceManager de secours au format suivant : HADOOP_SRM_PORT.*hadoop_srm_config_sec_1*=8088

Où *hadoop_srm_config_sec_1* est le nom d'hôte du noeud sur lequel le processus démon pour le ResourceManager de secours s'exécute, et 8088 est le numéro de port par défaut. Pour ajouter des ResourceManagers de secours, ajoutez le nom d'hôte et le numéro de port de chaque ResourceManager supplémentaire sur de nouvelles lignes, au même format.

3. Sauvegardez le fichier de réponses, puis exécutez la commande suivante :

   Linux AIX *rép_install*/bin/hadoop-agent.sh config *rép_install*/samples/hadoop_silent_config.txt

   Windows *rép_install*/bin/hadoop-agent.bat config *rép_install*/samples/hadoop_silent_config.txt

4. Démarrez l'agent :

   Linux AIX Exécutez la commande suivante : *rép_install*\bin\hadoop-agent.sh start

   Windows Cliquez avec le bouton droit de la souris sur **Monitoring Agent for Hadoop**, puis cliquez sur **Start**.

Que faire ensuite

1. Activez les événements de sous-noeud pour visualiser les seuils de génération d'événement de l'agent Hadoop. Pour plus d'informations sur l'activation des événements de sous-noeud, voir «Configuration du tableau de bord pour visualiser des événements Hadoop», à la page 269.
2. Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration du tableau de bord pour visualiser des événements Hadoop

Vous devez configurer le tableau de bord pour activer les événements de sous-noeud de sorte que l'onglet **Événements** puisse afficher des événements Hadoop.

Pourquoi et quand exécuter cette tâche

La valeur par défaut pour **Activer les événements sous-noeud** est "false". Modifiez cette valeur par "true" pour afficher les événements Hadoop.

Procédure

1. Ouvrez la console Cloud APM et accédez à **Configuration système**.
2. Sur la page **Configuration avancée**, cliquez sur **Intégration d'UI** sous **Catégories de configuration**.
3. Dans la liste **Activer les événements de sous-noeud**, sélectionnez **Vrai**.
4. Cliquez sur **Save**.

Attribution de droits aux utilisateurs non administrateurs

Sur les systèmes Windows, accordez le droit *Debug program* à un utilisateur non administrateur pour l'exécution de l'agent Hadoop. Ce droit est obligatoire pour pouvoir afficher des données dans les tableaux de bord de l'agent Hadoop.

Procédure

Procédez comme suit sur l'ordinateur où l'agent Hadoop est installé :

1. Cliquez sur **Démarrer > Panneau de configuration > Outils d'administration**.
2. Cliquez deux fois sur **Stratégie de sécurité locale**.
3. Dans le panneau Paramètres de sécurité, développez **Stratégies locales** et cliquez sur **Attribution des droits utilisateur**.
4. Cliquez avec le bouton droit de la souris sur **Déboguer les programmes** et sélectionnez **Propriétés**.
5. Cliquez sur **Ajouter un utilisateur ou un groupe** et ajoutez le nom de l'utilisateur non administrateur auquel vous voulez accorder ce droit.
6. Cliquez sur **OK**.

Que faire ensuite

Configurez et exécutez l'agent Hadoop en tant qu'utilisateur non administrateur.

Configuration de la surveillance de HMC Base

Monitoring Agent for HMC Base offre la possibilité de surveiller la console HMC (Hardware Management Console). Il surveille la disponibilité et la santé des ressources HMC : UC, mémoire, stockage et réseau. L'agent génère également des rapports sur l'inventaire et la configuration HMC des serveurs Power, des pools d'UC et des partitions logiques. Les utilisations de l'UC par les serveurs Power, les partitions logiques et les pools sont surveillées à l'aide des exemple de données de performances HMC.

Avant de commencer

Avant de configurer l'agent HMC Base, exécutez les tâches suivantes :

- Configurez la connexion SSH entre le système qui exécute l'agent et la console HMC. Pour plus d'informations, voir «Configuration de la connexion SSH», à la page 272.
- Préparez le SDK de la console HMC avant de démarrer la première instance d'agent. Pour plus d'informations, voir «Préparation du kit SDK pour HMC», à la page 273.

Procédure

- Pour configurer l'agent en éditant le fichier de réponses silencieux et en exécutant le script sans intervenir, procédez comme suit :
  1. Ouvrez le fichier `hmc_base_silent_config.txt` dans un éditeur de texte :
     - AIX *rép_install*`/samples/hmc_base_silent_config.txt`.
  2. Pour **`HMC Hostname`**, vous pouvez spécifier l'adresse IP ou le nom d'hôte.
  3. Pour **`HMC Username`**, vous devez entrer le nom de l'utilisateur de connexion de la console HMC. Par exemple, **`HMC_USERNAME=`** *hscroot*.

     Remarque : Le nom de l'utilisateur de connexion que vous affectez à la console HMC requiert au minimum les droits hscviewer.
  4. Pour **`HMC Password`**, vous devez saisir le mot de passe de l'utilisateur.
  5. Pour **`Maximum Number of Data Provider Log Files:`**, vous devez spécifier le nombre maximal de fichiers journaux de fournisseur de données créés. Par exemple, **`KPH_LOG_FILE_MAX_COUNT=`***10*.

6. Pour **Maximum Size in KB of Each Data Provider Log**, vous devez entrer la taille maximale en kilooctets qu'un fichier journal de fournisseur de données peut atteindre avant qu'un nouveau fichier journal ne soit créé. Par exemple, **KPH_LOG_FILE_MAX_SIZE=** *5190*.
7. Pour **Level of Detail in Data Provider Log**, vous devez entrer la quantité de détails que le fournisseur de données inclut dans les fichiers journaux du fournisseur de données. Par exemple, **KPH_LOG_LEVEL=***Fine*. Vous devez spécifier l'une des valeurs suivantes :
   - 1= Off
   - 2=Severe
   - 3=Warning
   - 4=Info
   - 5=Fine
   - 6=Finer
   - 7=Finest
   - 8=All

   Important : La valeur par défaut est 4.
8. Sauvegardez et fermez le fichier `hmc_base_silent_config.txt`, puis entrez : `./hmc_base-agent.sh config` *`nom_instance rép_install`*`/samples/hmc_base_silent_config.txt`, *nom_instance* représentant le nom que vous souhaitez affecter à l'instance et *rép_install*, le répertoire d'installation de l'agent HMC Base. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.

- AIX Pour configurer l'agent en répondant à des invites, procédez comme suit :

1. Ouvrez le répertoire *`rép_install`*`/bin`, où *rép_install* est le répertoire d'installation de l'agent HMC Base.
2. Pour configurer agent HMC Base, exécutez la commande **./hmc_base-agent.sh config instance_name**.
3. Lorsque le système demande de **modifier les paramètres de Monitoring Agent for HMC Base**, appuyez sur **Entrée**. La valeur par défaut est `Oui`.
4. Pour entrer les informations de configuration de la console HMC, procédez comme suit :
   a. Lorsque le système vous demande le **nom d'hôte HMC**, tapez le nom d'hôte ou l'adresse IP et appuyez sur **Entrée**.
   b. Lorsque le système vous demande le **nom d'utilisateur HMC**, entrez le nom de l'utilisateur de connexion associé à la console HMC, puis appuyez sur **Entrée**.
5. Lorsque vous y êtes invité, saisissez dans **HMC Password** le mot de passe de l'utilisateur.
6. Pour entrer les informations sur le fournisseur de données, procédez comme suit :
   a. Lorsque le système vous demande le **nombre maximal de fichiers journaux de fournisseur de données**, entrez-le, puis appuyez sur **Entrée**.

      Le nombre maximal par défaut de fichiers journaux de fournisseur de données est de 10.
   b. Lorsque le système vous demande le **la taille maximale en kilooctets de chaque journal de fournisseur de données**, entrez-la, puis appuyez sur **Entrée**.

      la taille maximale par défaut en kilooctets est de 5190.
   c. Lorsque le système vous demande le **niveau de détail dans le journal de fournisseur de données**, entrez l'un des niveaux suivants, puis appuyez sur **Entrée** :
      - 1= Off
      - 2=Severe
      - 3=Warning
      - 4=Info

- 5=Fine
- 6=Finer
- 7=Finest
- 8=All

Que faire ensuite

- Pour démarrer l'agent, entrez : `./hmc_base-agent.sh start NomInstance`.
- Configurez le serveur de la console HMC selon les instructions de la rubrique «Configuration du serveur de la console HMC pour la surveillance des entrées-sorties virtuelles», à la page 274 pour la surveillance des entrées-sorties virtuelles.
- Activez la surveillance de l'utilisation de l'UC et de la mémoire selon les instructions de la rubrique «Activation de la surveillance de l'utilisation d'UC et de mémoire», à la page 275.

Configuration de la connexion SSH

Vous devez installer la connexion SSH entre le système qui exécute l'agent et la console HMC pour que celui-ci collecte des données.

Pourquoi et quand exécuter cette tâche

Le fournisseur de données d'agent collecte des données à partir de la console de gestion en exécutant des commandes CLI via SSH. Par défaut, le fournisseur de données patiente pendant 1 minute pour l'exécution de la commande CLI. Passé ce délai, le fournisseur de données ferme la session SSH dans laquelle la commande CLI est en cours d'exécution, et aucune des données de cette commande n'est disponible dans les ensembles de données de l'agent jusqu'à ce que la commande aboutisse. Le chemin par défaut de la commande SSH est `/usr/bin/ssh`. Si SSH est installé à un autre emplacement, spécifiez le chemin d'accès à l'aide de la variable d'environnement **KPH_SSH_PATH**.

Procédure

Utilisez l'une des méthodes ci-après pour configurer la connexion SSH.

- Utilisez le script `setup_hmc_key.pl` pour configurer la connexion SSH.
  a) Ouvrez une session sur le serveur sur lequel l'agent est installé.
  b) Ouvrez le répertoire `rép_install/aix526/ph/bin`, `rép_install` correspondant au répertoire d'installation de l'agent HMC Base.
  c) Exécutez la commande `perl setup_hmc_key.pl`.
  d) Répondez aux invites et indiquez le nom d'hôte ou l'adresse IP de la console HMC, le nom d'utilisateur de la console HMC (qui doit avoir des droits d'accès équivalents à `hscviewer`) et le mot de passe pour créer la paire de clés.
  e) Après avoir créé la paire de clés, testez la connectivité en exécutant une commande telle que `ssh hscroot@hmchost lshmc -V`.
  Si SSH se connecte à la console HMC pour la première fois, ajoutez la console HMC au fichier `ssh known_hosts` en répondant `yes` au message suivant :

```
The authenticity of host 'hmchost (3.3.333.333)' can't be established.
RSA key fingerprint is 4c:b4:26:27:38:f3:ec:58:01:92:26:f9:61:32:bb:4d.
Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added 'hmchost,3.3.333.333' (RSA) to the list of known hosts.
```

  L'agent peut désormais utiliser SSH pour collecter des données à partir de la console HMC.
- Utilisez l'utilitaire `ssh-keygen` pour générer des clés et configurer la connexion SSH.
  a) Ouvrez une session sur le serveur sur lequel l'agent est installé.
  b) Générez des clés publiques et privées, sans paraphrase, à l'aide de l'utilitaire `ssh-keygen`. Par exemple, la commande suivante génère un ensemble de clés publiques et de clés privées :

```
ssh-keygen -t rsa -f /.ssh/id-rsa
```

Appuyez sur Entrée lorsque vous êtes invité à entrer une paraphrase. La clé publique générée est stockée dans le fichier /.ssh/id-rsa.pub. La clé privée est stockée dans le fichier /.ssh/id-rsa.

c) Transférez le fichier qui contient la clé publique à l'ordinateur HMC à l'aide d'utilitaires tels que scp.

d) Sur l'ordinateur HMC, ajoutez le fichier de clés publiques à la collection de clés stockées sur la console HMC.

Les clés sont sauvegardées dans le fichier /.ssh/authorized_keys2.

e) Ajoutez le nom d'hôte et la clé de la console HMC au fichier known_hosts.

Ce fichier se trouve dans le répertoire /.ssh.

a. Exécutez la commande ssh "user"@"hmc_hostname" -i "private_keyfile" date.

b. Indiquez yes pour placer les clés dans la mémoire cache. Cette commande ajoute l'entrée au fichier known_hosts pour les connexions ultérieures.

f) Exécutez la commande ssh "user"@"hmc_hostname" date.

Si la date est renvoyée sans l'invite de mot de passe, les clés SSH ont été correctement installées.

Préparation du kit SDK pour HMC

Vous devez préparer le kit SDK pour HMC avant de démarrer l'instance d'agent pour la première fois.

Pourquoi et quand exécuter cette tâche

Avant de démarrer votre première instance d'agent, vous devez préparer la version correspondante du kit SDK pour HMC. Une fois la préparation terminée, il n'est pas nécessaire de répéter cette tâche pour une autre instance de l'agent HMC Base que vous créez pour la console HMC au même niveau de version. Pour surveiller une autre version de la console HMC, répétez cette tâche pour préparer à nouveau le kit SDK.

Procédure

- A partir du répertoire *agent_dir*/aix526/ph/bin, exécutez l'outil de script **prepareSDK.sh** pour préparer automatiquement le kit SDK pour HMC.
  - Si le message SDK is ready for HMC s'affiche, la préparation est terminée.
  - S'il n'apparaît pas, vous pouvez préparer manuellement le kit SDK pour HMC.

    Pour HMC version 8.5.0, procédez comme suit :

    1. Utilisez un navigateur pour télécharger le kit SDK pour HMC directement avec l'URL suivante :

       ```
       https://IP_HMC:12443/rest/api/web/sdk
       ```

       Lorsque vous y êtes invité, entrez le nom d'utilisateur et le mot de passe du compte hscroot. Le nom du fichier SDK est au format pmc_sdk_*.zip.

    2. . Décompressez le fichier zip du kit SDK et accédez au répertoire IBM HMC REST Web Services SDK Runtime/lib/ibm3.

    3. S'il n'existe pas, créez un sous-répertoire <rép_agent>/aix526/ph/lib/*ma_version_hmc*, où *ma_version_hmc* est la version de votre environnement HMC (par exemple, 8502). Pour déterminer la version de votre environnement HMC, exécutez la commande suivante :

       ```
       ssh hscroot@<HMC_IP> 'lshmc -v' | grep RM |
       awk -FR '{print $3}' | tr -d '.'
       ```

4. Copiez tous les fichiers `.jar` du dossier `IBM HMC REST Web Services SDK Runtime/lib/ibm3` du kit SDK pour HMC dans le répertoire *rép_agent*`/aix526/ph/lib/`*version_HMC*.

Pour HMC V8.6.0 ou V8.7.0, procédez comme suit :

1. Utilisez un navigateur pour télécharger le kit SDK de HMC directement avec l'URL suivante :

   ```
   https://IP_HMC:12443/rest/api/web/sdk
   ```

   Lorsque vous y êtes invité, entrez le nom d'utilisateur et le mot de passe du compte `hscroot`. Le nom du fichier SDK est au format `pmc-rest-sdk*.zip`.
2. Décompressez ce fichier et accédez au sous-répertoire `lib`.
3. S'il n'existe pas, créez un sous-répertoire `<rép_agent>/aix526/ph/lib/`*ma_version_hmc*, où *ma_version_hmc* est la version de votre environnement HMC (par exemple, 8602 ou 87012). Pour déterminer la version de votre environnement HMC, exécutez la commande suivante :

   ```
   ssh hscroot@<HMC_IP> 'lshmc -v' | grep RM |
   awk -FR '{print $3}' | tr -d '.'
   ```
4. Copiez tous les fichiers `.jar` du dossier `lib` du kit SDK pour HMC dans le répertoire *rép_agent*`/aix526/ph/lib/`*ma_version_hmc*.

Résultats
Vous avez préparé le kit SDK pour HMC.

Que faire ensuite
Configurez l'agent HMC Base conformément aux instructions fournies dans «Configuration de la surveillance de HMC Base», à la page 270.

Configuration du serveur de la console HMC pour la surveillance des entrées-sorties virtuelles

Avant que l'agent HMC Base puisse surveiller le statut des entrées-sorties virtuelles, vous devez configurer le serveur de la console HMC.

Procédure

Pour configurer le serveur de la console HMC conformément aux prérequis de l'agent HMC Base afin de surveiller les entrées-sorties virtuelles, procédez comme suit.

- Activez la fonction PMC du serveur de la console HMC et des serveurs virtuels d'entrée-sortie.
  a) Connectez-vous au serveur de la console HMC en utilisant le navigateur en mode classique.

     ```
     https://nomhôte_hmc
     ```

  b) Cliquez sur **HMC Management** > **Change Performance Monitoring Settings**.
     La fenêtre **Change Performance Monitoring Settings** s'affiche.
  c) Dans la section **Performance Monitoring Data Collection for Manage Servers**, activez la fonction **Collection** pour les serveurs correspondants.
  d) Cliquez sur chaque serveur virtuel d'entrée-sortie pour afficher la fenêtre **Partition Properties** pour ce serveur.
  e) Dans l'onglet **General**, vérifiez que la case de l'option **Allow performance information collection** est cochée.
     Cliquez sur **OK** pour sauvegarder les paramètres.

  Après plusieurs minutes, vous pouvez visualiser le trafic réseau et de stockage des serveurs correspondants sur la page **Performance Monitoring**.

- Vérifiez que l'utilisateur HMC de l'agent HMC Base possède le privilège correct.
  a) Lorsque vous ajoutez ou éditez l'utilisateur, vérifiez que l'utilisateur possède le rôle **hmcviewer** et que l'option **AllSystemResource** est activée pour cet utilisateur.
  b) Dans la fenêtre **User Properties**, activez l'option **Allow remote access via the web**.

Activation de la surveillance de l'utilisation d'UC et de mémoire

Si la collecte de données d'utilisation d'UC et de mémoire est désactivée, les données d'utilisation d'UC et de mémoire de chaque serveur d'alimentation ne s'affichent pas dans l'interface utilisateur.

Procédure

Utilisez l'une des méthodes suivantes pour activer la surveillance de l'utilisation d'UC et de mémoire.

- Activez la surveillance de l'utilisation d'UC et de mémoire en exécutant la commande de gestion HMC `chlparutil`.

```
chlparutil-r config -m <nomCEC> -s <taux d'échantillonnage en secondes, toujours 60>
```

- Activez la surveillance de l'utilisation de l'UC et de la mémoire sur le serveur de la console HMC.
  a) Connectez-vous au serveur de la console HMC en mode classique.
  b) Cliquez sur le noeud **Servers** dans l'arborescence de navigation.
  c) Sélectionnez le serveur et accédez à **Operations** > **Utilization Data** > **Change the Sample rate**.
  d) Définissez une fréquence d'échantillonnage.
  La fréquence d'échantillonnage est désactivée par défaut. Vous pouvez définir la fréquence à l'aide de valeurs appropriées, par exemple `30 minutes`.

Configuration de la surveillance de HTTP Server

Monitoring Agent for HTTP Server est automatiquement lancé après l'installation. Pour activer la collecte de données, assurez-vous que le serveur HTTP est en cours d'exécution et éditez le fichier de configuration du serveur HTTP de sorte qu'il inclue une référence au fichier de configuration du collecteur de données de l'agent HTTP Server.

Avant de commencer

Deux fichiers font partie de la configuration de l'agent HTTP Server. Pour visualiser des exemples de ces fichiers, voir Exemples. Localisez et consultez les fichiers suivants :

Fichier de configuration du collecteur de données de l'agent HTTP Server

Après avoir installé l'agent HTTP Server, ce dernier découvre le serveur HTTP et génère un fichier de configuration du collecteur de données dans le répertoire *rép_install*/tmp/khu, où *rép_install* est le répertoire d'installation de l'agent HTTP Server.

Si votre environnement contient plusieurs serveurs HTTP, un fichier de configuration d'agent HTTP Server est généré par serveur HTTP.

Le nom du fichier de configuration de l'agent HTTP Server se compose de deux parties au format suivant :

```
khu.chemin d'accès complet/nom du fichier de configuration du serveur HTTP.conf
```

La première partie du nom du fichier de configuration d'agent est khu, où hu est le code agent du serveur HTTP.

La seconde partie du nom du fichier de configuration d'agent est créée en utilisant le chemin d'accès complet et le nom du fichier de configuration du serveur HTTP, où / est remplacé par . . Par exemple, voici des noms de fichier possibles :

Linux AIX `khu.usr.local.apache24.conf.httpd.conf`

Windows `khu.C.Program Files.IBM.HTTPServer.conf.httpd.conf`

Le fichier de configuration du collecteur de données de l'agent HTTP Server contient les éléments suivants :

- Détails sur le chemin d'accès du fichier httpd.conf utilisé par HTTP Server. Par exemple, `KhuShmemPath "/IBM/HTTPServer/conf/httpd.conf"`.
- Emplacement de la bibliothèque à charger
- Droits d'accès associés à la mémoire partagée

Fichier de configuration du serveur HTTP

Chaque serveur HTTP possède un fichier de configuration qui se nomme *rép_install_serveur_http*`/conf/httpd.conf` par défaut, où *rép_install_serveur_http* désigne le répertoire d'installation du serveur HTTP. Dans certains environnements, ce nom de fichier peut être personnalisé. Vérifiez le nom de fichier exact auprès de l'administrateur du serveur HTTP.

Pourquoi et quand exécuter cette tâche

Activez la collecte de données sur l'agent HTTP Server dans les cas suivants :

- Après avoir installé l'agent HTTP Server
- Après avoir effectué une mise à niveau vers la version 1.0.0.4 de l'agent HTTP Server, le nouvel alias bascule les noeuds existants de l'agent HTTP Server hors ligne dans la console Cloud APM.
- Après avoir effectué une mise à niveau de la version 1.0.0.4, les noeuds existants de l'agent HTTP Server peuvent basculer hors ligne dans la console Cloud APM. Cette situation peut se produire si vous disposez de plusieurs instances du serveur HTTP portant des noms de fichier de configuration d'agent similaires, par exemple `httpd` et `httpd01`.

L'outil réseau de ligne de commande netstat permet à l'agent HTTP Server de reconnaître le serveur HTTP en cours d'exécution.

Important : Pour résoudre ce problème, vous devez ajouter la nouvelle instance du serveur HTTP dans la console Cloud APM une fois cette tâche terminée.

Procédure

1. Pour activer la collecte de données, vous devez référencer le fichier de configuration du collecteur de données dans le fichier de configuration du serveur HTTP en utilisant l'instruction `Include`. Ajoutez l'instruction suivante à la fin du fichier de configuration du serveur HTTP :

   ```
   Include "rép_install/tmp/khu/khu.chemin d'accès complet au nom du fichier de configuration du serveur HTTP.conf"
   ```

   Par exemple,

   Linux AIX Si IBM HTTP Server est installé dans le répertoire `/opt/IBM/HTTPServer` et que le fichier de configuration du collecteur de données se trouve dans le répertoire suivant :

   ```
   /opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf
   ```

   Ajoutez l'instruction suivante au fichier de configuration du serveur HTTP `/opt/IBM/HTTPServer/conf/httpd.conf` :

   ```
   Include "/opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf"
   ```

Windows Si un serveur IBM HTTP est installé dans le répertoire `C:\ProgramFiles\IBM\HTTPServer` et que le fichier de configuration du collecteur de données se trouve dans le répertoire

```
C:\IBM\APM\tmp\khu\khu.C.Program Files.IBM.HTTPServer.conf.httpd.conf,
```

ajoutez l'instruction suivante dans le fichier de configuration du serveur HTTP `C:\Program Files\IBM\HTTPServer\conf\httpd.conf` :

```
Include “C:\IBM\APM\tmp\khu\khu.C.Program Files.IBM.HTTPServer.conf.httpd.conf”
```

2. Accédez au répertoire suivant :

```
répertoire_installation_serveur_HTTP/bin
```

3. Redémarrez le serveur HTTP. Par exemple :

Linux AIX

```
./apachectl -k stop
./apachectl -k start
```

Windows

```
httpd.exe -k stop
httpd.exe -k start
```

Résultats
Vous avez correctement configuré l'agent.

Que faire ensuite
Vous pouvez à présent vérifier que les données de l'agent HTTP Server s'affichent dans la console Cloud APM. Pour obtenir des instructions de démarrage de la console Cloud APM, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.

Remarque : Si le trafic est inexistant sur le serveur HTTP, aucune donnée ne s'affichera dans la console Cloud APM.

module IBM HTTP Server Response Time

Lorsque vous installez l'agent Response Time Monitoring pour qu'il fonctionne avec le module IBM HTTP Server Response Time, il surveille les demandes HTTP et HTTPS sur tous les ports.

module IBM HTTP Server Response Time
Le module IBM HTTP Server Response Time fait partie de l'agent HTTP Server. Si l'agent HTTP Server est installé et configuré avant ou en même temps que l'agent Response Time Monitoring sur le serveur Apache HTTP Server ou sur le serveur IBM HTTP Server sous AIX, Linux ou Windows, le module IBM HTTP Server Response Time est automatiquement activé. Pour une description de la fonctionnalité du module IBM HTTP Server Response Time, voir «Configuration de l'module IBM HTTP Server Response Time», à la page 714.

Fichier de configuration du collecteur de données
Après avoir installé l'agent HTTP Server, ce dernier découvre le serveur HTTP et génère un fichier de configuration du collecteur de données dans le répertoire *rép_install*`/tmp/khu`, où *rép_install* est le répertoire d'installation de l'agent HTTP Server.

Pour le serveur Apache HTTP Server, le fichier de configuration du collecteur de données est : `khu.usr.local.apache24.conf.httpd.conf`
Pour le serveur IBM HTTP Server, le fichier de configuration du collecteur de données est : `khu.opt.IBM.HTTPServer.conf.httpd.conf`

Plug-ins
L'agent HTTP Server est composé de deux plug-in :

1. khu_module - correspond à l'agent HTTP Server. Ce plug-in est responsable de tous les tableaux de bord associés à l'agent HTTP Server. Pour plus d'informations, voir agent HTTP Server Reference.
2. wrt_module - correspond au module IBM HTTP Server Response Time

Ces deux plug-in sont indiqués dans le fichier de configuration de collecteur de données comme suit :

```
LoadModule khu_module

LoadModule wrt_module
```

Activer la collecte de données

Pour activer la collecte de données, vous devez référencer le fichier de configuration du collecteur de données dans le fichier de configuration du serveur HTTP en utilisant l'instruction Include. Ajoutez l'instruction suivante à la fin du fichier de configuration du serveur HTTP :

```
include /opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf
```

Pour plus d'informations, voir «Configuration de la surveillance de HTTP Server», à la page 275.

Une fois la collecte de données activée, le tableau de bord de l'utilisateur final est rempli.

Exemples de code pour l'agent HTTP Server

Deux fichiers font partie de la configuration de l'agent HTTP Server. Il s'agit du fichier de configuration du collecteur de données de l'agent HTTP Server et du fichier de configuration du serveur HTTP. Un exemple de fichier de mappage de l'alias d'instance est également fourni pour vous aider à comprendre le fonctionnement d'un alias.

Exemples de fichier du collecteur de données de l'agent HTTP Server

Pour IBM HTTP Server version 8 et ultérieure, 64 bits, le fichier de configuration du collecteur de données de l'agent HTTP Server contient les informations suivantes :

```
#
#Paramètres du module Monitoring Agent for HTTP Server.
#

LoadModule khu_module "/tmp/ihs/lx8266/hu/lib/khuapache22dc_64.so"

<IfModule mod_khu.c>
   KhuShmemPerm 660
   KhuShmemPath "/opt/IBM/IHS/conf/httpd.conf"
   KhuCpsPath "/tmp/ihs/tmp/khu/khu_cps.properties"
</IfModule>

Alias /khu "/tmp/ihs/lx8266/hu/etc"
<Directory "/tmp/ihs/lx8266/hu/etc">
  Order deny,allow
  Allow from all
  #Require all granted
</Directory>

LoadModule wrt_module /tmp/ihs/lx8266/hu/lib/mod_wrt_ap22_64.so
WrtOriginID HU:tivvm09_httpd:HUS
```

Pour IBM HTTP Server version 7, 32 bits, le fichier de configuration contient les informations suivantes :

```
#
#Paramètres du module Monitoring Agent for HTTP Server.
#

LoadModule khu_module "/tmp/ihs/lx8266/hu/lib/khuapache22dc_32.so"

<IfModule mod_khu.c>
 KhuShmemPerm 660
 KhuShmemPath "/opt/IBM/HTTPServer/conf/httpd.conf"
 KhuCpsPath "/tmp/ihs/tmp/khu/khu_cps.properties"
```

```
</IfModule>

Alias /khu "/tmp/ihs/lx8266/hu/etc"
<Directory "/tmp/ihs/lx8266/hu/etc">
  Order deny,allow
  Allow from all
  #Require all granted
</Directory>

LoadModule wrt_module /tmp/ihs/lx8266/hu/lib/mod_wrt_ap22.so
WrtOriginID HU:linux_httpd:HUS
```

Pour Apache version 2.4, 64 bits, le fichier de configuration de l'agent HTTP Server contient les informations suivantes :

```
#
# Settings for Monitoring Agent for HTTP Server module.
#

LoadModule khu_module "/tmp/ihs/lx8266/hu/lib/khuapache24dc_64.so"

<IfModule mod_khu.c>
 KhuShmemPerm 660
 KhuShmemPath "/usr/local/apache24/conf/httpd.conf"
</IfModule>

Alias /khu "/tmp/ihs/lx8266/hu/etc"
<Directory "/tmp/ihs/lx8266/hu/etc">
  Order deny,allow
  Allow from all
  Require all granted
</Directory>

LoadModule wrt_module /tmp/ihs/lx8266/hu/lib/mod_wrt_ap24_64.so
WrtOriginID HU:linux-tzsi_httpd:HUS
```

Exemple de fichier de mappage de l'alias d'instance

```
# Monitoring Agent for HTTP Server instance alias mapping
# INSTANCE: auto discovered by agent. Please do NOT modify.
# ALIAS: alias name for the instance. The name will be displayed in APM UI dashboard. It
must be unique
# among all instances and it must be less than 10 characters and consist of only
alphanumeric characters.
#
INSTANCE.1=/usr/local/apache24/conf/httpd.conf
ALIAS.1=httpd

INSTANCE.1=/usr/local/apache24/conf/admin.conf
ALIAS.1=admin
```

Configuration de la surveillance d'IBM Cloud

Monitoring Agent for IBM Cloud collecte l'inventaire de machine virtuelle et les métriques auprès de votre compte IBM Cloud (SoftLayer). L'agent IBM Cloud permet de suivre le nombre de périphériques virtuels que vous avez configurés et qui sont en cours d'exécution dans IBM Cloud. Vous pouvez visualiser les ressources allouées à chaque périphérique virtuel sur la page du tableau de bord détaillé, qui contient également certaines informations telles que le centre de données dans lequel se trouve un périphérique, le système d'exploitation et la bande passante de réseau public prévisionnelle pour le mois.

Avant de commencer

- Lisez l'intégralité de la rubrique «Configuration de la surveillance d'IBM Cloud», à la page 279 pour déterminer les éléments nécessaires à l'achèvement de la configuration.
- Les instructions figurant dans cette rubrique concernent l'édition la plus récente de l'agent, sauf indication contraire.

- Assurez-vous que votre environnement possède la configuration système requise pour l'agent IBM Cloud. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent IBM Cloud.
- Vérifiez que les informations suivantes sont disponibles :
  - Nom d'utilisateur pour un utilisateur disposant au moins des droits d'auditeur.
  - Clé d'API pour IBM Cloud pour l'utilisateur associé.

Pourquoi et quand exécuter cette tâche

L'agent IBM Cloud est à la fois un agent à plusieurs instances et un agent de sous-noeud. Après avoir configuré les instances d'agent, démarrez chacune d'elles manuellement.

Procédure

1. Configurez l'agent sur des systèmes Windows avec la fenêtre **IBM Performance Management** ou le fichier de réponses silencieux.
   - «Configuration de l'agent sur des systèmes Windows», à la page 280.
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 281.
2. Configurez l'agent sur des systèmes Linux avec le script qui génère des invites pour les réponses ou le fichier de réponses silencieux.
   - «Configuration de l'agent en répondant à des invites», à la page 281.
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 281.

Que faire ensuite

Dans la console Cloud APM, accédez à votre Tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Pour identifier et résoudre les incidents, reportez-vous au forum Cloud Application Performance Management.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent IBM Cloud sur les systèmes d'exploitation Windows dans la fenêtre IBM Cloud Application Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur le modèle **Monitoring Agent for IBM Cloud**, puis cliquez sur **Configure agent**.

   A faire : Une fois qu'une instance d'agent a été configurée, l'option **Configure agent** n'est pas disponible. Pour reconfigurer l'instance d'agent, cliquez dessus avec le bouton droit de la souris, puis cliquez sur **Reconfigure...**.

3. Entrez un nom d'instance unique, puis cliquez sur **OK**. N'utilisez que des lettres latines, des chiffres arabes, le caractère de soulignement et le caractère moins dans le nom de l'instance. Par exemple, `icloud-inst`.
4. Cliquez sur **Suivant** dans la fenêtre du nom d'instance de l'agent.
5. Cliquez sur **Nouveau**, entrez le nom d'utilisateur et les paramètres de clé de l'API IBM Cloud SoftLayer, puis cliquez sur **Suivant**.
6. Cliquez sur **OK** pour terminer la configuration.
7. Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur l'instance que vous avez configurée, puis cliquez sur **Démarrer**.

Configuration de l'agent en répondant à des invites

Après avoir installé l'agent IBM Cloud, vous devez le configurer pour pouvoir le démarrer. Si l'agent IBM Cloud est installé sur un ordinateur Linux, vous pouvez suivre ces instructions pour le configurer de manière interactive en suivant des invites de ligne de commande.

Pourquoi et quand exécuter cette tâche

A faire : Si vous reconfigurez une instance d'agent configurée, la valeur définie dans la dernière configuration s'affiche pour chaque paramètre. Pour effacer une valeur existante, appuyez sur la touche Espace lorsque le paramètre s'affiche.

Procédure

Procédez comme suit pour configurer l'agent IBM Cloud en exécutant un script et en répondant aux invites.

1. Exécutez la commande suivante :

   ```
   rép_install/bin/ibm_cloud-agent.sh config nom_instance
   ```

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent.

   Exemple

   ```
   /opt/ibm/apm/agent/bin/ibm_cloud-agent.sh config icloud-inst
   ```

2. Répondez aux invites pour définir les valeurs de configuration de l'agent.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'agent IBM Cloud», à la page 283.

3. Exécutez la commande suivante pour démarrer l'agent :

   ```
   rép_install/bin/ibm_cloud-agent.sh start nom_instance
   ```

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

   Exemple

   ```
   /opt/ibm/apm/agent/bin/ibm_cloud-agent.sh start icloud-inst
   ```

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de

configuration pour créer une instance et mettre à jour les valeurs de configuration de l'agent. Ce mode de configuration est appelé mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

- Configurez l'agent IBM Cloud en mode silencieux :
  a) Ouvrez le fichier `ibm_cloud_silent_config.txt` qui se trouve dans l'un des chemins ci-après, dans un éditeur de texte.
     – Linux *rép_install*`/samples/ibm_cloud_silent_config.txt`

       Par exemple, `/opt/ibm/apm/agent/samples/ibm_cloud_silent_config.txt`
     – Windows *rép_install*`\samples\ibm_cloud_silent_config.txt`

       Par exemple, `C:\IBM\APM\samples\ibm_cloud_silent_config.txt`

     où *rép_install* représente le chemin d'installation de l'agent.
  b) Dans le fichier `ibm_cloud_silent_config.txt`, spécifiez des valeurs pour tous les paramètres obligatoires et modifiez les valeurs des autres paramètres si nécessaire.

     Voir «Paramètres de configuration de l'agent IBM Cloud», à la page 283 pour obtenir une description de chaque paramètre de configuration.
  c) Sauvegardez et fermez le fichier `ibm_cloud_silent_config.txt` et exécutez la commande suivante :
     – Linux *rép_install*`/bin/ibm_cloud-agent.sh config` **nom_instance** *rép_install*`/samples/ibm_cloud_silent_config.txt`

       Par exemple, **/opt/ibm/apm/agent/bin/ibm_cloud-agent.sh config icloud-inst /opt/ibm/apm/agent/samples/ibm_cloud_silent_config.txt**
     – Windows *rép_install*`\bin\ibm_cloud-agent.bat config` **nom_instance** *rép_install*`\samples\ibm_cloud_silent_config.txt`

       Par exemple, **C:\IBM\APM\bin\ibm_cloud-agent.bat config icloud-inst C:\IBM\APM\samples\ibm_cloud_silent_config.txt**

     où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent.

     Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.
  d) Exécutez la commande suivante pour démarrer l'agent :
     – Linux *rép_install*`/bin/ibm_cloud-agent.sh start` **nom_instance**

       Par exemple, **/opt/ibm/apm/agent/bin/ibm_cloud-agent.sh start icloud-inst**
     – Windows *rép_install*`\bin\ibm_cloud-agent.bat start` **nom_instance**

       Par exemple, **C:\IBM\APM\bin\ibm_cloud-agent.bat start icloud-inst**

     où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

Paramètres de configuration de l'agent IBM Cloud

Les paramètres de configuration de l'agent IBM Cloud sont regroupés dans un tableau.

1. IBM Cloud Configuration - Paramètres de la surveillance à distance des instances IBM Cloud. Les instances sont automatiquement reconnues pour la clé d'API que vous souhaitez configurer.

Tableau 23. Configuration d'IBM Cloud

Nom de paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Nom d'utilisateur	Nom d'utilisateur du compte IBM SoftLayer utilisé pour extraire les métriques de l'API IBM Cloud.	**KFS_USERNAME**
Clé d'API	Clé d'API spécifique à l'utilisateur qui est requise pour terminer l'authentification. Les clés d'API sont générées et peuvent être extraites du portail client IBM SoftLayer.	**KFS_API_KEY_PASSWORD**

Configuration de la surveillance d'IBM Integration Bus

L'agent IBM Integration Bus est un agent multi-instance. Vous devez créer une première instance d'agent et la démarrer manuellement.

Avant de commencer

- Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.
- Assurez-vous que votre environnement possède la configuration système requise pour l'agent IBM Integration Bus. Pour les toutes dernières informations sur la configuration système requise, voir le rapport détaillé sur la configuration système requise pour l'agent IBM Integration Bus.

Pourquoi et quand exécuter cette tâche

La procédure suivante, qui inclut des étapes obligatoires et facultatives, permet de configurer l'agent IBM Integration Bus. Effectuez les étapes nécessaires en fonction de vos besoins.

Procédure

1. Assurez-vous que l'ID utilisateur qui sera utilisé pour démarrer et arrêter l'agent IBM Integration Bus appartient aux groupes d'utilisateurs **mqm** et **mqbrkrs**.
2. Windows
   Si IBM MQ (WebSphere MQ) est installé sur le système Windows, ajoutez le chemin d'accès à la bibliothèque IBM MQ (WebSphere MQ) à la variable d'environnement **PATH**. L'agent IBM Integration Bus pourra ainsi charger les bibliothèques IBM MQ (WebSphere MQ) requises pour démarrer.
   a) Ajoutez le chemin d'accès à la bibliothèque IBM MQ (WebSphere MQ) au début de la variable d'environnement **PATH**.

      Par exemple, si le chemin d'installation d'IBM MQ (WebSphere MQ) est `C:\IBM\WMQ75`, ajoutez `C:\IBM\WMQ75\bin` au début de la variable d'environnement **PATH** de votre système Windows.
   b) Redémarrez le système Windows pour que les modifications soient prises en compte.

3. Configurez l'agent IBM Integration Bus en spécifiant les paramètres de configuration suivants. Vous pouvez également spécifier des paramètres de configuration facultatifs pour l'agent. Pour des instructions détaillées, voir «Configuration de l'agent IBM Integration Bus», à la page 284.
   - ID de l'agent
   - Répertoire d'installation des noeuds d'intégration (courtiers) à surveiller
   - Chemin d'accès à la bibliothèque 64 bits d'IBM MQ (WebSphere MQ)
4. Configurez IBM Integration Bus pour activer les données que vous voulez surveiller. Voir «Configuration d'IBM Integration Bus pour l'activation des données», à la page 288 .
5. Si vous avez activé la collecte de données d'image instantanée pour votre noeud d'intégration (courtier), configurez l'agent IBM Integration Bus de sorte à ne pas stocker les données d'image instantanée. Pour obtenir des instructions, voir «Désactivation de la collecte de données d'image instantanée pour l'agent», à la page 295.
6. Facultatif : Pour configurer l'agent IBM Integration Bus afin d'activer le suivi des transactions, utilisez la page **Configuration d'agent**. Pour plus d'informations, voir «Configuration du suivi des transactions pour l'agent IBM Integration Bus», à la page 296.
7. Facultatif : Si vous n'avez plus besoin de la fonction de suivi des transactions ou si vous souhaitez désinstaller l'agent IBM Integration Bus, désactivez le suivi des transactions pour IBM Integration Bus et supprimez l'exit utilisateur fourni par l'agent. Pour plus d'informations, voir «Désactivation du suivi des transactions», à la page 294 et «Suppression de l'exit utilisateur KQIUserExit», à la page 298.

Configuration de l'agent IBM Integration Bus

Vous devez attribuer un nom d'instance à l'agent IBM Integration Bus et configurer l'agent pour qu'il puisse commencer à surveiller votre environnement IBM Integration Bus.

Avant de commencer

- Vérifiez que l'ID utilisateur utilisé pour démarrer et arrêter l'agent fait partie des groupes d'utilisateurs **mqm** et **mqbrkrs**.
- Windows Si IBM MQ (WebSphere MQ) est installé sur le système Windows, ajoutez le chemin d'accès à la bibliothèque IBM MQ (WebSphere MQ) à la variable d'environnement **PATH**. L'agent IBM Integration Bus pourra ainsi charger les bibliothèques IBM MQ (WebSphere MQ) requises pour démarrer.
  1. Ajoutez le chemin d'accès à la bibliothèque IBM MQ (WebSphere MQ) au début de la variable d'environnement **PATH**.

     Par exemple, si le chemin d'installation d'IBM MQ (WebSphere MQ) est `C:\IBM\WMQ75`, ajoutez `C:\IBM\WMQ75\bin` au début de la variable d'environnement **PATH** de votre système Windows.
  2. Redémarrez le système Windows pour que les modifications soient prises en compte.
- Vous devrez peut-être fournir les informations suivantes en fonction de votre environnement au cours de la configuration d'agent. Si vous n'avez aucune idée de la valeur de configuration à spécifier, renseignez-vous auprès de l'administrateur d'IBM MQ (WebSphere MQ) et d'IBM Integration Bus.
  - Si IBM MQ (WebSphere MQ) est installé sur le même système que l'agent IBM Integration Bus, vous devez fournir le chemin d'accès à la bibliothèque 64 bits d'IBM MQ (WebSphere MQ).
  - Si l'agent IBM Integration Bus est configuré pour surveiller les noeuds d'intégration d'IBM Integration Bus V10 ou IBM App Connect Enterprise V11, vous devez fournir le répertoire d'installation de l'un de ces produits.
  - Pour que l'agent IBM Integration Bus ne surveille que certains noeuds d'intégration (courtiers) plutôt que tous les noeuds sur le même système, vous devez fournir le nom et le chemin d'installation de chaque noeud d'intégration (courtier).

Pourquoi et quand exécuter cette tâche

L'agent IBM Integration Bus est un agent d'instance multiple. Vous devez créer la première instance et démarrer l'agent manuellement.

Vous pouvez choisir de configurer l'agent avec ou sans interactions sur les systèmes UNIX or Linux. Sur les systèmes Windows, vous pouvez configurer l'agent sans interactions uniquement.

- Pour configurer l'agent avec interaction, exécutez le script de configuration et répondez aux invites. Voir «Configuration interactive», à la page 285 .
- Pour configurer l'agent sans interaction, éditez le fichier de réponses silencieux, puis exécutez le script de configuration. Voir «Configuration en mode silencieux», à la page 286 .

Important : Si vous avez également installé ITCAM Agent for WebSphere Message Broker, fourni en tant que produit ITCAM for Applications, sur le même système que l'agent IBM Integration Bus, fourni dans Cloud APM, ne les utilisez pas pour surveiller le même noeud d'intégration (courtier) sur le système.

Configuration interactive

Procédure

Pour configurer l'agent en exécutant le script et en répondant aux invites, procédez comme suit :

1. Exécutez la commande suivante :

   ```
   rép_install/bin/iib-agent.sh config nom_instance
   ```

   où *nom_instance* est le nom que vous souhaitez attribuer à l'instance d'agent.

   Important : La configuration interactive n'est pas prise en charge sur les systèmes Windows.
2. Une fois que vous avez confirmé que vous souhaitez configurer l'agent IBM Integration Bus, spécifiez des valeurs de configuration pour les paramètres généraux de l'agent.
   a) Lorsque le système vous invite à indiquer le paramètre **Agent Id**, spécifiez une chaîne alphanumérique unique comportant au maximum 8 caractères.

   A faire : La longueur maximale de l'ID agent est passée à 8 caractères depuis l'agent IBM Integration Bus version 7.3.0.1. Dans les versions précédentes, la longueur maximale de l'ID agent était de 4 caractères.

   Le nom de système géré comprend l'ID agent que vous spécifiez, par exemple, *nom_courtier_surveillé*:*ID_agent*:KQIB, où *nom_courtier_surveillé* est le nom du noeud d'intégration (courtier) surveillé.

   b) Lorsque le système vous invite à indiquer le paramètre Install Directory **IIB version 10 or ACE version 11** et que vous souhaitez surveiller les noeuds d'intégration d'IBM Integration Bus V10 ou IBM App Connect Enterprise V11, indiquez le répertoire d'installation de l'un de ces produits. Par exemple, `/opt/ibm/mqsi/ace-11.0.0.3`. Si vous ne souhaitez pas surveiller IBM Integration Bus V10 et IBM App Connect Enterprise V11, appuyez sur la touche Entrée pour accepter la valeur par défaut.

   A faire : Vous ne pouvez spécifier qu'un seul répertoire d'installation pour le paramètre **IIB version 10 ou ACE version 11 Install Directory**. Si vous avez installé IBM Integration Bus V10 ou IBM App Connect Enterprise V11 dans des répertoires différents et que vous souhaitez surveiller toutes leurs instances, créez des instances d'agent multiples et spécifiez un répertoire d'installation d'IBM Integration Bus V10 ou IBM App Connect Enterprise V11 pour chaque instance d'agent.
3. Facultatif : Utilisez la section **Monitored Broker Settings** pour préciser si cet agent doit surveiller uniquement certains noeuds d'intégration (courtiers).

   Par défaut, tous les noeuds d'intégration (courtiers) exécutés sur le même système hôte que l'agent IBM Integration Bus sont surveillés, comme le détermine la fonction d'auto-reconnaissance. Si vous souhaitez que l'agent surveille certains noeuds d'intégration (courtiers), spécifiez le nom du noeud d'intégration (courtier) que vous souhaitez surveiller et définissez le paramètre **Collect Node Data** sur No (valeur par défaut) dans la section **Monitored Broker Settings**. Il peut y avoir plusieurs sections **Monitored Broker Settings**. Chaque section contrôle les paramètres de surveillance d'un noeud d'intégration (courtier).

Conseil : Vous pouvez spécifier plusieurs sections **Monitored Broker Settings**. Lorsque vous éditez la section **Monitored Broker Settings**, les options suivantes sont disponibles :

- Add : créez une section **Monitored Broker Settings** pour configurer un autre noeud d'intégration (courtier).
- Edit : modifiez les paramètres de la section **Monitored Broker Settings** en cours.
- Del : supprimez la section **Monitored Broker Settings** en cours.
- Next : passez à la section **Monitored Broker Settings** suivante.
- Exit : quittez la configuration **Monitored Broker Settings**.

4. Si vous confirmez qu'IBM MQ (WebSphere MQ) est installé sur le même système, vous êtes invité à spécifier le paramètre **WebSphere MQ 64-bit library path**. Appuyez sur Entrée pour accepter la valeur par défaut, qui est le chemin d'accès à la bibliothèque 64 bits d'IBM MQ (WebSphere MQ) automatiquement découvert par l'agent. Si aucune valeur par défaut n'est affichée, vous devez fournir le chemin d'accès à la bibliothèque 64 bits d'IBM MQ (WebSphere MQ) pour passer à l'étape suivante. Par exemple, `/opt/mqm8/lib64`.

   A faire : Si vos noeuds d'intégration (courtiers) utilisent différentes versions des gestionnaires de files d'attente, indiquez la dernière version du chemin d'accès à la bibliothèque 64 bits d'IBM MQ (WebSphere MQ) pour ce paramètre.
5. Une fois la configuration terminée, entrez la commande suivante pour démarrer l'agent :

```
rép_install/bin/iib-agent.sh start
nom_instance
```

Configuration en mode silencieux

Procédure

Pour configurer l'agent en éditant le fichier de réponses silencieux et en exécutant le script sans intervenir, procédez comme suit :

1. Ouvrez le fichier de réponses silencieux de l'agent ci-après dans un éditeur de texte.
   - Linux AIX *rép_install*`/samples/iib_silent_config.txt`
   - Windows *rép_install*`\tmaitm6_x64\samples\qi_silent_config.txt`

   où *rép_install* correspond au répertoire d'installation de l'agent IBM Integration Bus. Le répertoire d'installation par défaut est le suivant :
   - Linux AIX `/opt/ibm/apm/agent`
   - Windows `C:\IBM\APM`
2. Pour le paramètre **agentId**, spécifiez une chaîne alphanumérique unique comportant au maximum 8 caractères qui servira d'identificateur court à l'agent.

   A faire : La longueur maximale de l'ID agent est passée à 8 caractères depuis l'agent IBM Integration Bus version 7.3.0.1. Dans les versions précédentes, la longueur maximale de l'ID agent était de 4 caractères.

   Le nom de système géré comprend l'ID agent que vous spécifiez, par exemple, *nom_courtier_surveillé*`:`*ID_agent*`:KQIB`, où *nom_courtier_surveillé* est le nom du noeud d'intégration (courtier) surveillé.
3. Si vous souhaitez surveiller les noeuds d'intégration d'IBM Integration Bus V10 ou IBM App Connect Enterprise V11, indiquez le répertoire d'installation de l'un de ces produits dans le paramètre **defaultWMBInstallDirectory**. Par exemple, `C:\Program Files\IBM\ACE\11.0.0.3\` pour un système Windows ou `/opt/ibm/mqsi/ace-11.0.0.3` pour un système Linux. Si vous ne souhaitez pas surveiller IBM Integration Bus V10 et IBM App Connect Enterprise V11, ce paramètre n'est pas obligatoire car l'agent IBM Integration Bus peut reconnaître automatiquement les noeuds d'intégration (courtiers) des versions précédentes.

A faire : Vous ne pouvez spécifier qu'un seul répertoire d'installation pour le paramètre **defaultWMBInstallDirectory**. Si vous avez installé IBM Integration Bus V10 ou IBM App Connect Enterprise V11 dans des répertoires différents et que vous souhaitez surveiller toutes leurs instances, créez des instances d'agent multiples et spécifiez un répertoire d'installation d'IBM Integration Bus V10 ou IBM App Connect Enterprise V11 pour chaque instance d'agent.

4. Facultatif : Précisez si cet agent doit surveiller uniquement certains noeuds d'intégration (courtiers).

   Par défaut, tous les noeuds d'intégration (courtiers) exécutés sur le même système hôte que l'agent IBM Integration Bus sont surveillés, comme le détermine la fonction d'auto-reconnaissance. Pour surveiller des noeuds d'intégration (courtiers) spécifiques, définissez les paramètres **collectNodeData** et **WMBInstallDirectory** pour chaque noeud d'intégration (courtier) que vous voulez surveiller.

   collectNodeData
   Indique si les données de définition de noeud sont collectées pour le noeud d'intégration (courtier) surveillé. La syntaxe est `collectNodeData.`*`nom_courtier`*`=NO|YES`, où *nom_courtier* est le nom du noeud d'intégration (courtier).

   La valeur par défaut est NO. Il est recommandé d'utiliser la valeur par défaut car les données de définition de noeud ne sont pas prises en charge dans la console Cloud APM.

   WMBInstallDirectory
   Répertoire d'installation du noeud d'intégration (courtier) à surveiller. La syntaxe est `WMBInstallDirectory.`*`nom_courtier=rép_install_courtier`*, où *rép_install_courtier* est le répertoire d'installation du noeud d'intégration (courtier) à surveiller.

   A faire : Pour un noeud d'intégration version 10, le paramètre **WMBInstallDirectory** peut remplacer le paramètre **defaultWMBInstallDirectory** que vous avez défini à l'étape précédente.

   Par exemple, pour ne surveiller que deux noeuds d'intégration (courtiers) nommés BK1 et BK2, définissez les paramètres comme suit :

   ```
   collectNodeData.BK1=NO
   collectNodeData.BK2=NO
   WMBInstallDirectory.BK1=rép_install_BK1
   WMBInstallDirectory.BK2=rép_install_BK2
   ```

5. Pour surveiller les courtiers qui sont antérieurs à la version 10 d'IBM Integration Bus, spécifiez le chemin de la bibliothèque 64 bits d'IBM MQ (WebSphere MQ) pour le paramètre **WMQLIBPATH**. Par exemple, `C:\Program Files\IBM\WebSphere MQ\bin64` pour un système Windows ou `/opt/mqm8/lib64` pour un système Linux.

   A faire : Si vos noeuds d'intégration (courtiers) utilisent différentes versions des gestionnaires de files d'attente, indiquez la dernière version du chemin d'accès à la bibliothèque 64 bits d'IBM MQ (WebSphere MQ) pour ce paramètre.

6. Sauvegardez et fermez le fichier de réponses silencieux de l'agent, puis entrez la commande suivante :

   - Linux AIX *rép_install*`/bin/iib-agent.sh config `*nom_instance chemin_vers_fichier_réponses*
   - Windows *rép_install*`\BIN\iib-agent.bat config "`*nom_instance chemin_vers_fichier_réponses*`"`

   où *nom_instance* est le nom de l'instance que vous configurez et *chemin_fichier_réponses* le chemin d'accès complet au fichier de réponses silencieux.

   Avertissement : Sur les systèmes Windows, n'insérez pas de guillemets ("") qui entourent le chemin d'accès du fichier de réponses silencieux, car cela entraînerait une erreur de configuration.

7. Une fois la configuration terminée, entrez la commande suivante pour démarrer l'agent :

   - Linux AIX

```
rép_install/bin/iib-agent.sh start
nom_instance
```

- Windows

```
rép_install\bin\iib-agent.bat start nom_instance
```

Résultats

Vous pouvez à présent vous connecter à la console Cloud APM et utiliser l'éditeur d'applications pour ajouter l'instance de l'agent IBM Integration Bus au Tableau de bord d'Application Performance. Pour obtenir des instructions de démarrage de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir «Gestion des applications», à la page 1129.

A faire : Chaque fois que vous mettez à jour ou migrez un noeud d'intégration (courtier) surveillé, vous devez redémarrer l'agent IBM Integration Bus après la mise à niveau ou la migration du noeud d'intégration (courtier).

Que faire ensuite

L'étape suivante consiste à configurer IBM Integration Bus pour l'activation des données. Les données suivantes sont disponibles dans le Tableau de bord d'Application Performance uniquement après les avoir activées dans IBM Integration Bus :

- Comptabilité des archives et statistiques
- Statistiques de ressource de la machine virtuelle Java
- Suivi des transactions

Pour obtenir des instructions, voir «Configuration d'IBM Integration Bus pour l'activation des données», à la page 288.

Configuration d'IBM Integration Bus pour l'activation des données

Pour que certaines données soient disponibles dans la console Cloud APM, vous devez configurer IBM Integration Bus de telle sorte à activer la collecte de données requise.

Avant de commencer

Assurez-vous que l'agent IBM Integration Bus est configuré.

A faire : L'activation du suivi des transactions vous demande de redémarrer le noeud d'intégration (courtier).

Pourquoi et quand exécuter cette tâche

Les statistiques d'archivage et de ressource peuvent être surveillées par l'agent IBM Integration Bus uniquement après avoir activé la collecte de données pour le noeud d'intégration (courtier). De même, si vous souhaitez visualiser le suivi des transactions dans les tableaux de bord de topologie et du middleware, vous devez activer le suivi des transactions au sein du noeud d'intégration (courtier) avant d'activer le suivi des transactions pour l'agent IBM Integration Bus.

Déterminez le type de données que vous voulez surveiller avec l'agent IBM Integration Bus et procédez comme suit en fonction de vos besoins.

Chaque serveur d'intégration détenu par le noeud d'intégration possède un fichier de configuration `server.conf.yaml` par défaut qui est stocké dans un sous-répertoire du répertoire des noeuds d'intégration. Les propriétés que vous définissez pour le noeud d'intégration dans le fichier `node.conf.yaml` sont héritées par les serveurs d'intégration détenus par lui. Vous pouvez néanmoins modifier les propriétés d'un serveur d'intégration dans le fichier `server.conf.yaml` correspondant.

(Pour plus d'informations, voir Configuration d'un noeud d'intégration en modifiant le fichier node.conf.yaml dans la documentation d'IBM App Connect Enterprise.)

Procédure

- Pour activer la collecte des statistiques d'archivage pour le noeud d'intégration (courtier), voir «Activation de la collecte des données statistiques et de comptabilité des archives», à la page 289.
- Pour activer la collecte des statistiques de ressource pour un noeud d'intégration (courtier), voir «Activation des statistiques de ressource de la machine virtuelle Java», à la page 292.
- Pour activer le suivi des transactions pour les flux de messages au sein d'un noeud d'intégration (courtier), voir «Activation du suivi de transaction», à la page 293.
- Si vous ne souhaitez plus de données de suivi des transactions, n'oubliez pas de désactiver le suivi des transactions pour le noeud d'intégration (courtier) sur lequel il a été activé. Voir «Désactivation du suivi des transactions», à la page 294 .

Activation de la collecte des données statistiques et de comptabilité des archives

Pourquoi et quand exécuter cette tâche

Pour activer la collecte des statistiques et des données de comptabilité des archives pour les flux de messages qui appartiennent au noeud de courtier d'intégration (courtier), exécutez la commande **mqsichangeflowstats** à partir du répertoire `bin` dans le répertoire d'installation du noeud d'intégration (courtier).

A faire : Emettez la commande **mqsichangeflowstats** au noeud d'intégration (courtier) en fonction de vos besoins en matière de données de surveillance. Il est recommandé d'activer seulement les statistiques nécessaires, car des flux de messages importants génèrent beaucoup de données et de traitement. Pour des informations détaillées sur la commande **mqsichangeflowstats**, reportez-vous à la documentation d'IBM Integration Bus.

Important : IBM Cloud Application Performance Management ne prend pas en charge les données statistiques et de comptabilité des instantanés en raison de la quantité de données et de traitement requise pour l'intervalle de prise d'instantané de 20 secondes défini. Les données d'archive fournissent les mêmes attributs exacts que les données d'instantané et sont plus appropriées pour la surveillance normale de la production fournie par IBM Cloud Application Performance Management. Si vous avez activé la collecte de données d'image instantanée pour le noeud d'intégration (courtier), n'oubliez pas de configurer l'agent IBM Integration Bus de telle sorte à ne pas stocker les données d'image instantanée. Pour obtenir des instructions, voir «Désactivation de la collecte de données d'image instantanée pour l'agent», à la page 295.

Procédure

- Pour obtenir la plupart des données des flux de messages, exécutez la commande suivante. Cette commande est recommandée car elle n'active pas les statistiques de terminal les plus détaillées, qui fournissent le nombre d'appels par terminal et par noeud. Le niveau de terminal utilise un grand volume de stockage.

```
mqsichangeflowstats nom_courtier -a -g -j -c active -t none -n basic -o xml
```

- Dans ACE version 11, pour obtenir la plupart des données des flux de messages, modifiez le fichier `node.conf.yaml` ou `server.conf.yaml` comme indiqué ci-dessous. Ces propriétés sont recommandées car elles n'activent pas les statistiques de terminal les plus détaillées, qui fournissent le nombre d'appels par terminal par noeud. Le niveau de terminal utilise un grand volume de stockage.

```
Statistiques :
  # Les flux de messages d'application héritent par défaut des valeurs Instantané et Archive
  # définies ici
  Instantané :
    #publicationOn: 'inactive' # Choisissez entre : active|inactive (valeur par défaut :
inactive)
                               # Vérifiez qu'Events.OperationalEvents.MQ|MQTT
```

```
                              # est défini pour outputFormat json,xml
    #accountingOrigin: 'none'  # Choisissez entre : none|basic
    #nodeDataLevel: 'none'     # Choisissez entre : none|basic|advanced
    #outputFormat: 'usertrace' # Liste séparée par des virgules :
                              # csv,bluemix,json,xml,usertrace
    #threadDataLevel: 'none'   # Choisissez entre : none|basic
  Archive :
    archivalOn: 'active'     # Choisissez entre : active|inactive
                             # (valeur par défaut : inactive)
                               # Vérifiez qu'Events.OperationalEvents.MQ|MQTT
                               # est défini pour outputFormat xml
    #accountingOrigin: 'none'  # Choisissez entre : none|basic
    #majorInterval: 60         # Définit l'intervalle, en minutes,
                            # de publication des statistiques d'archivage
    nodeDataLevel: 'basic'          # Choisissez entre : none|basic|advanced
    outputFormat: 'xml'  # Liste séparée par des virgules : csv,xml,usertrace
    #threadDataLevel: 'none'   # Choisissez entre : none|basic
```

Remarque : Si vous voulez désactiver ce paramètre, mettez en commentaire les lignes **archivalOn: 'active'**, **nodeDataLevel: 'basic'** et **outputFormat: 'xml'**.

- Pour obtenir toutes les données prises en charge par l'agent IBM Integration Bus, émettez la commande suivante :

```
mqsichangeflowstats nom_courtier -a -g -j -c active -t none -n advanced -o xml
```

- Dans ACE version 11, pour obtenir toutes les données prises en charge par l'agent IBM Integration Bus, modifiez le fichier `node.conf.yaml` ou `server.conf.yaml` de la manière suivante :

```
Statistiques :
  # Les flux de messages d'application héritent par défaut des valeurs Instantané et Archive
  # définies ici
  Instantané :
    #publicationOn: 'inactive' # Choisissez entre : active|inactive (valeur par défaut :
inactive)
                              # Vérifiez qu'Events.OperationalEvents.MQ|MQTT
                              # est défini pour outputFormat json,xml
    #accountingOrigin: 'none'  # Choisissez entre : none|basic
    #nodeDataLevel: 'none'     # Choisissez entre : none|basic|advanced
    #outputFormat: 'usertrace' # Liste séparée par des virgules :
                              # csv,bluemix,json,xml,usertrace
    #threadDataLevel: 'none'   # Choisissez entre : none|basic
  Archive :
    archivalOn: 'active'    # Choisissez entre : active|inactive (valeur par défaut :
inactive)
                              # Vérifiez qu'Events.OperationalEvents.MQ|MQTT
                              # est défini pour outputFormat xml
    #accountingOrigin: 'none'  # Choisissez entre : none|basic
    #majorInterval: 60       # Définit l'intervalle, en minutes,
                             # de publication des statistiques d'archivage
    nodeDataLevel: 'advanced'     # Choisissez entre : none|basic|advanced
    outputFormat: 'xml' # Liste séparée par des virgules : csv,xml,usertrace
    #threadDataLevel: 'none' # Choisissez entre : none|basic
```

Remarque : Si vous voulez désactiver ce paramètre, mettez en commentaire les lignes **archivalOn: 'active'**, **nodeDataLevel: 'advanced'** et **outputFormat: 'xml'**.

- Pour réduire la quantité de données mais malgré tout surveiller raisonnablement tous les flux de messages sans d'autres détails, émettez la commande suivante :

```
mqsichangeflowstats nom_courtier -a -g -j -c active -t none -n none -o xml
```

- Dans ACE version 11, pour réduire la quantité de données mais malgré tout surveiller raisonnablement tous les flux de messages sans d'autres détails, modifiez le fichier `node.conf.yaml` ou `server.conf.yaml` de la manière suivante :

```
Statistiques :
  # Les flux de messages d'application héritent par défaut des valeurs Instantané et Archive
  # définies ici
  Instantané :
    #publicationOn: 'inactive' # Choisissez entre : active|inactive (valeur par défaut :
inactive)
                              # Vérifiez qu'Events.OperationalEvents.MQ|MQTT
                              # est défini pour outputFormat json,xml
    #accountingOrigin: 'none'  # Choisissez entre : none|basic
```

```
    #nodeDataLevel: 'none'     # Choisissez entre : none|basic|advanced
    #outputFormat: 'usertrace' # Liste séparée par des virgules :
                               # csv,bluemix,json,xml,usertrace
    #threadDataLevel: 'none'   # Choisissez entre : none|basic
  Archive :
    archivalOn: 'active'    # Choisissez entre : active|inactive (valeur par défaut :
inactive)
                               # Vérifiez qu'Events.OperationalEvents.MQ|MQTT
                               # est défini pour outputFormat xml
    #accountingOrigin: 'none'  # Choisissez entre : none|basic
    #majorInterval: 60       # Définit l'intervalle, en minutes,
                              # de publication des statistiques d'archivage
    nodeDataLevel: 'none'         # Choisissez entre : none|basic|advanced
    outputFormat: 'xml' # Liste séparée par des virgules : csv,xml,usertrace
    #threadDataLevel: 'none' # Choisissez entre : none|basic
```

Remarque : Si vous voulez désactiver ce paramètre, mettez en commentaire les lignes **archivalOn: 'active'**, **nodeDataLevel: 'none'** et **outputFormat: 'xml'**.

- Si vous disposez d'un grand nombre de flux de messages mais voulez réduire la quantité de données, vous pouvez spécifier les flux de messages à surveiller en remplaçant l'option `-g` ou `-j` dans les commandes susmentionnées.
  - Pour spécifier un serveur d'intégration particulier (groupe d'exécution) pour l'activation, remplacez l'option `-g` par `-e` *`nom_serveur_intégration`*.
  - Pour identifier un flux de messages particulier pour l'activation, remplacez l'option `-j` par `-f` *`nom_flux_message`*.
  - Si vous avez regroupé vos flux de messages dans des applications, pour spécifier une application particulière pour l'activation, ajoutez l'option `-k` *`nom_application`* à l'option `-j`.
- L'agent IBM Integration Bus collecte les données statistiques et de comptabilité des archives toutes les 5 minutes. Pour définir l'intervalle auquel le noeud d'intégration (courtier) génère les données statistiques et de comptabilité des archives sur la même valeur, émettez la commande suivante en ayant arrêté le noeud d'intégration (courtier), puis redémarrez le noeud d'intégration (courtier) :

```
mqsichangebroker nom_courtier -v 5
```

- Dans ACE version 11, l'agent IBM Integration Bus collecte les données statistiques et de comptabilité des archives toutes les 5 minutes. Pour définir l'intervalle auquel le noeud d'intégration (courtier) génère les données statistiques et de comptabilité des archives sur la même valeur, modifiez le fichier `node.conf.yaml` ou `server.conf.yaml` de la manière suivante :

```
Statistiques :
  # Les flux de messages d'application héritent par défaut des valeurs Instantané et Archive
  # définies ici
  Instantané :
    #publicationOn: 'inactive' # Choisissez entre : active|inactive (valeur par défaut :
inactive)
                               # Vérifiez qu'Events.OperationalEvents.MQ|MQTT
                               # est défini pour outputFormat json,xml
    #accountingOrigin: 'none'  # Choisissez entre : none|basic
    #nodeDataLevel: 'none'     # Choisissez entre : none|basic|advanced
    #outputFormat: 'usertrace' # Liste séparée par des virgules :
                               # csv,bluemix,json,xml,usertrace
    #threadDataLevel: 'none'   # Choisissez entre : none|basic
  Archive :
    archivalOn: 'active'     # Choisissez entre : active|inactive (valeur par défaut :
inactive)
                               # Vérifiez qu'Events.OperationalEvents.MQ|MQTT
                               # est défini pour outputFormat xml
    #accountingOrigin: 'none'  # Choisissez entre : none|basic
    majorInterval: 5         # Définit l'intervalle, en minutes,
                             # de publication des statistiques d'archivage
    nodeDataLevel: 'none'         # Choisissez entre : none|basic|advanced
    outputFormat: 'xml' # Liste séparée par des virgules : csv,xml,usertrace
    #threadDataLevel: 'none'       # Choisissez entre : one|basic
```

Résultats

Une fois l'agent IBM Integration Bus configuré et démarré, les données statistiques et de comptabilité des flux de messages s'affichent dans les widgets de groupe suivants :

- Tableau de bord des flux de messages
  - Validations et annulations
  - UC en microsecondes
  - Temps écoulé en microsecondes
  - Débit d'octets d'entrée
  - Débit de messages d'entrée
  - Taille du message d'entrée
  - Temps d'attente UC des messages d'entrée en microsecondes
  - Temps d'attente écoulé des messages d'entrée en microsecondes
  - Erreurs de flux de messages
  - Statistiques sur le noeud de traitement des messages
- Tableau de bord du noeud de traitement
  - UC en microsecondes
  - Temps écoulé en microsecondes
  - Appels
  - Statut du noeud de traitement
  - Statistiques du terminal

Activation des statistiques de ressource de la machine virtuelle Java

Pourquoi et quand exécuter cette tâche
Pour activer les statistiques de ressource de la machine virtuelle Java pour les serveurs d'intégration qui appartiennent au noeud de courtier d'intégration (courtier), exécutez la commande **mqsichangeresourcestats** à partir du répertoire `bin` dans le répertoire d'installation du noeud d'intégration (courtier).

A faire : Les statistiques de ressource de la machine virtuelle Java sont considérées comme facultatives car seuls quelques attributs des données sont affichés par rapport au coût élevé de l'agent qui traite ces données toutes les 20 secondes. Demandez-vous si vous avez vraiment besoin des données statistiques de ressource JVM.

Procédure

- Pour activer les statistiques relatives à tous les serveurs d'intégration dans le noeud d'intégration (courtier), émettez la commande suivante :

```
mqsichangeresourcestats nom_courtier -c active
```

- Dans ACE version 11, pour activer les statistiques relatives à tous les serveurs d'intégration dans le noeud d'intégration (courtier), modifiez le fichier `node.conf.yaml` comme suit :

```
Statistiques :
  # Les flux de messages d'application héritent par défaut des valeurs Instantané et Archive
  # définies ici
  Instantané :
    #publicationOn: 'inactive' # Choisissez entre : active|inactive (valeur par défaut :
inactive)
                               # Vérifiez qu'Events.OperationalEvents.MQ|MQTT
                               # est défini pour outputFormat json,xml
    #accountingOrigin: 'none'  # Choisissez entre : none|basic
    #nodeDataLevel: 'none'     # Choisissez entre : none|basic|advanced
    #outputFormat: 'usertrace' # Liste séparée par des virgules :
                               # csv,bluemix,json,xml,usertrace
    #threadDataLevel: 'none'   # Choisissez entre : none|basic
  Archive :
    archivalOn: 'active'     # Choisissez entre : active|inactive (valeur par défaut :
inactive)
                               # Vérifiez qu'Events.OperationalEvents.MQ|MQTT
```

```
                              # est défini pour outputFormat xml
    #accountingOrigin: 'none'  # Choisissez entre : none|basic
    majorInterval: 5         # Définit l'intervalle, en minutes,
                             # de publication des statistiques d'archivage
    nodeDataLevel: 'advanced'     # Choisissez entre : none|basic|advanced
    outputFormat: 'xml' # Liste séparée par des virgules : csv,xml,usertrace
    threadDataLevel: 'basic'      # Choisissez entre : none|basic
   Resource:
     reportingOn: true       # Choisissez entre : true|false (valeur par défaut : false)
......
```

Remarque : Si vous voulez désactiver ce paramètre, mettez en commentaire **reportingOn: true**.

- Pour activer les statistiques relatives à un serveur d'intégration donné dans le noeud d'intégration (courtier), émettez la commande suivante :

```
mqsichangeresourcestats nom_courtier -e nom_serveur_intégration -c active
```

- Dans ACE version 11, pour activer les statistiques relatives à un serveur d'intégration donné dans le noeud d'intégration (courtier), modifiez le fichier `server.conf.yaml` comme suit :

```
Statistiques :
  # Les flux de messages d'application héritent par défaut des valeurs Instantané et Archive
  # définies ici
  Instantané :
    #publicationOn: 'inactive' # Choisissez entre : active|inactive (valeur par défaut :
inactive)
                              # Vérifiez qu'Events.OperationalEvents.MQ|MQTT
                              # est défini pour outputFormat json,xml
    #accountingOrigin: 'none'  # Choisissez entre : none|basic
    #nodeDataLevel: 'none'     # Choisissez entre : none|basic|advanced
    #outputFormat: 'usertrace' # Liste séparée par des virgules :
                              # csv,bluemix,json,xml,usertrace
    #threadDataLevel: 'none'   # Choisissez entre : none|basic
  Archive :
    archivalOn: 'active'     # Choisissez entre : active|inactive (valeur par défaut :
inactive)
                              # Vérifiez qu'Events.OperationalEvents.MQ|MQTT
                              # est défini pour outputFormat xml
    #accountingOrigin: 'none'  # Choisissez entre : none|basic
    majorInterval: 5         # Définit l'intervalle, en minutes,
                             # de publication des statistiques d'archivage
    nodeDataLevel: 'advanced'     # Choisissez entre : none|basic|advanced
    outputFormat: 'xml' # Liste séparée par des virgules : csv,xml,usertrace
    threadDataLevel: 'basic'   # Choisissez entre : none|basic
  Resource:
    reportingOn: true        # Choisissez entre : true|false (valeur par défaut : false)
```

Remarque : Si vous voulez désactiver ce paramètre, mettez en commentaire **reportingOn: true**.

Résultats

Les données statistiques de ressource JVM sont affichées dans les widgets de groupe suivants :

- Comptage de récupération de place
- Durée de récupération de place
- Mémoire non dynamique de la machine JVM
- Mémoire dynamique de la machine JVM

Activation du suivi de transaction

Avant de commencer

1. Assurez-vous que l'agent IBM Integration Bus est installé. Un exit utilisateur, nommé `KQIUserExit`, est fourni pour activer le suivi des transactions sur IBM Integration Bus.
2. Assurez-vous que l'utilisateur qui démarre le noeud d'intégration (courtier) dispose des droits d'accès au répertoire du module KQI User Exit. En d'autres termes, veillez à ajouter l'ID utilisateur utilisé pour démarrer le noeud d'intégration (courtier) au groupe sous lequel vous avez installé l'agent IBM Integration Bus.

Pourquoi et quand exécuter cette tâche

Vous devez déployer l'exit utilisateur `KQIUserExit` sur le noeud d'intégration (courtier). Sinon, aucune donnée n'est mise à disposition dans les tableaux de bord de middleware et de topologie, même après avoir activé le suivi des transactions sur l'agent IBM Integration Bus.

Conseil : Les noeuds IBM Integration Bus suivants sont inclus dans les tableaux de bord de topologie et du middleware par l'exit utilisateur `KQIUserExit` en tant que services non instrumentés :

- Noeuds de calcul et de base de données où une source de données ODBC est spécifiée
- Noeuds TCP/IP
- Noeuds de fichiers pour serveurs FTP ou FTPS distants
- Noeuds MQ, sauf s'ils sont déjà instrumentés

Procédure

Pour activer le suivi des transactions pour IBM Integration Bus, procédez comme suit :

1. Linux AIX
   Fermez tous les interpréteurs de commandes de courtier qui ont chargé l'environnement MQSI.
2. Ouvrez la console de commande IBM Integration Bus en utilisant l'une des méthodes suivantes. Si plusieurs versions des noeuds d'intégration (courtiers) sont installées sur votre système, assurez-vous de démarrer la console de commande pour la version appropriée.
   - Windows Cliquez sur **Démarrer** > **IBM Integration Bus** > **IBM Integration Console**
   - Linux AIX A partir du répertoire `bin` du répertoire d'installation du noeud d'intégration (courtier), émettez la commande **`mqsiprofile`**.
3. Arrêtez le noeud d'intégration (courtier) que vous voulez configurer à l'aide de la commande **`mqsistop`**.
4. Activez le suivi des transactions pour le flux de messages dans le noeud d'intégration (courtier) en ajoutant l'exit utilisateur KQIUserExit à l'aide de la commande **`mqsichangebroker`**.
   - Pour activer le suivi des transactions pour tous les flux de messages au sein du noeud d'intégration (courtier), exécutez la commande suivante :

     ```
     mqsichangebroker nom_courtier -e "KQIUserExit"
     ```

   - Pour activer le suivi des transactions pour un flux de messages spécifique au sein du noeud d'intégration (courtier), exécutez la commande suivante :

     ```
     mqsichangeflowuserexits nom_courtier -e nom_groupe_exécution -k nom_application -f
     nom_flux_messages -a "KQIUserExit"
     ```

5. Dans ACE version 11, vous pouvez également activer le suivi des transactions pour le flux de messages dans le noeud d'intégration (courtier) en ajoutant `KQIUserExit` au fichier `node.conf.yaml` ou `server.conf.yaml`.

   ```
   UserExits:
   activeUserExitList: 'KQIUserExit' # Indiquez le nom
   #d'une sortie utilisateur installée à activer.
   ```

   Remarque : Si vous souhaitez désactiver le suivi des transactions, mettez en commentaire **activeUserExitList: 'KQIUserExit'**.
6. Redémarrez le noeud d'intégration (courtier) à l'aide de la commande **`mqsistart`**.

Désactivation du suivi des transactions

Procédure

Pour désactiver le suivi des transactions pour IBM Integration Bus, procédez comme suit :

1. Ouvrez la console de commande IBM Integration Bus en utilisant l'une des méthodes suivantes. Si plusieurs versions des noeuds d'intégration (courtiers) sont installées sur votre système, assurez-vous de démarrer la console de commande pour la version appropriée.
   - Windows Cliquez sur **Démarrer** > **IBM Integration Bus** > **IBM Integration Console**
   - Linux AIX A partir du répertoire `bin` du répertoire d'installation du noeud d'intégration (courtier), émettez la commande **mqsiprofile**.
2. Désactivez le suivi des transactions pour le flux de messages dans un noeud d'intégration (courtier) en utilisant l'une des méthodes suivantes :
   - Pour désactiver le suivi des transactions pour un flux de messages spécifique, utilisez la commande **mqsichangeflowuserexits** :

     ```
     mqsichangeflowuserexits nom_courtier -e nom_groupe_exécution -f nom_flux_messages -a ""
     ```
   - Pour désactiver le suivi des transactions pour tous les flux de messages au sein du noeud d'intégration (courtier), commencez par arrêter le noeud d'intégration (courtier) à l'aide de la commande **mqsistop**, puis émettez la commande **mqsichangebroker** :

     ```
     mqsichangebroker nom_courtier -e ""
     ```

Que faire ensuite

- Pour le suivi des transactions, après avoir activé le suivi des transactions pour IBM Integration Bus, vous devez également activer le suivi des transactions pour l'agent. Pour obtenir des instructions, voir «Configuration du suivi des transactions pour l'agent IBM Integration Bus», à la page 296.
- Si vous avez activé la collecte de données d'image instantanée pour votre noeud d'intégration (courtier), configurez l'agent IBM Integration Bus de sorte à ne pas stocker les données d'image instantanée. Cloud APM ne prend pas en charge la comptabilité des instantanés et les données statistiques en raison de la quantité de données et de traitement requise pour l'intervalle de prise d'instantané de 20 secondes défini. Pour obtenir des instructions, voir «Désactivation de la collecte de données d'image instantanée pour l'agent», à la page 295.

Désactivation de la collecte de données d'image instantanée pour l'agent

Cloud APM ne prend pas en charge la comptabilité des images instantanées et les données statistiques en raison de la quantité de données et de traitement requise pour l'intervalle de prise d'instantané de 20 secondes défini. Si vous avez activé la collecte de données d'image instantanée pour le courtier, n'oubliez pas de configurer l'agent IBM Integration Bus pour ne pas stocker les données d'image instantanée.

Procédure

1. Ouvrez le fichier de configuration d'agent dans un éditeur de texte. Le fichier de configuration d'agent se trouve dans l'un des répertoires suivants en fonction du système d'exploitation utilisé :
   - Linux AIX *rép_install*/config/<*nom_hôte*>_qi_<*nom_instance*>.cfg
   - Windows *rép_install*\TMAITM6_x64\<*nom_hôte*>_qi_<*nom_instance*>.cfg

   où *rép_install* est le répertoire d'installation d'agent, *nom_hôte* est le nom d'hôte du système d'exploitation et *nom_instance* est le nom d'instance d'agent.
2. Editez le fichier en ajoutant le paramètre suivant dans la section KqiAgent :

   ```
   defaultRetainRecentSnapshotSamples=0
   ```

   Exemple :

   ```
   INSTANCE=inst1 [
   SECTION=KqiAgent [ { agentId=inst1 } { instName=inst1 }
   {defaultRetainRecentSnapshotSamples=0}]
   SECTION=MonitorBroker:BRK1 [ { collectNodeData=NO } ]
   ```

```
SECTION=MonitorBroker:BRK2 [ { collectNodeData=NO } ]
]
```

3. Sauvegardez et fermez le fichier.
4. Redémarrez l'agent IBM Integration Bus pour que les modifications soient prises en compte.

Configuration du suivi des transactions pour l'agent IBM Integration Bus

Les données de suivi des transactions pour IBM Integration Bus peuvent être affichées dans les tableaux de bord de topologie et du middleware une fois la collecte de données activée sur la page **Configuration d'agent** pour l'agent IBM Integration Bus.

Avant de commencer

- Assurez-vous que le suivi des transactions est activé pour IBM Integration Bus avec l'exit utilisateur fourni par l'agent `KQIUserExit`. Si ce n'est pas fait, suivez les instructions de la rubrique «Activation du suivi de transaction», à la page 293.
- Assurez-vous que l'agent IBM Integration Bus est correctement configuré. Si ce n'est pas fait, suivez les instructions de la rubrique «Configuration de l'agent IBM Integration Bus», à la page 284.

Procédure

Pour configurer le suivi des transactions pour l'agent IBM Integration Bus, procédez comme suit :

1. A partir de la barre de navigation, cliquez sur **Configuration système** > **Configuration d'agent**.
   La page **Configuration d'agent** s'affiche.
2. Cliquez sur l'onglet **IBM Integration Bus**.
3. Cochez les cases des instances d'agent et effectuez l'une des actions suivantes de la liste **Actions** :
   - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Enabled**. Le statut de la colonne **Transaction Tracking** est mis à jour sur Enabled.
   - Pour désactiver les données de suivi des transactions, cliquez sur **Set Transaction Tracking** > **Disabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour sur Disabled.

Résultats

Vous avez configuré le suivi des transactions pour les instances d'agent sélectionnées. Les données de suivi des transactions peuvent être affichées dans les tableaux de bord de topologie et de middleware une fois que vous avez activé la collecte de données. Pour plus d'informations, voir «Ajout d'applications middleware au Tableau de bord d'Application Performance », à la page 100.

Spécification d'un nom de système géré unique pour agent IBM Integration Bus

Le nom d'instance agent IBM Integration Bus affiché sur la console Cloud APM est également connu comme le nom de système géré. Vous pouvez utiliser le paramètre de configuration d'agent pour indiquer un nom de système géré unique pour chaque instance d'agent.

Pourquoi et quand exécuter cette tâche

Lorsque l'agent IBM Integration Bus est démarré, il enregistre le nom de système géré au format suivant : *nom_courtier_surveillé*:*ID_agent*:KQIB pour chaque instance d'agent, où *nom_courtier_surveillé* est le nom du courtier surveillé et *ID_agent* est l'ID agent défini par le paramètre de configuration d'agent. La longueur maximale du nom de système géré est de 32 caractères. Si la longueur du nom de système géré dépasse ce nombre, le nom est alors tronqué.

Un nom de système géré unique peut être nécessaire dans les cas suivants :

- Plus d'un agent IBM Integration Bus sont en cours d'exécution sur le même système.
- Plusieurs courtiers surveillés du même nom sont en cours d'exécution sur des systèmes différents.

Pour indiquer un ID agent de manière à obtenir un nom de système géré unique, utilisez l'option **ID agent** pendant la configuration interactive ou utilisez le paramètre **agentId** dans le fichier de réponses silencieux.

A faire : Si vous n'avez jamais configuré l'agent IBM Integration Bus suite à l'installation, procédez comme indiqué dans la section «Configuration de l'agent IBM Integration Bus», à la page 284.

Procédure

- Pour utiliser l'option **ID agent** pendant la configuration interactive, procédez comme suit :
  a) Exécutez la commande suivante :

  ```
  rép_install/bin/iib-agent.sh config nom_instance
  ```

  où *nom_instance* est le nom de l'instance d'agent pour laquelle vous souhaitez indiquer un ID agent.
  b) Suivez les options pour configurer l'instance d'agent.
  Si, pour une option, aucune modification n'est nécessaire, utilisez la valeur par défaut.
  c) Lorsque l'option `ID agent` apparaît, indiquez le qualificateur intermédiaire du nom de système géré.
  Le format valide est une chaîne alphanumérique comportant au maximum 8 caractères.
- Pour utiliser le paramètre **agentId** dans le fichier de réponses silencieux, procédez comme suit :
  a) Ouvrez le fichier de réponses silencieux de l'agent ci-après dans un éditeur de texte.
  – Linux AIX *rép_install*/samples/iib_silent_config.txt
  – Windows *rép_install*\tmaitm6_x64\samples\qi_silent_config.txt
  b) Indiquez un ID agent pour le paramètre **agentId**.
  Le format valide est une chaîne alphanumérique comportant au maximum 8 caractères.
  c) Sauvegardez et fermez le fichier de réponses silencieux, puis exécutez la commande suivante à partir de la ligne de commande :
  – Linux AIX *rép_install*/bin/iib-agent.sh config *nom_instance chemin_vers_fichier_réponses*
  – Windows *rép_install*\BIN\iib-agent.bat config "*nom_instance chemin_vers_fichier_réponses*"
  où *nom_instance* est le nom de l'instance que vous configurez et *chemin_fichier_réponses* le chemin d'accès complet au fichier de réponses silencieux.

  Avertissement : Sur les systèmes Windows, n'insérez pas de guillemets ("") qui entourent le chemin d'accès du fichier de réponses silencieux, car cela entraînerait une erreur de configuration.
  d) Une fois la configuration terminée, entrez la commande suivante pour démarrer l'agent :
  – Linux AIX

  ```
  rép_install/bin/iib-agent.sh start
  nom_instance
  ```

  – Windows

  ```
  rép_install\bin\iib-agent.bat start nom_instance
  ```

Que faire ensuite

Connectez vous à console Cloud APM. Si l'instance d'agent portant l'ancien nom de système géré apparaît toujours comme déconnectée, éditez votre application pour la supprimer, puis ajoutez la nouvelle instance d'agent portant l'ID agent attribué.

Suppression de l'exit utilisateur KQIUserExit

Avant de désinstaller l'agent IBM Integration Bus, vous devez commencer par supprimer l'exit utilisateur `KQIUserExit`.

Procédure

Pour supprimer l'exit utilisateur `KQIUserExit` que vous avez déployé sur IBM Integration Bus pour le suivi des transactions, procédez comme suit :

1. Accédez au répertoire `bin` de l'agent IBM Integration Bus.
   - Windows *rép_install_agent*\arch\qi\bin
   - Linux AIX *rép_install_agent*/arch/qi/bin

   où :
   - *rép_install_agent* est le répertoire d'installation de l'agent. La valeur par défaut est `C:\IBM\APM` sur les systèmes Windows et `/opt/ibm/apm/agent` sur les systèmes Linux et AIX.
   - *arch* est le code d'architecture de la plateforme. Par exemple, lx8266 représente Linux Intel version 2.6 (64 bits). Pour obtenir la liste complète des codes d'architecture, voir le fichier *rép_install_agent*`/archdsc.tbl`.
2. Exécutez le script **configDC** pour supprimer la bibliothèque d'exits utilisateur de manière interactive :
   - Windows

     ```
     configDC.bat -disable rép_install_iib
     ```
   - Linux AIX

     ```
     ./configDC.sh -disable rép_install_iib
     ```

   où *rép_install_iib* est le répertoire d'installation d'IBM Integration Bus.

Exemple

L'exemple suivant supprime l'exit utilisateur fourni par l'agent pour les courtiers version 9.0 installés sur un système AIX :

```
cd /opt/IBM/ITM/aix513/qi/bin
./configDC.sh -disable /opt/IBM/mqsi/9.0
```

Configuration de la surveillance d'IBM MQ Appliances

L'Agent MQ Appliance est un agent multi-instance. Après l'installation, vous devez le configurer en créant une instance d'agent pour pouvoir l'utiliser pour la surveillance.

Avant de commencer

- Les instructions figurant dans cette rubrique concernent l'édition la plus récente de l'agent, sauf indication contraire.

Procédure

- Sur les systèmes Linux et UNIX, vous pouvez configurer l'agent avec le script de configuration qui génère des invites pour les réponses ou le fichier de réponses silencieux.
  - «Configuration de l'agent en répondant à des invites», à la page 299
  - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 300
- Sur les systèmes Windows, vous pouvez configurer l'agent uniquement avec le fichier de réponses silencieux.
  - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 300

Que faire ensuite

Dans la console Cloud APM, accédez au tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux AIX `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Configuration de l'agent en répondant à des invites

Vous devez attribuer un nom d'instance à Agent MQ Appliance et configurer l'agent pour qu'il puisse commencer à surveiller IBM MQ Appliances.

Procédure

Pour configurer l'agent en exécutant le script et en répondant aux invites, procédez comme suit :

1. Exécutez la commande suivante :

   ```
   rép_install/bin/mq_appliance-agent.sh config nom_instance
   ```

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent.

   Exemple :

   ```
   /opt/ibm/apm/agent/bin/mq_appliance-agent.sh config AQM904
   ```

2. Répondez aux invites pour définir les valeurs de configuration de l'agent.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'Agent MQ Appliance», à la page 301.

3. Exécutez la commande suivante pour démarrer l'agent :

   ```
   rép_install/bin/mq_appliance-agent.sh start nom_instance
   ```

   Exemple :

   ```
   /opt/ibm/apm/agent/bin/mq_appliance-agent.sh start AQM904
   ```

Résultats

Vous pouvez à présent vous connecter à la console Cloud APM et utiliser l'éditeur d'applications pour ajouter l'instance de l'Agent MQ Appliance au tableau de bord des performances des applications. Pour obtenir des instructions de démarrage de la console Cloud APM, voir «Démarrage de la console Cloud

APM», à la page 1003. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir «Gestion des applications», à la page 1129.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

Pour configurer l'agent en éditant le fichier de réponses silencieux et en exécutant le script sans intervenir, procédez comme suit :

1. Ouvrez le fichier `mq_appliance_silent_config.txt` dans l'un des répertoires suivants dans un éditeur de texte.
   - Linux AIX *rép_install*`/samples/mq_appliance_silent_config.txt`
   - Windows *rép_install*`\samples\mq_appliance_silent_config.txt`

   où *rép_install* correspond au répertoire d'installation de l'agent. Par exemple, `/opt/ibm/apm/agent`.
2. Dans le fichier `mq_appliance_silent_config.txt`, spécifiez des valeurs pour tous les paramètres obligatoires et modifiez les valeurs des autres paramètres si nécessaire.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'Agent MQ Appliance», à la page 301.
3. Sauvegardez et fermez le fichier `mq_appliance_silent_config.txt` et exécutez la commande suivante :
   - Linux AIX

     ```
     rép_install/bin/mq_appliance-agent.sh config nom_instance
     chemin_accès_au_fichier_silencieux
     ```
   - Windows

     ```
     rép_install\bin\mq_appliance-agent.bat config nom_instance
     chemin_accès_au_fichier_silencieux
     ```

   où :
   - *nom_instance* correspond au nom à attribuer à l'instance d'agent. Par exemple, `AQM904`.
   - *chemin_accès_au_fichier_silencieux* correspond au chemin d'accès au fichier `mq_appliance_silent_config.txt`. Par exemple, `/opt/ibm/apm/agent/samples/mq_appliance_silent_config.txt`.
4. Une fois la configuration terminée, exécutez la commande suivante pour démarrer l'agent :
   - Linux AIX

     ```
     rép_install/bin/mq_appliance-agent.sh start nom_instance
     ```
   - Windows

```
rép_install\bin\mq_appliance-agent.bat start nom_instance
```

Résultats

Vous pouvez à présent vous connecter à la console Cloud APM et utiliser l'éditeur d'applications pour ajouter l'instance de l'Agent MQ Appliance au tableau de bord des performances des applications. Pour obtenir des instructions de démarrage de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir «Gestion des applications», à la page 1129.

Paramètres de configuration de l'Agent MQ Appliance

Les paramètres de configuration de l'Agent MQ Appliance sont affichés dans des tableaux qui les regroupent par sections.

- Tableau 24, à la page 301 : Propriétés pour la réception d'événements SNMP et le décodage des événements V3.
- Tableau 25, à la page 302 : Propriétés pour les paramètres Java.
- Tableau 26, à la page 302 : Propriétés pour le serveur proxy utilisé par les fournisseurs HTTP.
- Tableau 27, à la page 303 : Propriétés pour le serveur HTTP.
- Tableau 28, à la page 303 : Propriétés pour la connexion au dispositif MQ.

Tableau 24. Paramètres de configuration d'événement SNMP

Nom du paramètre	Description	Nom de paramètre dans le fichier de configuration silencieux
Numéro de port	Numéro de port utilisé pour écouter les événements SNMP. La valeur par défaut est 162.	KQZ_SNMPEVENT_PORT
Niveau de sécurité	Niveau de sécurité utilisé pour la connexion à l'événement SNMP. Il peut correspondre à l'une des valeurs suivantes : • 1=noAuthNoPriv • 2=authNoPriv • 3=authPriv La valeur par défaut est 2.	KQZ_SNMPEVENT_ SECURITY_LEVEL
Nom d'utilisateur	Nom d'utilisateur utilisé pour la connexion à l'agent SNMP. La valeur par défaut est `snmpuser`.	KQZ_SNMPEVENT _USER_NAME
Protocole d'autorisation	Protocole d'autorisation utilisé pour la connexion à l'agent SNMP. Il peut correspondre à l'une des valeurs suivantes : • 1=MD5 • 2=SHA La valeur par défaut est 2.	KQZ_SNMPEVENT_AUTH _PROTOCOL
Mot de passe d'autorisation	Phrase passe d'autorisation utilisée pour la connexion à l'agent SNMP.	KQZ_SNMPEVENT_AUTH _PASSWORD

Tableau 24. Paramètres de configuration d'événement SNMP (suite)		
Nom du paramètre	**Description**	**Nom de paramètre dans le fichier de configuration silencieux**
Mot de passe de confidentialité	Phrase passe de confidentialité utilisée pour la connexion à l'agent SNMP.	KQZ_SNMPEVENT_PRIV _PASSWORD
Fichier de configuration des alertes	Emplacement du fichier de configuration des alertes.	KQZ_SNMPEVENT_ TRAPCNFG_FILE

Tableau 25. Paramètres de configuration Java		
Nom du paramètre	**Description**	**Nom de paramètre dans le fichier de configuration silencieux**
Niveau de trace Java	Niveau de trace utilisé par les fournisseurs Java. Il peut correspondre à l'une des valeurs suivantes : • 1=Arrêt • 2=Erreur • 3=Warning • 4=Information • 5=Débogage minimum • 6=Débogage moyen • 7=Débogage maximum • 8=All La valeur par défaut est 2.	JAVA_TRACE _LEVEL

Tableau 26. Paramètres de configuration du serveur proxy		
Nom du paramètre	**Description**	**Nom de paramètre dans le fichier de configuration silencieux**
Nom d'hôte du proxy	Nom d'hôte du serveur proxy.	KQZ_HTTP _PROXY_HOSTNAME
Port du proxy	Numéro de port du serveur proxy. La valeur par défaut est 80.	KQZ_HTTP_PROXY_PORT
Nom de l'utilisateur du proxy	Nom d'utilisateur du serveur proxy.	KQZ_HTTP _PROXY_USER
Mot de passe du proxy	Mot de passe du serveur proxy.	KQZ_HTTP _PROXY_PASSWORD

Tableau 27. Paramètres de configuration du serveur HTTP

Nom du paramètre	Description	Nom de paramètre dans le fichier de configuration silencieux
Nom d'utilisateur HTTP	Nom d'utilisateur pour l'accès à l'interface MQ Appliance REST Management.	KQZ_HTTP _USER
Mot de passe HTTP	Mot de passe pour l'accès à l'interface MQ Appliance REST Management.	KQZ_HTTP _PASSWORD
Validation des certificats activée	Indique si la validation de certificat est activée. Il peut correspondre à l'une des valeurs suivantes : • 1=true • 2=false La valeur par défaut est 2.	KQZ_HTTP_CERTIFICATE _VALIDATION

Tableau 28. Paramètres de configuration de la connexion au dispositif MQ

Nom du paramètre	Description	Nom de paramètre dans le fichier de configuration silencieux
Hôte ou adresse IP du dispositif	Nom d'hôte ou adresse IP du dispositif MQ. La valeur par défaut est `https://hostnameoripaddress:` `https://9.123.123.123`.	KMK_APPLIANCE _HOST_OR _IP_ADDRESS.arm1
Numéro de port du dispositif	Numéro de port pour la connexion HTTPS au dispositif MQ. La valeur par défaut est 5554.	KMK_APPLIANCE _PORT_NUMBER.arm1
Nom de l'utilisateur du dispositif	Nom d'utilisateur utilisé pour la connexion au dispositif MQ.	KMK_APPLIANCE _USER_NAME.arm1
Mot de passe de l'utilisateur du dispositif	Mot de passe de l'utilisateur du dispositif MQ.	KMK_APPLIANCE _USER_PASSWORD.arm1
Identification de l'hôte de l'agent	Nom d'hôte du système où Agent MQ Appliance est exécuté. La valeur par défaut est `9.123.123.111`.	KMK_APM_ AGENT_IDENTIFICATION .arm1
Validation des certificats activée	Indique si la validation de certificat est activée pour la connexion HTTP. • 1=true • 2=false La valeur par défaut est 2.	KMK_CERTIFICATE _VALIDATION_ ENABLED.arm1

Configuration de la surveillance d'InfoSphere DataStage

Vous devez configurer l'agent DataStage pour la collecte des données de surveillance de la santé et des performances des ressources du serveur DataStage.

Avant de commencer

Pour connaître les prérequis matériels et logiciels, voir Software Product Compatibility Reports for DataStage agent.

Pourquoi et quand exécuter cette tâche

L'agent DataStage est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

Les versions du produit et de l'agent sont souvent différentes. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Configuration de l'agent sur les systèmes Windows

Vous pouvez utiliser la fenêtre IBM Cloud Application Performance Management pour configurer l'agent sur des systèmes Windows.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Modèle** dans la colonne **Tâche/sous-système**, puis sélectionnez **Configurer avec les valeurs par défaut**.

   La fenêtre **Monitoring Agent for DataStage** s'ouvre.
3. Dans la zone **Enter a unique instance name**, entrez le nom d'instance de l'agent et cliquez sur **OK**.
4. Dans la fenêtre **Monitoring Agent for DataStage**, indiquez des valeurs pour les paramètres de configuration et cliquez sur **OK**.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 306.
5. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis cliquez sur **Démarrer** pour démarrer l'agent.

Configuration de l'agent sur des systèmes Linux

Pour configurer l'agent sur des systèmes d'exploitation Linux, vous pouvez exécuter le script ou répondre à des invites.

Procédure

1. Dans la ligne de commande, modifiez le chemin d'accès au répertoire d'installation de l'agent. Exemple : `/opt/ibm/apm/agent/bin`
2. Exécutez la commande suivante, où nom_instance est le nom que vous souhaitez donner à l'instance :

   `./datastage-agent.sh config nom_instance`
3. Lorsque la ligne de commande affiche le message suivant, tapez 1 et entrez :

   `Edit 'Monitoring Agent for DataStage' setting? [1=Yes, 2=No]`
4. A l'invite, indiquez les valeurs des paramètres de configuration.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 306.

5. Exécutez la commande suivante pour démarrer l'agent :

   ```
   ./datastage-agent.sh start nom_instance
   ```

Configuration des variables d'environnement

Vous pouvez configurer les variables d'environnement pour modifier le comportement de l'agent DataStage.

Procédure

1. Ouvrez le fichier suivant dans un éditeur de texte :
   a) Windows *rép_install*\TMAITM6_x64\KDTENV_*nom_instance*
   b) Linux *rép_install*/config/.dt.environment
2. Editez les variables d'environnement suivantes :
   - **KDT_FIRST_COLLECTION_INTERVAL** : intervalle de temps en secondes de la première collecte de données. Définissez cet intervalle de temps sur une durée au cours de laquelle l'agent collecte les données des exécutions de travail précédentes dans le délai spécifié jusqu'à ce que l'agent démarre. La valeur par défaut est 300 secondes (5 minutes). Ainsi, si l'agent démarre à 14:00, il collecte les données des exécutions de travail de 13:55 à 14:00. Cela permet d'éviter une tempête de données d'exécutions de travail historiques lorsque l'agent commence à collecter les données. Toutes les collectes de données d'agent suivantes pour les exécutions de travaux extraient uniquement les exécutions de travaux récemment ajoutées qui ont eu lieu depuis la dernière collecte.
   - **KDT_SSL_CONTEXT** : protocole SSL activé sur le niveau service (WebSphere Application Server). La valeur par défaut est TLS.
   - **KDT_META_SCHEMA_NAME** : nom du schéma de base de données créé pour le référentiel de métadonnées. La valeur par défaut est DSODB pour Db2 et xmeta pour les bases de données MSSQL et Oracle.
   - **KDT_DATABASE_SERVICE_NAME** : nom de base de données ou de service utilisé par l'agent pour se connecter au référentiel de métadonnées. La valeur par défaut est XMETA pour Db2, xmeta pour MSSQL et ORCL pour les bases de données Oracle.
   - **KDT_DISABLED_ATTRIBUTEGROUP** : liste de groupes d'attributs séparés par une virgule dont la collecte de données ne doit pas être disponible. Les valeurs suivantes peuvent être définies seules ou ensemble pour le groupe d'attributs respectif : JobRuns, JobProperties, JobRunLog, JobStages, JobParameters, EngineSystemConfiguration, EngineSystemResources, EngineServiceStatus, EngineStatusSummary, JobActivity, AgentConfiguration et JobConfiguration.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'agent DataStage sur les systèmes Linux and Windows. Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

1. Dans un éditeur de texte, ouvrez le fichier de configuration en mode silencieux qui est disponible à l'emplacement suivant et indiquez des valeurs pour tous les paramètres :
   Windows *rép_install*\samples\datastage_silent_config.txt
   Linux *rép_install*\samples\datastage_silent_config_UNIX.txt

Windows `C:\IBM\APM\samples`

Linux `/opt/ibm/apm/agent/samples`

Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 306.

2. Sur la ligne de commande, changez le chemin d'accès au *rép_install* `\casier`.
3. Exécutez la commande suivante :

   Windows `datastage-agent.bat config` *nom_instance rép_install*`\samples \datastage_silent_config.txt`

   Linux `datastage-agent.sh config` *nom_instance rép_install*`\samples \datastage_silent_config_UNIX.txt`
4. Démarrez l'agent.

   Windows Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis sur **Démarrer**.

   Linux Exécutez la commande suivante : `./datastage-agent.sh start` *nom_instance*

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Pour obtenir de l'aide sur le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Paramètres de configuration de l'agent

Lorsque vous configurez l'agent DataStage, vous pouvez modifier les paramètres de configuration du niveau service, du référentiel de métadonnées ainsi que les paramètres de configuration avancés.

Paramètres de configuration du niveau service

Il s'agit des paramètres de configuration requis pour que l'agent se connecte au niveau service.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration du niveau service de l'agent DataStage.

Tableau 29. Noms et descriptions des paramètres de configuration du niveau service

Nom du paramètre	Description	Zone obligatoire
Nom d'hôte	Nom d'hôte de l'ordinateur sur lequel le niveau service est installé. Si l'ordinateur fait partie d'un domaine, indiquez le nom de domaine complet. La valeur par défaut est localhost.	Oui
Port HTTPS	Port HTTPS de l'interface REST de l'ordinateur sur lequel le niveau service est installé. La valeur par défaut est 9443.	Oui
Nom d'utilisateur WAS	Nom d'utilisateur utilisé pour la connexion à WebSphere Application Server. La valeur par défaut est wasadmin.	Oui
Mot de passe WAS	Mot de passe utilisé pour la connexion à WebSphere Application Server.	Oui
Confirm WAS Password	Mot de passe indiqué dans la zone **WAS Password**.	Oui

Paramètres de configuration du référentiel de métadonnées

Il s'agit des paramètres de configuration requis pour que l'agent se connecte au référentiel de métadonnées.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration du référentiel de métadonnées de l'agent DataStage.

Tableau 30. Noms et descriptions des paramètres de configuration du référentiel de métadonnées

Nom du paramètre	Description	Zone obligatoire
Type de base de données	Type de la base de données du référentiel de métadonnées. La valeur par défaut pour Db2 est 1.	Oui
Nom d'hôte	Nom d'hôte de l'ordinateur sur lequel le référentiel de métadonnées est installé. Si l'ordinateur fait partie d'un domaine, indiquez le nom de domaine complet. La valeur par défaut est localhost.	Oui
Port de la base de données	Port de la base de données du référentiel de métadonnées utilisé pour la connexion JDBC. La valeur par défaut est 50000.	Oui
Nom d'utilisateur de la base de données	Nom d'utilisateur utilisé pour la connexion à la base de données d'opérations. La valeur par défaut est dsodb.	Oui
Mot de passe de la base de données	Mot de passe utilisé pour la connexion à la base de données d'opérations.	Oui
Confirm Database Password	Mot de passe indiqué dans la zone **Database Password**.	Oui
Chemin de pilote JDBC	Chemin d'accès au pilote JDBC, incluant le fichier jar. Par exemple, /home/jars/db.jar sur le système Linux.	Oui

Paramètres de configuration avancés

Tableau 31. Noms et descriptions des paramètres de configuration avancés

Nom du paramètre	Description	Zone obligatoire
Niveau de trace Java	Niveaux de trace utilisés par les fournisseurs personnalisés Java. La valeur par défaut est 2.	Oui

Paramètres de configuration client de l'interface de programme d'application Java

Tableau 32. Noms et descriptions des paramètres de configuration client de l'interface de programme d'application Java

Nom du paramètre	Description	Zone obligatoire
Chemin d'accès aux classes pour les fichiers JAR		Non

Configuration d'Internet Service Monitor

L'agent Internet Service Monitoring offre la possibilité de déterminer si un service spécifique fonctionne correctement, d'identifier les domaines problématiques et d'établir un rapport sur la performance des services par rapport aux accords sur les niveaux de service. Internet Service Monitoring agent fonctionne par émulation des actions d'un utilisateur réel. Il interroge ou teste régulièrement les services Internet pour vérifier leur statut et leurs performances.

Présentation

Lors de la surveillance des services Internet, vous définissez ce qui doit être surveillé, pour qui et quand. Vous pouvez configurer la surveillance des services Internet par le biais de l'interface utilisateur de configuration d'Internet Service Monitoring agent.

Les moniteurs de service Internet testent les services Internet spécifiques et réacheminent les résultats des tests à Databridge. Les moniteurs émulent les actions d'un utilisateur réel du service.

Par exemple, le moniteur HTTP tente à intervalles réguliers d'accéder à une page Web en émulant les demandes généralement envoyées par un navigateur Web lorsqu'un utilisateur consulte cette page. Le moniteur enregistre le résultat du test, qui est envoyé à la passerelle de données.

Internet Service Monitoring

Chaque moniteur est conçu pour tester un type de protocole ou service. Par exemple, le moniteur HTTP teste la disponibilité des ressources, telles les pages Web via le protocole HTTP, et le moniteur FTP teste le transfert des fichiers entre les hôtes exécutant le protocole FTP.

Un moniteur peut tester plusieurs instances différentes du même service, comme une série de pages Web prises en charge par une plage d'hôtes.

Surveillance des services Web

Grâce à la gamme de moniteurs d'Internet Service Monitoring, vous pouvez personnaliser le type de surveillance des services Web à appliquer, en allant d'une surveillance basique des services Internet testant la disponibilité d'une page Web jusqu'à la combinaison de séquences de tests.

La surveillance des services Internet utilise une grande quantité d'interrogations simples pour tester la disponibilité des services Web. Par exemple, si vous voulez surveiller la disponibilité générale d'un site Web, vous devez utiliser le moniteur HTTP pour interroger un grand nombre d'URL à intervalles réguliers.

A l'aide d'une combinaison de moniteurs, vous pouvez créer un niveau de surveillance de service approprié à la spécification de vos besoins :

- Moniteurs HTTP et HTTPS

  Surveillent la disponibilité des ressources des protocoles HTTP ou HTTPS en exécutant en grande quantité des tests de base à une seule interrogation.
- Moniteur de transactions (TRANSX)

  Combine des séquences de tests effectués par un groupe de moniteurs, simulant ainsi les actions d'un utilisateur réel. Par exemple, se connecter à un service, accéder à un nombre de pages sur plusieurs sites Web, puis accéder aux services de messagerie électronique.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Configuration d'Internet Service Monitoring par le biais de l'interface utilisateur

Pour surveiller les services Internet, créez des profils utilisateur, des éléments de profil et des plannings de surveillance. Configurez des profils utilisateur, des éléments de profil et des plannings de surveillance à l'aide de l'interface utilisateur d'Internet Service Monitoring.

Pourquoi et quand exécuter cette tâche

Un profil utilisateur est un client, un département ou un groupe de services dont vous surveillez les services Internet ou Web. Pour chaque profil utilisateur, l'utilisateur doit définir un ou plusieurs éléments de profil. Par exemple, un utilisateur peut définir un élément de profil pour surveiller une page Web distribuée via un service HTTP ou pour surveiller la disponibilité d'un service FTP. Les profils utilisateur contiennent généralement plusieurs éléments de profil qui testent chacun l'un des services fournis à cet

utilisateur. Chaque profil utilisateur dispose également d'une planification de surveillance associée qui détermine le jour et l'heure auxquels s'exécutent les tests définis dans le profil.

Pour accéder à la fenêtre de configuration de l'agent Internet Service Monitoring par le biais du tableau de bord IBM Application Performance Management, procédez comme suit :

Procédure

1. Dans le tableau de bord Application Performance Management, cliquez sur l'icône  . Cliquez sur **Configuration de l'agent**.

   La fenêtre Configuration de l'agent s'ouvre.
2. Cliquez sur l'onglet **ISM** pour configurer l'agent Internet Service Monitoring.

   Vous pouvez créer, éditer, supprimer, actualiser, planifier et filtrer des profils utilisateur. Déployez les profils utilisateur créés sur le système géré sélectionné. La version qui s'affiche est celle du système géré. Le nom du profil indique le profil utilisateur déployé sur les systèmes gérés sélectionnés. Pour configurer les profils et les déployer sur les systèmes gérés, procédez comme suit.
3. Pour ajouter un profil, cliquez sur l'icône  . Entrez le **Nom de profil** et la **Description** dans la boîte de dialogue.
4. Cliquez sur **Suivant**.
5. Sélectionnez un moniteur dans la liste déroulante et cliquez sur **Suivant**.
6. Indiquez les valeurs des zones et cliquez sur **Ajouter**.

   Plusieurs moniteurs peuvent être sélectionnés pour un profil. Pour savoir quels moniteurs sont disponibles, voir «Moniteurs Internet Service Monitoring disponibles», à la page 312.
7. Cliquez sur **Terminé**.
8. Cliquez sur l'icône  .
9. Dans la zone **Filtrer**, recherchez les profils utilisateur par leur nom.
10. Pour déployer le profil créé sur un système géré, cochez la case correspondant aux profils créés qui doivent être configurés et sélectionnez un système géré. Cliquez sur **Déployer** pour déployer le profil sur le système géré que vous avez choisi.

Modification des profils
Tous les profils utilisateur créés sont modifiables.

Pourquoi et quand exécuter cette tâche

Pour modifier les profils, procédez comme suit :

Procédure

1. Sélectionnez le **nom du profil** et cliquez sur  .
2. Sélectionnez un service à modifier et cliquez sur **Editer**.

   a. Ajoutez un moniteur à l'aide de l'icône  et supprimez un moniteur à l'aide de l'icône 

   b. Pour renommer un profil, cliquez deux fois sur la zone de texte **Profile Name**, modifiez son nom et cliquez sur **Rename Profile**.
3. Modifiez les valeurs pour le service sélectionné.

   Remarque :

   - Pour pouvoir modifier la zone du mot de passe, cliquez deux fois sur la zone de texte **nom d'utilisateur**. L'utilisateur peut modifier ou ajouter un nom d'utilisateur et modifier le mot de passe.
   - Pour pouvoir modifier la zone **sslkeypassword**, cliquez deux fois sur son texte pour modifier la clé confidentielle.

4. Cliquez sur **Sauvegarder**, puis sur l'icône pour actualiser l'écran.

Programmation d'un profil
Les profils créés peuvent être planifiés en vue de leur déploiement à une date et heure données.

Pourquoi et quand exécuter cette tâche

Pour planifier les profils, procédez comme suit :

Procédure

1. Sélectionnez le **nom du profil**.
2. Cliquez sur le bouton **Planifier**.
3. Planifiez le profil en sélectionnant le jour en face de l'heure. L'utilisateur peut faire glisser la grille pour sélectionner une heure voulue.
4. Cliquez sur **Sauvegarder**.
5. Cliquez sur l'icône pour actualiser l'écran.

Suppression d'un profil
Les profils créés peuvent être supprimés définitivement.

Pourquoi et quand exécuter cette tâche

Pour supprimer le profil, procédez comme suit :

Procédure

1. Sélectionnez le **nom du profil**.
2. Cliquez sur l'icône pour supprimer le profil.

Groupes d'ID objet
Les groupes d'ID objet sont des paramètres facultatifs propres au moniteur. Ils définissent un ou plusieurs ID objet d'un objet MIB d'une unité. Le moniteur SNMP utilise les groupes d'ID objet pour extraire des données des objets MIB dont les ID objet apparaissent dans un groupe d'ID objet spécifié.

Les détails des objets MIB à partir desquels le moniteur extrait des données sont les suivants :

- Valeur d'ID objet

  Identificateur numérique de l'instance d'objet MIB exprimé à l'aide de la notation ASN.1, par exemple `.1.3.6.1.2.1.1.2.0` ou à l'aide du nom d'objet, par exemple `sysObjectID.0`

  Remarque : Remarque : lors de l'utilisation d'une notation ASN.1, vous devez inclure le caractère `.` au début de l'ID objet.

  Remarque : Vous pouvez utiliser un nom d'instance d'objet uniquement pour définir la valeur d'ID objet si le document MIB qui définit le nom est accessible par le moniteur. Le répertoire par défaut des documents MIB est `$ISHOME/mibs`.
- Nom d'ID objet

  Nom de l'objet MIB, par exemple `sysObjectID`. Ce nom est utilisé dans les classifications des niveaux de services dans les éléments de moniteur `$oidName`*n*.
- Unité d'ID objet

  Unités des données se trouvant dans l'objet MIB. Par exemple, secondes, octets ou bits par seconde (BPS). Sélectionnez BPS pour activer le calcul des bits par seconde pour l'ID objet. Les valeurs de bits par seconde sont calculées de la manière suivante :

  ```
  valeur_interrogation_en_cours - valeur_interrogation_précédente) / intervalle_interrogation *
  8
  ```

- Sélecteur

  Valeur d'index de l'objet MIB. Le tableau suivant présente un exemple où le sélecteur recherche la valeur `FastEthernet0/1` sur toutes les lignes `ifDescr`, ce qui donne un index de ligne 2. La recherche porte ensuite sur la ligne `ifPhysAddress.2`, ce qui renvoie la valeur `0:6:53:34:d2:a1`. L'index 2 n'est pas directement spécifié. Ainsi, si l'index de `FastEthernet0/1` change, il n'est pas nécessaire de reconfigurer les groupes d'ID objet.

Tableau 33. Utilisation de la valeur d'index

Objet MIB	**Valeur d'objet MIB**
Valeur d'ID objet	`ifPhysAddress`
Nom d'ID objet	`FastEthernet0/1PhysicalAddress`
Unité d'ID objet	`chaîne`
Sélecteur	`ifDescr=FastEthernet0/1`

Création d'un groupe d'ID objet et d'un objet MIB

Les groupes d'ID objet sont créés de manière globale et peuvent être utilisés par tous les profils utilisateur qui surveillent les périphériques SNMP

Procédure

Pour créer un groupe d'ID objet et un objet MIB, suivez la procédure ci-dessous.

1. Cliquez sur le bouton **OIDs** pour créer un groupe d'ID objet dans le tableau de bord de l'agent Internet Service Monitoring.
2. Cliquez sur l'icône ⊕ et entrez le nom du groupe d'ID objet dans la zone **OID Group Name**.
3. Cliquez sur l'icône ⊕ pour ajouter l'objet MIB.
   a. Entrez la **valeur**, le **nom**, l'**unité** et le **sélecteur** de l'objet MIB.
   b. Cliquez sur **Ajouter**.

   L'objet MIB est créé.
4. Cliquez sur l'icône ↻ pour actualiser l'écran.

   Le groupe d'ID objet est créé
5. Sélectionnez un **nom de groupe d'ID objet** et cliquez sur **Afficher** pour afficher la liste de tous les objets MIB créés sous le **groupe d'ID objet** sélectionné.
6. Cliquez sur **Fermer**.

Edition d'un groupe d'ID objet et d'un objet MIB

Vous pouvez éditer les groupes d'ID objet. Il est également possible de modifier les objets MIB lors de la création du groupe d'ID objet ou après la création de ce dernier.

Procédure

Pour éditer un groupe d'ID objet, suivez la procédure ci-dessous.

1. Cliquez sur le bouton **OIDs** pour éditer un groupe d'ID objet dans le tableau de bord de l'agent Internet Service Monitoring.
2. Sélectionnez le nom du groupe d'ID objet dans la liste **OID Group Name** et cliquez sur l'icône ✎.
3. Sélectionnez la valeur dans la zone **Edit OID Group** et cliquez sur l'icône ✎.
4. Modifiez les zones de l'objet MIB conformément à vos exigences et cliquez sur le bouton **Sauvegarder**.
5. Cliquez sur **Sauvegarder** dans la page en incrustation **OID Groups**.
6. Cliquez sur **Fermer**.

Suppression d'un groupe d'ID objet
Les objets MIB se trouvent dans des groupes d'ID objet et sont utilisés par le moniteur SNMP pour obtenir des données. Vous pouvez supprimer des objets MIB individuels à partir d'un groupe d'ID objet ou supprimer tous les objets MIB en supprimant l'intégralité du groupe d'ID objet.

Procédure

Pour supprimer un groupe d'ID objet, suivez la procédure ci-dessous.

1. Cliquez sur le bouton **OIDs** dans le tableau de bord de l'agent Internet Service Monitoring.
2. Sélectionnez le nom du groupe d'ID objet dans la liste **OID Group Name** et cliquez sur l'icône  .
   Le groupe d'ID objet associé à l'objet MIB est supprimé.
3. Cliquez sur **Fermer**.

Suppression d'un objet MIB

Procédure

Pour supprimer le groupe MIB, suivez la procédure ci-dessous.

1. Pour supprimer l'objet MIB, cliquez sur le bouton **OIDs** dans le tableau de bord de l'agent Internet Service Monitoring.
2. Sélectionnez le nom du groupe d'ID objet dans la liste **OID Group Name** et cliquez sur l'icône  .
3. Sélectionnez la valeur de l'objet MIB et cliquez sur l'icône  .
   L'objet MIB est supprimé.
4. Cliquez sur **Sauvegarder** dans la page en incrustation **Edit OID Group**.
5. Cliquez sur **Fermer**.

Moniteurs Internet Service Monitoring disponibles
L'ensemble des moniteurs Internet Service Monitoring agent couvre une large gamme de services Internet.

Le tableau suivant répertorie les moniteurs disponibles avec l'Internet Service Monitoring agent et les types de service surveillés.

Tableau 34. Moniteurs de service Internet disponibles

Nom de contrôleur	**Type de service contrôlé**
DHCP	Dynamic Host Configuration Protocol. Pour configurer DHCP, voir «Moniteur DHCP», à la page 326.
DNS	Domain Name Service. Pour configurer DNS, voir «Moniteur DNS», à la page 328.
FTP	File Transport Protocol. Pour configurer FTP, voir «Moniteur FTP», à la page 333.
HTTP	HyperText Transport Protocol. Pour configurer HTTP, voir «Moniteur HTTP», à la page 338.
HTTPS	HyperText Transport Protocol (Secure). Pour configurer HTTPS, voir «Moniteur HTTPS», à la page 348.

Tableau 34. Moniteurs de service Internet disponibles (suite)	
Nom de contrôleur	**Type de service contrôlé**
ICMP	Internet Control Message Protocol. Pour configurer ICMP, voir «Moniteur ICMP», à la page 353.
LDAP	Lightweight Directory Access Protocol. Pour configurer LDAP, voir «Moniteur LDAP», à la page 359.
IMAP4	Internet Message Access Protocol. Pour configurer IMAP4, voir «Moniteur IMAP4», à la page 365.
NTP	Network Time Protocol. Pour configurer NTP, voir «Moniteur NTP», à la page 370.
NNTP	Network News Transport Protocol. Pour configurer NNTP, voir «Moniteur NNTP», à la page 373.
POP3	Post Office Protocol. Pour configurer POP3, voir «Moniteur POP3», à la page 378.
RADIUS	Remote Authentication Dial-In User Service. Pour configurer RADIUS, voir «Moniteur RADIUS», à la page 383.
RPING	Remote Ping (Cisco, Juniper et RFC2925). Pour configurer RPING, voir «Moniteur RPING», à la page 388.
RTSP	Real-Time Streaming Protocol. Pour configurer RTSP, voir «Moniteur RTSP», à la page 393.
SAA	Cisco Service Assurance Agent. Pour configurer SAA, voir «Moniteur SAA», à la page 398.
SIP	Session Initiation Protocol. Pour configurer SIP, voir «Moniteur SIP», à la page 414
SMTP	Simple Mail Transport Protocol. Pour configurer SMTP, voir «Moniteur SMTP», à la page 419.
SNMP	Simple Network Management Protocol. Pour configurer SNMP, voir «Moniteur SNMP», à la page 424.
SOAP	XML-based messaging protocol. Pour configurer SOAP, voir «Moniteur SOAP», à la page 429.
TCPPort	Transmission Control Protocol. Pour configurer TCPPort, voir «Moniteur TCPPort», à la page 434

Tableau 34. Moniteurs de service Internet disponibles (suite)	
Nom de contrôleur	**Type de service contrôlé**
TFTP	Trivial File Transfer Protocol. Pour configurer TFTP, voir «Moniteur TFTP», à la page 437.
TRANSX	Transactions. Pour configurer TRANSX, voir «Moniteur TRANSX», à la page 442.

Fichiers

Fichier exécutable

Chaque moniteur de service Internet est constitué d'un fichier exécutable, d'un fichier de propriétés, d'un fichier de règles et d'un fichier journal.

Les fichiers exécutables du moniteur se trouvent dans le répertoire `$ISHOME/platform/arch/bin`. La valeur `arch` est le code d'architecture du système d'exploitation Windows - `win 32`.

Fichier de propriétés

Le fichier des propriétés est un fichier texte qui comporte des paramètres par défaut précédés du symbole dièse.

Pour modifier un paramètre, vous pouvez soit modifier le paramètre par défaut et supprimer le dièse, soit copier et coller la ligne contenant le paramètre au-dessous des paramètres par défaut, puis effectuer la modification et supprimer le symbole dièse. Cela permet de restaurer les valeurs par défaut ultérieurement. Les fichiers de propriétés du moniteur se trouvent dans le répertoire `$ISHOME/etc/props`.

Fichier de règles

Les fichiers de règles sont similaires aux fichiers de règles de sonde IBM Application Performance Management Netcool/OMNIbus. Pour plus d'informations sur leur syntaxe, reportez-vous au document *IBM Application Performance Management Netcool/OMNIbus Probe and Gateway Guide*.

Les fichiers de règles du moniteur se trouvent dans le répertoire `$ISHOME/etc/rules`.

Fichier journal

Les fichiers journaux stockent les messages concernant l'opération du moniteur.

Les fichiers journaux du moniteur se trouvent dans le répertoire `$ISHOME/log`. La propriété `MessageLog` détermine l'emplacement et le nom du fichier journal. La propriété `MessageLevel` sélectionne le niveau d'information écrit sur le fichier journal, par exemple, les messages de débogage détaillés ou les messages d'erreur fatale. La propriété `MaxLogFileSize` détermine la taille du fichier journal avant le report.

Le nom par défaut du fichier journal est `nom.log` où *nom* correspond au nom du moniteur.

Fonctions communes

Un certain nombre de fonctions sont communes à tous les moniteurs de services Internet. Elles incluent des propriétés, les résultats produits par les moniteurs et les messages d'état.

Cette section décrit les propriétés de tous les moniteurs. Les propriétés de moniteurs spécifiques sont décrites dans la section dédiée au moniteur individuel.

Les paramètres de propriété par défaut sont mis en évidence dans le tableau suivant, le cas échéant.

Tableau 35. Propriétés communes

Nom de la propriété	Paramètre de la propriété	Description
AddRoute	0|1	Crée une route entre l'adresse IP de l'interface réseau utilisée par le moniteur et l'adresse IP de l'hôte surveillé. 0 - désactivé 1 - activé (le moniteur utilise la route spécifiée dans l'élément de profil et non une autre interface réseau). **Remarque :** Cette propriété n'est pas prise en charge sur les plateformes AIX et HP-UX.
BridgeIPAddress	non applicable	Indique l'adresse IP du Databridge. Cette propriété n'est pas configurable ; le Databridge se trouve toujours sur l'hôte local.
BridgePort	entier	Numéro de port utilisé par le Databridge. Définissez cette propriété sur une valeur identique à celle de la propriété SocketPort du Databridge. Valeur par défaut : 9510
BridgeSSLAuthenticatePeer	0|1	Si vous voulez configurer l'authentification SSL entre le moniteur et le pont ou entre le pont et l'agent, définissez BridgeSSLAuthenticatePeer sur 1 et redémarrez le pont. Cette action permet d'authentifier les certificats du serveur. Des certificats sont stockés dans BridgeSSLTrustStore. 0 - désactivé 1 - activé
BridgeSSLCertificateFile	chaîne	Indique le chemin et le nom de fichier du certificat SSL Bridge numérique. Valeur par défaut : $ISHOME/certificates/monitorCert.pem
BridgeSSLCipherSet	chaîne	Définit un ensemble de chiffrements. Si vous modifiez cette valeur, utilisez la syntaxe de chiffrement définie dans la documentation OpenSSL. **Remarque :** Définissez la même valeur sur l'agent Internet Service Monitoring, tous les moniteurs et Databridge. Valeur par défaut : RC4:3DES:DES:+EXP

Tableau 35. Propriétés communes (suite)

Nom de la propriété	Paramètre de la propriété	Description
BridgeSSLDisableSSLv2	0|1	Détermine quels types de socket sont acceptés. • Si elle est définie sur 0, SSLv2 et SSLv3 sont acceptés. • Si elle est définie sur 1, seuls des sockets SSLv3 sont ouverts. **Restriction :** Définissez la même valeur sur l'agent Internet Service Monitoring, tous les moniteurs et Databridge.
BridgeSSLEncryption	0|1	Active le chiffrement SSL Bridge. Définissez cette propriété sur une valeur identique à celle de la propriété Databridge correspondante. 0 - désactivé 1 - activé **Remarque :** Définissez la même valeur pour tous les moniteurs.
BridgeSSLKeyFile	chaîne	Chemin et nom du fichier de clé privée SSL Bridge. Valeur par défaut : $ISHOME/certificates/monitorKey.pem
BridgeSSLKeyPassword	chaîne	Mot de passe utilisé pour chiffrer la clé privée SSL Bridge. Valeur par défaut : tivoli

Tableau 35. Propriétés communes (suite)

Nom de la propriété	Paramètre de la propriété	Description
BridgeSSLTruststore	chaîne	Chemin et nom du fichier de certificat sécurisé pour l'authentification. Nécessaire uniquement lorsque le paramètre BridgeSSLAuthenticatePeer est utilisé. Si vous voulez configurer l'authentification SSL entre le moniteur et le pont ou entre le pont et l'agent, définissez BridgeSSLAuthenticatePeer sur 1 et redémarrez le pont. Cette action permet d'authentifier les certificats du serveur. Vous pouvez stocker des certificats dans SSLTrustStoreFile et SSLTrustStorePath. Valeurs par défaut : • SSLTrustStoreFile, $ISHOME/certificates/trust.pem • SSLTrustStorePath, $ISHOME/certificates/ Pour ajouter de nouveaux certificats, effectuez l'une des étapes suivantes : • Ajoutez un certificat à la fin de la liste dans le fichier texte SSLTrustStoreFile. • Ajoutez un certificat au répertoire SSLTrustStorePath et exécutez la commande OpenSSL c_rehash *rép_certificat* pour hacher les certificats.
BridgeTimeout	entier	Délai d'attente, en secondes, par le moniteur d'une réponse du Databridge.
ConfigFile	chaîne	Utilisé pour pointer vers un fichier de configuration de surveillance. Valeur par défaut : blanc (chaîne vide).
ConfigurationCheckInterval	entier	Intervalle (en secondes) auquel le moniteur recherche des modifications du profil. Valeur par défaut : 1
Datalog	0|1	Oblige le moniteur à consigner les données de performance dans un fichier datalog. Les données de performance sont consignées dans : $ISHOME/datalogs/*profil_utilisateur* 0 - désactivé 1 - activé

Tableau 35. Propriétés communes (suite)		
Nom de la propriété	**Paramètre de la propriété**	**Description**
DatalogFormat	chaîne	Définit le format du fichier datalog. Le paramètre est une liste d'éléments séparés par des espaces, dont les valeurs doivent être stockées dans le fichier datalog. Pour chaque interrogation, le résultat est écrit dans le fichier datalog, l'heure en cours ($time) et la durée ($totalTime) sont consignées, suivies de tous les éléments définis dans cette propriété.
DatalogNameFormat	chaîne	Format du nom de fichier datalog.
Domain	chaîne	Indique le nom de domaine de l'hôte exécutant le moniteur. Si cette propriété n'est pas définie, le moniteur tente de déterminer le nom de domaine à l'aide des configurations NIS et DNS.
DumpProps	non applicable	Affiche une liste de toutes les propriétés d'un moniteur.
FullHostInfo	0|1	Indique si l'élément $host doit être mappé à un élément d'adresse IP $hostIP (si $host est un nom DNS) ou à un élément de nom DNS (si $host est une adresse IP). 0 - désactivé 1 - activé **Remarque :** Non disponible dans le moniteur TRANSX.
GroupID	chaîne	ID de groupe sous lequel le moniteur doit être exécuté.
Aide	0|1	Affiche l'aide des options de ligne de commande sans exécuter le moniteur. 0 - désactivé 1 - activé
IdentifierChecksumFields	chaîne	Déprécié.
IgnoreUnmatchedDVC	0|1	Si une classification de niveau de service particulière n'obtient pas de correspondance (élément non créé par le moniteur), ignorez cet élément dans le calcul du niveau de service. **Conseil :** Dans les versions précédentes de Internet Service Monitoring agent, les classifications de niveau de service étaient appelées DVC (Discrete Value Classifications). 0 - désactivé 1 - activé

Tableau 35. Propriétés communes (suite)

Nom de la propriété	Paramètre de la propriété	Description
IpAddress	chaîne	Indique l'adresse IP de l'interface réseau utilisée par le moniteur pendant les tests. Si cette propriété n'est pas définie, le moniteur tente de déterminer l'adresse IP de la machine hôte à l'aide d'une recherche de nom d'hôte. Cette tentative peut échouer si la machine hôte possède plusieurs interfaces réseau.
Manager	chaîne	Indique le nom de l'application de gestion utilisée dans la déduplication de l'événement ObjectServer.
MaxCCA	entier	Définit le nombre maximal de connexions simultanées que peut avoir le moniteur à un moment donné. Notez que si vous définissez une valeur trop élevée, vous pouvez gravement affecter les performances du moniteur. Cette propriété n'est pas disponible pour le moniteur ICMP. Valeur par défaut : 10
MaxLogFileSize	entier	Taille maximale (en octets) du fichier journal. Valeur par défaut : 1 048 576
MessageLevel	chaîne	Niveau le plus grave des messages à envoyer au journal des messages. Les valeurs, par ordre croissant de gravité sont : debug, info, warn, error et fatal. Valeur par défaut : warn
MessageLog	chaîne	Emplacement du fichier journal. Valeur par défaut : $ISHOME/log/*moniteur*.log
MinPoll	entier	Définit l'intervalle d'interrogation minimum autorisé. Si les fichiers de configuration de surveillance ont un intervalle d'interrogation inférieur à la valeur définie, la valeur du fichier de configuration est substituée. Valeur par défaut : 60
MsgDailyLog	entier	Active la génération d'un fichier journal quotidien. Valeur par défaut : 0 - Journal quotidien désactivé

Tableau 35. Propriétés communes (suite)

Nom de la propriété	Paramètre de la propriété	Description
`MsgTimeLog`	chaîne	Indique l'heure (au format 24 heures `HHMM`) après laquelle le moniteur génère un journal quotidien, si MsgDailyLog est activée. Valeur par défaut : `0000` - 12 minuit
`Nom`	chaîne	Nom du moniteur. Définir cette propriété rétablit la valeur par défaut des propriétés `PropsFile`, `RulesFile` et `MessageLog`.
`NewProfileCheckMultiple`	entier	Multiple qui indique la fréquence à laquelle le moniteur vérifie les nouveaux fichiers de configuration lorsqu'il vérifie les modifications de profil. Valeur par défaut : `10`
`NoRecover`	entier	Ordonne au moniteur de ne pas récupérer le fichier SAF. Valeur par défaut : `0` - la reprise n'est pas supprimée
`Pause`	entier	Définit l'intervalle (en secondes) auquel un moniteur génère des unités d'exécution. La définition de cette propriété sur des valeurs élevées, 100 ou plus par exemple, force le moniteur à générer des unités d'exécution à une fréquence inférieure. En règle générale, augmenter cette valeur n'est nécessaire que sur des systèmes lents. Cette propriété n'est pas prise en charge pour le moniteur ICMP. Valeur par défaut : `50`
`PreviousFields`	chaîne	Les éléments indiqués par cette propriété (au format "`<element>, <element>, …`") sont stockés pour un sondage et précédés de la chaîne `previous`.
`Profile`	chaîne	Nom du ou des profils client à utiliser. La chaîne peut être un nom de profil unique, une liste de noms de profils séparés par des espaces ou un astérisque (`*`) qui force le moniteur à utiliser tous les profils disponibles. Valeur par défaut : `*`

Tableau 35. Propriétés communes (suite)

Nom de la propriété	Paramètre de la propriété	Description
`ProfileUpdateTimeout`	entier	Nombre de millisecondes pendant lesquelles un fichier de profil doit rester statique avant de pouvoir être lu par un moniteur, puis mis à jour. La plage autorisée est comprise entre `1-20000` millisecondes. Valeur par défaut : `100`
`PropsFile`	chaîne	Nom du fichier de propriétés. Valeur par défaut : `$ISHOME/etc/props/`*`moniteur`*`.props`
`QFile`	chaîne	Définit le nom du fichier SAF. Valeur par défaut : `$ISHOME/var/`*`moniteur`*`.saf`.
`QSize`	entier	Définit la taille réservée (en octets) du fichier SAF. Valeur par défaut : `10240000`
`ID utilisateur`	chaîne	ID utilisateur sous lequel le moniteur doit être exécuté. **Remarque :** N'utilisez pas cette propriété avec le moniteur DHCP.
`Version`	non applicable	Imprime la version du moniteur sans exécuter ce dernier.

Eléments de moniteur communs

Cette section décrit les éléments générés par tous les moniteurs. Les éléments propres à un moniteur sont décrits dans les sections consacrées à chaque moniteur. Les éléments produits peuvent être affichés dans le tableau de bord de l'agent Internet Service Monitoring.

Si vous utilisez IBM Application Performance Management, les éléments pouvant être affichés dans les espaces de travail en tant qu'attributs sont déterminés par un fichier de mappage généré par l'agent Internet Service Monitoring. Ce fichier de mappage n'est pas configurable.

Le Tableau 36, à la page 322 répertorie les éléments générés par tous les moniteurs. Les éléments indiqués par un astérisque (*) sont disponibles en tant qu'attributs d'espace de travail. Le nom des attributs est affiché entre parenthèses. L'absence d'astérisque indique qu'il n'existe pas d'attribut d'espace de travail équivalent. Les attributs placés entre parenthèses mais sans élément indiquent qu'ils sont disponibles uniquement en tant qu'attributs d'espace de travail, il n'existe pas d'élément équivalent.

Tableau 36. Eléments de moniteur communs	
Nom de l'élément.	**Description de l'élément**
$consecutiveFailures	Si la valeur $failureRetests est différente de zéro et que le test échoue en termes de classification du niveau de service, cet élément est créé à partir de la valeur 1. La valeur augmente jusqu'à ce que le test n'échoue plus, point auquel $consecutiveFailures est défini sur 0, ou jusqu'à l'interrogation suivante. Si, lors de cette interrogation, le niveau de service est atteint ou recommence à augmenter, l'élément n'est plus créé. Si la valeur de cet élément dépasse la valeur de $failureRetests, la valeur de $consecutiveFailures revient à 1. **Remarque :** Le moniteur TRANSX ne génère pas cet élément.
$datalogPath* (guid)	Chemin du fichier datalog utilisé par le moniteur. L'attribut d'espace de travail utilise les 100 derniers caractères du chemin.
$description* (Description)	Contient la description sous forme de texte fournie dans la zone **Description** de l'élément de profil du moniteur.
$failureRetestInterval	Intervalle d'interrogation utilisé lors de la nouvelle tentative de test de l'incident. Ce paramètre est valide uniquement si $failureRetests a une valeur supérieure à 0. Si l'intervalle de nouveau test est supérieur à l'intervalle d'interrogation normal, il redevient égal à ce dernier. **Remarque :** Le moniteur TRANSX ne génère pas cet élément.
$failureRetests	Nombre d'incidents de niveau de service à dépasser avant qu'un événement ayant échoué soit enregistré et envoyé à ObjectServer. **Remarque :** Le moniteur TRANSX ne génère pas cet élément.
$host* (Host)	Nom de l'hôte ou du serveur. Il est stocké dans le fichier de configuration.
$hostName	Contient le nom d'hôte de l'élément $host (si $host est une adresse IP).
$hostIP	Contient l'adresse IP hôte de $host (si $host est un nom DNS).
$identchecksum* (Identchecksum)	Identificateur de l'élément de profil.
$lastServiceLevel* (LastServiceLevel)	Numéro de niveau de service de l'interrogation précédente. Cette valeur est effacée si le profil change.
$lastServiceLevelCounter	Elément serviceLevelCounter de l'interrogation précédente. Cette valeur est redéfinie si le profil est modifié.

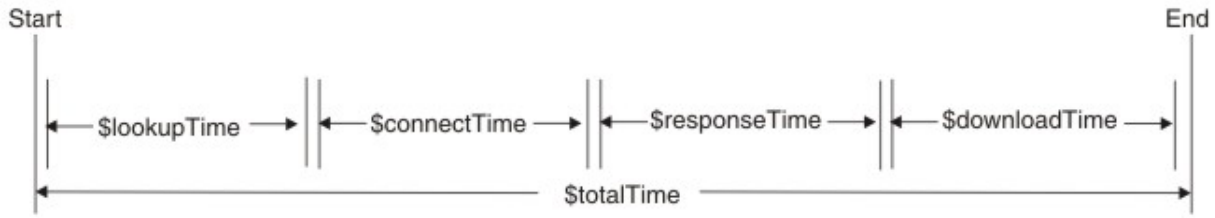
Tableau 36. Eléments de moniteur communs (suite)

Nom de l'élément.	**Description de l'élément**
$monitorDNSdomain	Nom de domaine de la machine exécutant le moniteur, tel qu'il est utilisé par le système de noms de domaine.
$monitorHost* (MonitorLocation)	Nom de l'hôte exécutant le moniteur.
$monitorNISdomain	Nom de domaine de l'hôte exécutant le moniteur, tel qu'il est utilisé par NIS (Network Information Service).
$monitorDomain	Remplace les paramètres $monitorDNSdomain et $monitorNISdomain.
$message* (ResultMessage)	chaîne de texte décrivant le résultat de l'interrogation. Par exemple, Echec de la connexion, OK ou Réussite.
(Node)	Nom du système sur lequel Internet Service Monitoring s'exécute. Cet attribut est ajouté par l'agent Internet Service Monitoring.
$pollInterval	Intervalle d'interrogation spécifié dans chaque moniteur.
$resultString* (ResultString)	Chaîne de texte indiquant la classification des niveaux de services appliquée aux résultats de l'interrogation. Par exemple, TotalTime > 20.
$service* (Service)	Nom du service surveillé. Par exemple, FTP ou HTTP.
$serviceLevel* (ServiceLevel)	Numéro du niveau de service de l'interrogation, tel qu'il est défini dans la classification des niveaux de services : 0 - Unknown 1 - Good 2 - Marginal 3 - Failed
$serviceLevelCounter	Nombre de fois que le numéro du niveau de service n'a pas changé.
(ServiceLevelString)	Chaîne associée au niveau de service renvoyé (Unknown, Good, Marginal ou Failed).
$startTimePoll	Heure de début de l'interrogation.
$time	Heure UNIX, en secondes, à laquelle l'interrogation a été effectuée.
$timeStamp* (Timestamp)	Date et heure d'exécution du test. Le format d'horodatage utilise des paramètres locaux.
$transxName	Nom de la transaction. Il est généré par un moniteur si celui-ci est utilisé dans une transaction.

Tableau 36. Eléments de moniteur communs (suite)	
Nom de l'élément.	**Description de l'élément**
Détails du profil	
`$profile*` (`IsmProfile`)	Nom du profil utilisateur.
Durées - Pour plus d'informations sur la méthode de mesure des durées, voir «Calculs des délais», à la page 324.	
`$timeout`	Délai de réponse du serveur, en secondes. Extrait du fichier de configuration.
`$totalTime*` (`TotalTime`)	Durée totale, en secondes, nécessaire à l'exécution d'une opération. Elle inclut toutes les durées de consultation, de connexion et de téléchargement le cas échéant, ainsi que le temps de traitement intermédiaire.

Calculs des délais

Les moniteurs tentent de diviser le délai nécessaire à l'exécution d'une interrogation en différentes étapes temporisées. Par exemple, cela peut inclure le délai nécessaire à l'obtention de l'adresse IP d'un hôte ou le délai nécessaire à l'aboutissement de la connexion à un hôte.



La durée `$totalTime` est toujours légèrement supérieure à la somme des autres durées car elle inclut le temps système utilisé par les activités du moniteur, telles que le traitement des données reçues et l'exécution d'appels système. `$totalTime` est exprimé en secondes.

Messages d'état
Les moniteurs renvoient les messages d'état générés après chaque test du service. Ils indiquent le résultat des tests.

Les messages proviennent généralement du service surveillé ou de l'environnement réseau extérieur au moniteur. Le Tableau 37, à la page 325 décrit les messages d'état communs renvoyés par les moniteurs dans l'attribut `ResultMessage` lors de l'utilisation d'IBM Application Performance Management. Les messages d'état propres à un moniteur sont décrits dans les sections consacrées à chaque moniteur.

Outre les messages fournis par chaque moniteur, certains moniteurs (le moniteur HTTP, par exemple) signalent les messages du système d'exploitation sous-jacent. Par exemple, si la connexion TCP échoue, Internet Service Monitoring agent utilise la chaîne définie par le système d'exploitation, telle que **`connection refused`**, **`timeout`**, **`network unreachable`**.

Tableau 37. Messages d'état communs

Message	**Description**
OK	La demande émanant du moniteur a abouti. Les moniteurs peuvent avoir d'autres messages d'état qui indiquent l'aboutissement d'un processus. Reportez-vous à la section *Messages d'état* de chaque moniteur.
Received response to request not originating from this monitor - ignored	Le système a reçu une réponse du serveur à un message qui ne provient pas du moniteur désigné.
Connection failed Connect to server failed	Le moniteur n'a pas pu se connecter au serveur. Pour plus d'informations, reportez-vous au fichier journal.
Connection closed unexpectedly	La connexion au serveur a été interrompue.
Connection timed out	La connexion a abouti mais le serveur a cessé de répondre.
Connection closed by foreign host	L'hôte distant a fermé la connexion plus tôt que prévu par le moniteur.
Timed out waiting to read/ write	Une connexion de données au serveur surveillé a été établie, mais elle a cessé de répondre.
No Response from server	Délai d'attente de la demande dépassé.
Format Error Server Failure No such host or domain Not Implemented Request refused Erreur inconnue	Erreur renvoyée par le serveur surveillé.

Tableau 37. Messages d'état communs (suite)	
Message	**Description**

`Network is down`
`Network is unreachable`
`Network dropped connection on reset`
`Software caused connection abort`
`Connection reset by peer`
`Connection timed out`
`Connection refused`
`Host is down`
`No route to host`
`Remote peer released connection`
	Un incident a été détecté sur le réseau.

Moniteur DHCP

Le moniteur DHCP vérifie la disponibilité et le temps de réponse des serveurs DHCP.

Vous affectez les classifications des niveaux de services en fonction du temps nécessaire au serveur DHCP pour répondre à une demande du moniteur DHCP à l'aide du temps total, de recherche ou de réponse.

Tableau 38. Fichiers du moniteur DHCP	
Fichiers du moniteur	**Nom ou emplacement**
Exécutable du moniteur	`nco_m_dhcp`
Fichier de propriétés	`$ISMHOME/etc/props/dhcp.props`
Fichier de règles	`$ISMHOME/etc/rules/dhcp.rules`
Fichier journal	`$ISMHOME/log/dhcp.log`

Consignes de configuration du moniteur DHCP

Le moniteur DHCP teste les services DHCP en se comportant comme un client DHCP limité. Il envoie une demande DHCP INFORM au serveur DHCP cible sur le même réseau en utilisant UDP en tant que protocole de transport via une connexion établie et attend un accusé de réception DHCP correspondant du serveur. Le moniteur ne demande pas d'adresse IP et n'affecte pas l'expiration sur des adresses IP existantes.

Remarque : Les serveurs DHCP surveillés doivent prendre en charge les demandes DHCP INFORM et être compatibles RFC2131.

Le moniteur DHCP doit être exécuté en tant que `root` car il est associé à un port inférieur à 1024.

Limitation

Le moniteur DHCP ne peut utiliser aucune interface réseau configurée à l'aide d'un client DHCP. Il doit être configuré pour utiliser une interface réseau dont l'adresse IP n'est pas affectée dynamiquement.

Configuration du test du service de surveillance DHCP

Tableau 39. Configuration du moniteur DHCP	
Zone	**Description**
server	Nom d'hôte du serveur DHCP. Par exemple : dhcp1.mycompany.com
localip	Interface réseau de l'adresse IP utilisée par le moniteur pour effectuer le test. Par exemple : 192.168.n.n
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément. Par exemple : moniteur DHCP
port	Numéro de port du serveur DHCP ; la valeur par défaut est 67.
localport	Numéro de port utilisé par le moniteur pour effectuer le test ; la valeur par défaut est 68.
timeout	Délai d'attente, en secondes, d'une réponse du serveur ; la valeur par défaut est 30.
retries	Nombre de tentatives de connexion au serveur DHCP que le moniteur doit effectuer avant d'abandonner. La valeur par défaut est 0. Exemple : 2.
poll	Délai, en secondes, entre chaque interrogation du serveur en utilisant l'élément de profil en cours. La valeur par défaut est 300.
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. La valeur par défaut est 0.
retestinterval	Délai, en secondes, entre chaque nouveau test en cas d'incident. La valeur par défaut est 30.

Outre les résultats de test communs à tous les éléments, le moniteur DHCP génère un ensemble de résultats de test contenant les données propres aux tests de service DHCP.

Tableau 40. Eléments du moniteur DHCP	
Elément	**Description**
`$clientIP*ClientIp`	Adresse IP de l'hôte sur lequel le moniteur s'exécute.
`$lookupTime*(LookupTime)`	Temps mis pour obtenir l'adresse IP du serveur hôte.
`$responseTime*ResponseTime`	Délai entre l'établissement de la connexion et la réception du premier octet de données.
`$retries`	Nombre maximal d'entrées, tel que spécifié pendant la configuration du moniteur.
`$router`	Adresse IP du routeur telle que renvoyée par le serveur DHCP.

Messages d'état

Le moniteur DHCP fournit des messages d'état dans l'attribut `ResultMessage` lorsqu'IBM Application Performance Management est utilisé. Ces messages indiquent le résultat du test.

Tableau 41. Messages d'état du moniteur DHCP

Message	**Description**
`Received DHCPACK Received DHCPNAK`	Un serveur DHCP répond à la demande d'informations DHCP envoyée par le moniteur.
`This monitor requires root privileges to run`	Connectez-vous en tant que superutilisateur.
`Did not receive valid DHCP MESSAGE`	Réponse non reconnue du serveur DHCP.
`Did not receive valid DHCP MESSAGE TYPE`	Réponse non reconnue du serveur DHCP (DHCPACK ou DHCPNAK était attendue).
`Invalid transaction ID` `Received response to request not originating from this monitor - ignored`	Une réponse à un message ne provenant pas de ce moniteur a été reçue d'un serveur DHCP .
`Unexpected op-code returned`	Un message imprévu a été reçu sur ce port.
`Connection failed`	Le nom du serveur spécifié n'est pas valide.
`Failed to send request to DHCP server`	Le système d'exploitation ne peut pas identifier précisément la raison pour laquelle la demande n'a pas pu être transmise au serveur et renvoie donc ce message d'état indiquant qu'un problème de réseau s'est produit.
`No Response from server`	Le serveur DHCP ne répond pas.

Moniteur DNS

Le moniteur DNS utilise le service DNS (Domain Name System) pour trouver des informations sur un ou plusieurs hôtes.

Le moniteur DNS utilise soit l'adresse IP de l'hôte pour rechercher le nom de l'hôte, soit le nom de l'hôte pour rechercher l'adresse IP. Le moniteur mesure la performance du service en enregistrant le résultat de la recherche et les temps de réponse. Le moniteur enregistre également des détails sur chaque demande envoyée au serveur.

Tableau 42. Récapitulatif des fichiers du moniteur DNS

Fichiers du moniteur	**Nom ou emplacement**
Exécutable du moniteur	`nco_m_dns`
Fichier de propriétés	`$ISMHOME/etc/props/dns.props`
Fichier de règles	`$ISMHOME/etc/rules/dns.rules`
Fichier journal	`$ISMHOME/log/dns.log`

Consignes de configuration du moniteur DNS

Le moniteur DNS peut être configuré pour rechercher l'adresse IP ou le nom d'hôte de l'hôte cible. En fonction du type de recherche, le moniteur communique avec le serveur DNS différemment.

Recherche d'adresse IP

Lors d'un test de recherche d'adresse IP, un nom d'hôte est attribué au moniteur. Ce nom permet de définir l'emplacement d'une adresse IP.

Le moniteur teste le serveur DNS de la manière suivante :

1. Le moniteur interroge le serveur DNS en utilisant le nom d'hôte complet de HostA (`hosta.dev.net`) pour demander son adresse IP.

   Si le serveur DNS peut définir l'emplacement de l'adresse IP de l'hôte, il est renvoyé au moniteur. Si le serveur DNS ne peut définir l'emplacement de l'adresse IP de l'hôte, il renvoie un message contenant les détails de l'échec de la recherche au moniteur.

   Si la demande arrive à expiration, le moniteur fait de nouvelles tentatives (si de nouvelles tentatives sont configurées). Lorsque toutes les nouvelles tentatives ont été effectuées, le moniteur crée un événement d'échec.

   Si le nom d'hôte indiqué dans la configuration est un nom de domaine, tel que `mycompany.com` et non un nom d'hôte qualifié complet, tel que `hostx.mycompany.com`, le moniteur extrait des informations sur l'intégralité du domaine. Ces informations sont stockées dans deux éléments supplémentaires : `$domainNameServer` et `$domainNameAddr`.
2. Si le message renvoyé au moniteur contient un nom canonique, le moniteur en déduit que le nom indiqué dans le fichier de configuration devait être un alias. Le moniteur envoie le nom canonique au serveur DNS afin de demander l'adresse IP de l'hôte.

   Si le serveur DNS définit l'emplacement de l'adresse IP de l'hôte à l'aide de son nom canonique, il est renvoyé au moniteur. Si le serveur DNS ne peut définir l'emplacement de l'adresse IP de l'hôte, il renvoie un message contenant les détails de l'échec de la recherche au moniteur.
3. Si les deux premières tentatives d'interrogation du serveur DNS n'aboutissent pas, le moniteur envoie l'adresse IP du serveur DNS (`192.168.n.n`) au serveur DNS et demande son nom qualifié complet.

   Si le serveur DNS peut définir l'emplacement de son nom d'hôte complet, ce dernier est renvoyé au moniteur. Si le serveur DNS ne peut définir l'emplacement de son nom d'hôte complet, il renvoie un message contenant les détails de l'échec de la recherche. La demande du nom d'hôte qualifié complet du serveur (une demande de recherche DNS inversée), n'est pas prise en charge sur tous les types de serveurs DNS. Si le serveur DNS cible ne prend pas en charge les recherches inversées, vous pouvez empêcher le moniteur DNS d'envoyer cette demande en définissant la propriété `LookupServerName` sur `0`.

Recherche récursive

Les recherches non récursives présentent une vue précise du mode de fonctionnement du serveur DNS alors que les recherches récursives offrent une meilleure indication des performances DNS obtenues par les applications Internet (et donc les utilisateurs). Le moniteur DNS prend en charge les recherches récursives et non récursives.

Les applications Internet font généralement fonctionner les requêtes DNS de cette manière. Par exemple, un navigateur Web spécifie toujours des recherches récursives lorsqu'il tente de résoudre la partie hôte d'une URL.

Si un serveur DNS ne peut pas répondre à une requête parce que sa base de données ne contient pas d'entrée pour l'hôte, il peut périodiquement interroger les serveurs DNS situés plus hauts dans la hiérarchie.

Types de requête DNS

Le moniteur DNS prend en charge plusieurs types de requête DNS. Utilisez le code de requête lors de la spécification du type de requête DNS.

Tableau 43. Types de requête DNS	
Code de requête	**Type de requête**
A	Host Address
NS	Authoritative name server
MD	Mail destination
MF	Mail forwarder
CNAME	Canonical name for an alias
SOA	Start of a zone of authority
MB	Mailbox domain name
MG	Mail group member
MR	Mail rename domain name.
NULL	Null RR
WKS	Well known service description
PTR	Domain name pointer
HINFO	Host information
MINFO	Mailbox or mail list information
MX	Mail exchange
TXT	Text strings
AXFR	Transfer of an entire zone
MAILB	Mailbox-related records
MAILA	Mail agent RR
ANY	All records

Configuration des tests de service du moniteur DNS

Les paramètres de configuration du moniteur DNS permettent de définir les tests de service DNS.

Tableau 44. Tableau 3. Configuration du moniteur DNS	
Zone	**Description**
server	Adresse IP du serveur DNS principal. Par exemple, 192.168.n.n
host	Nom d'hôte de l'hôte cible. Par exemple, www.mycompany.com
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément. Par exemple, moniteur DNS.
recursivelookups	Active ou désactive les recherches récursives. • `recurse` (utilisez `true` dans ismbatch) • `norecurse` (utilisez `false` dans ismbatch) Valeur par défaut : `recurse`.
port	Port du serveur DNS que le moniteur écoute et dont la valeur par défaut est 53.

Tableau 44. Tableau 3. Configuration du moniteur DNS (suite)	
Zone	**Description**
localip	Spécifie l'adresse IP de l'interface réseau sur la machine hôte à laquelle le moniteur est associé lorsqu'il effectue le test. Si la propriété `IpAddress` du moniteur est définie, elle remplace la valeur de cette zone.
querytype	Type de requête DNS utilisé dans le test. Pour une liste des types de requête pris en charge, voir Tableau 43, à la page 330.
timeout	Délai d'attente, en secondes, avant une réponse du serveur. Valeur par défaut : `10`.
retries	Nombre de tentatives du moniteur pour contacter le serveur DNS avant d'abandonner.
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`.
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`.
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`.

Eléments de contrôle

Outre les résultats de test communs à tous les éléments, le moniteur DNS génère un ensemble de résultats de test contenant les données propres aux tests de service DNS.

Tableau 45. Tableau 4. Eléments du moniteur DNS	
Elément	**Description**
`$authoritative`	Cet élément est créé uniquement si les informations récupérées proviennent d'un serveur DNS de référence. S'il ne s'agissait pas d'un serveur DNS de référence, cet élément n'est pas créé.
`$domainEmailAddr`	Adresse de contact du domaine cible.
`$domainNameServer`	Nom du serveur DNS pour le domaine cible.
`$fromAliasTime`	Durée entre l'émission d'une demande de nom conique, reçu depuis une demande précédente, et la réception d'une adresse IP.
`$localIP`	Adresse IP locale que le moniteur doit utiliser. Cet élément peut être vide sur une machine ayant une seule interface.
`$lookup*(HostLookup)`	Nom d'hôte ou adresse IP de l'hôte cible dont le moniteur tente de définir l'emplacement.
`$lookupCName`	Nom d'hôte officiel de l'hôte cible. Cet élément est créé uniquement si le nom d'hôte officiel est différent du nom d'hôte de `$lookupName`.
`$lookupIP*(HostIp)`	Adresse IP de l'hôte cible.
`$lookupName*(Host)`	Nom d'hôte complet de l'hôte cible.
`$mxRecords`	Nombre d'enregistrements MX trouvés.

Tableau 45. Tableau 4. Eléments du moniteur DNS (suite)	
Elément	**Description**
$port	Port sur lequel le service est surveillé.
$queryType	Type de requête DNS utilisée dans le test. Pour une liste des types de requête pris en charge, Voir Tableau 43, à la page 330 .
$responseTime*(ResponseTime)	Durée entre l'émission par le moniteur d'une demande au serveur DNS et la réception d'une réponse.
$retries	Nombre maximal de nouvelles tentatives, comme indiqué dans l'élément de profil.
$serverIP	Adresse IP du serveur DNS.
$serverName	Nom d'hôte du serveur DNS.
$serverTime	Temps que le serveur passe pour résoudre son propre nom.

Gestion des enregistrements MX

Deux éléments sont créés pour chaque enregistrement MX trouvé par le moniteur DNS : $mxHostn et $mxPreferencen.

$mxHostn stocke le nom d'hôte d'un enregistrement MX. $mxPreferencen contient la préférence de pondération de l'hôte. Le n augmente pour chaque paire d'enregistrement afin de les différencier. Le moniteur stocke le nombre total d'enregistrements MX pour un hôte spécifique dans l'élément $mxRecords. Les paires d'enregistrements sont triées dans l'ordre décroissant des préférences MX.

Message d'état

Le moniteur DNS fournit des messages d'état dans l'attribut ResultMessage lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Tableau 46. Tableau 5. Messages d'état du moniteur DNS	
Message	**Description**
Domain information received	Demande de nom de domaine effectuée.
Success	Demande effectuée.
Invalid Response	Réponse non reconnue du serveur DNS.
Connection failed	Le nom du serveur spécifié n'est pas valide.
No Response from server	Délai d'attente de la demande dépassé.
Failed to send DNS request	Un incident a été détecté sur le réseau.
No such domain (no recursion)	Nom de domaine incorrect.

Propriétés

Les propriétés spécifiques au moniteur DNS sont décrites dans le tableau suivant.

Tableau 47. Propriétés du moniteur DNS		
Nom de la propriété	**Paramètre de la propriété**	**Description**
AcceptCNAME	0|1	Si elle est activée, le moniteur DNS accepte le nom canonique contenu dans la réponse DNS et n'effectue pas d'autres recherches.
DNSQueryType	chaîne	Type de requête DNS utilisée dans les tests. Voir Tableau 43, à la page 330 pour une liste des types de requête pris en charge. Valeur par défaut : ANY.
LookupServerName	0|1	Active la recherche DNS inversée sur l'adresse IP du serveur DNS. 0 - désactivé 1 - activé

Moniteur FTP

Le moniteur FTP teste les services FTP en téléchargeant des fichiers vers ou à partir de serveurs FTP. Il surveille la performance du service en enregistrant le temps de réponse et les taux de transfert des données et surveille l'espace du disque et l'intégrité du fichier.

Tableau 48. Récapitulatif du moniteur FTP	
Fichiers du moniteur	**Nom ou emplacement**
Exécutable du moniteur	nco_m_ftp
Fichier de propriétés	$ISHOME/etc/props/ftp.props
Fichier de règles	$ISHOME/etc/rules/ftp.rules
Fichier journal	$ISHOME/log/ftp.log

Consignes de configuration du moniteur FTP

Le moniteur FTP teste la disponibilité d'un serveur FTP en téléchargeant un fichier sur le serveur à l'aide d'une commande FTP STOR ou en téléchargeant un fichier à partir du serveur à l'aide d'une commande FTP RETR.

Configuration des tests de service du moniteur FTP

Les paramètres de configuration du moniteur FTP sont décrits dans le tableau suivant.

Tableau 49. Configuration du moniteur FTP	
Zone	**Description**
server	Adresse IP du serveur FTP cible ou de la machine à partir de laquelle récupérer des données via FTP. Par exemple : ftp.mycompany.com

Tableau 49. Configuration du moniteur FTP (suite)	
Zone	**Description**
localfile	Pour les opérations GET FTP, cette zone spécifie le nom et le chemin vers lequel le fichier est téléchargé. Pour les opérations PUT FTP, cette zone spécifie le nom et le chemin du fichier qui est chargé sur le serveur FTP. La valeur par défaut est FULL PATHNAME. Par exemple : `$ISMHOME/etc/ism/downloads/ftp-test.tar.Z`
remotefile	Pour les opérations GET FTP, cette zone spécifie le nom et le chemin du fichier téléchargé à partir du serveur. Pour les opérations PUT FTP, cette zone spécifie le nom et le chemin vers lequel le fichier est chargé sur le serveur FTP. La valeur par défaut est FULL PATHNAME. Par exemple : `/sales/prodlist.tar.Z`
description	Zone de texte dans laquelle placer des informations descriptives sur l'élément.
port	Port par défaut utilisé par le serveur FTP. Port par défaut : `21`
username	Nom d'utilisateur permettant de se connecter au serveur FTP cible.
password	Mot de passe permettant de se connecter au serveur FTP cible. Ne remplissez pas cette zone si le compte FTP ne requiert pas de mot de passe.
command	Commande FTP pour le moniteur à utiliser : • GET ou RECV - Téléchargement d'un fichier à partir du serveur FTP cible • SEND ou PUT - Chargement d'un fichier vers le serveur FTP cible Valeur par défaut : GET.
conntype	Spécifie le type de connexion pour le moniteur afin d'établir une connexion au serveur lors de la tentative de transfert du fichier : • `Rapports actifs` • `Passif` Valeur par défaut : `Actif`
timeout	Délai d'attente, en secondes, avant une réponse du serveur. Valeur par défaut : `30`.
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`.

Tableau 49. Configuration du moniteur FTP (suite)	
Zone	**Description**
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`.

Correspondance d'expressions régulières

Vous pouvez effectuer une recherche d'expression régulière sur les informations téléchargées en entrant jusqu'à 50 expressions régulières différentes. Le moniteur FTP tente de faire correspondre le contenu extrait à chaque expression régulière.

Si une correspondance d'une expression régulière indiquée est trouvée, les lignes correspondantes (ou le nombre maximal de lignes correspondantes pouvant être stockées dans la mémoire tampon interne du moniteur) sont renvoyées dans l'élément `$regexpMatchn` correspondant. Si l'expression régulière a plusieurs correspondances dans les informations téléchargées, seule la première correspondance est renvoyée. L'état de chaque test d'expression régulière est indiqué par les éléments `$regexpStatusn`. Vous pouvez utiliser les correspondances d'expression régulière et les informations d'état en tant que critères pour les classifications de niveau de service.

Les expressions régulières effectuent la correspondance de chaînes pour le contenu téléchargé lors des tests de service. Ces expressions peuvent contenir un ou plusieurs opérateurs d'expression réguliers, qui déterminent le contenu à vérifier par l'expression.

Remarque : La syntaxe de l'expression régulière peut être utilisée pour correspondre à des chaînes sur des lignes uniques seulement. Internet Service Monitoring ne peut pas établir de correspondance avec des chaînes qui incluent de nouvelles lignes ou des retours chariot. Utilisez plusieurs expressions régulières pour établir des correspondances avec des chaînes qui s'étendent sur plusieurs lignes. Vous pouvez également utiliser des règles SLC pour déclencher des alarmes en fonction du résultat de plusieurs expressions régulières.

Tableau 50. Opérateurs génériques	
Caractère	**Description**
.	Correspond à un caractère. Par exemple, l'expression régulière `r.t` correspond aux chaînes `rat`, `rut`, `r t`, mais non à `root`.
$	Correspond à la fin d'une ligne. Par exemple, l'expression régulière dog$ correspond à la fin de la chaîne `it's a dog` mais non à la chaîne `There are a lot of dogs`.
^	Correspond au début d'une ligne. Par exemple, l'expression régulière `^When in` correspond au début de la chaîne `When in the course of human events` mais non à `What and When in the`.
*	Ne correspond à aucune occurrence ou à plusieurs occurrences du caractère précédant. Par exemple, l'expression régulière `.*` correspond à un nombre indéfini de caractères.
\	Traite le caractère suivant en tant que caractère ordinaire. Par exemple, `\$` correspond au caractère dollar $ et non à la fin d'une ligne. De même, l'expression `\.` correspond au point et non à un seul caractère.

Tableau 50. Opérateurs génériques (suite)	
Caractère	**Description**
`[]`	Correspond à un des caractères compris entre crochets. Par exemple, l'expression régulière `r[aou]t` correspond à `rat`, `rot`, et `rut` mais non à `rit`. Indiquez des plages de caractères en utilisant un tiret. Par exemple, l'expression régulière `[0-9]` correspond à tout chiffre. Vous pouvez également spécifier plusieurs plages. Par exemple, l'expression régulière `[A-Za-z]` correspond à une lettre majuscule ou minuscule.
`|`	Correspond à des phrases contenant une des conditions spécifiées. Par exemple, `him|her` correspond à la ligne `it belongs to him` et à la ligne `it belongs to her`, mais non à la ligne `it belongs to them`.

Remarque : Si vous préférez placer les chaînes de données de sortie entre `accolades {}` ou `guillemets doubles ""`, vous devez ajouter le caractère d'échappement `barre oblique inversée \` avant chaque `accolade` et chaque `guillemet double` dans l'expression régulière.

Par exemple, si la chaîne de données est `{"templates":true,"mongodb":true,"ldap":true,"ucd":true,"github":true}`, l'expression régulière doit être `\{\"templates\":true,\"mongodb\":true,\"ldap\":true,\"ucd\":true,\"github\":true\}`

Eléments du moniteur

Outre les résultats de test communs à tous les éléments, le moniteur FTP génère un ensemble de résultats de test contenant les données propres aux tests de service FTP.

Tableau 51. Eléments du moniteur FTP	
Elément	**Description**
`$bytesPerSec*(BytesPerSec)`	Nombre moyen d'octets transférés par seconde.
`$bytesTransfered*(BytesTransferred)`	Nombre d'octets transférés ou téléchargés.
`$checksum`	Généralement, l'élément Checksum ne fournit pas de valeurs significatives pour les classifications de niveau de service car les valeurs de car les valeurs de total de contrôle sont inconnues au moment de la création de l'élément de profil (le moniteur calcule les valeurs de total de contrôle pendant l'exécution des tests). Les éléments de moniteur $checksum et $previousChecksum sont destinés à l'enrichissement des alertes à l'aide du fichier de règles du moniteur.
`$command*(FtpCommand)`	Commande FTP émise par le moniteur.
`$connectionType*(FtpConnection)`	Type de connexion de données utilisé. Il peut s'agir de `ACTIVE` ou de `PASSIVE`.
`$connectTime*(ConnectTime)`	Temps mis pour se connecter au serveur FTP.
`$downloadTime`	Temps mis pour télécharger le fichier.

Tableau 51. Eléments du moniteur FTP (suite)	
Elément	**Description**
$localFile*(FtpLocalFile)	Nom de chemin complet du fichier stocké sur l'hôte local. Cet élément est tiré du fichier de configuration.
$lookupTime*(LookupTime)	Temps mis pour rechercher l'adresse IP du serveur FTP.
$previousChecksum	Généralement, l'élément PreviousChecksum ne fournit pas de valeurs significatives pour les classifications de niveau de service car les valeurs de total de contrôle sont inconnues au moment de la création de l'élément de profil (le moniteur calcule les valeurs de total de contrôle pendant l'exécution des tests). Les éléments de moniteur $previousChecksum et $checksum sont destinés à l'enrichissement des alertes à l'aide du fichier de règles du moniteur.
$regexp*n*	Expression régulière.
$regexpMatch*n*	Contenu de la ligne correspondant à l'expression régulière.
$regexpStatus*n*	Etat de la correspondance des expressions régulières : NONE - Aucune vérification d'expression régulière n'est configurée MATCHED - une correspondance a été trouvée pour l'expression régulière FAILED - aucune correspondance n'a été trouvée pour l'expression régulière
$remoteFile*(FtpRemoteFile)	Nom de chemin complet du fichier stocké sur l'hôte distant (serveur FTP). Cet élément est tiré du fichier de configuration.
$responseTime*(ResponseTime)	Délai entre l'établissement d'une connexion et la réception du premier octet du fichier cible.
$status	Code d'état renvoyé par le serveur FTP.
$transferTime*(TransferTime)	Définit la valeur sur $uploadTime ou $downloadTime.
$uploadTime	Temps mis pour charger le fichier.
$username	Nom d'utilisateur (nom de compte) utilisé par le moniteur pour la connexion à l'hôte cible. Cet élément est issu du fichier de configuration si $message contient OK.

Messages d'état

Le moniteur FTP fournit des messages d'état dans l'attribut ResultMessage lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Tableau 52. Messages d'état du moniteur FTP	
Message	**Description**
OK	Demande FTP effectuée.
Unable to open local file for reading/writing	Voir le fichier journal du moniteur FTP pour plus d'informations.
Unable to read from/write to local file	

Tableau 52. Messages d'état du moniteur FTP (suite)	
Message	**Description**
`Unable to read from data connection`	Une connexion de données au serveur FTP a été établie, mais un incident s'est produit.
`Unable to upload to ftp server`	
`Timed out waiting to read/write`	
`Connection closed by foreign host`	Connexion au serveur FTP rompue.
`Connection closed unexpectedly`	
`Connection failed`	Le moniteur n'a pas pu se connecter au serveur FTP. Voir le fichier journal du moniteur FTP pour plus d'informations.

Moniteur HTTP

Le moniteur HTTP vérifie la disponibilité et le temps de réponse des serveurs Web.

Il peut surveiller des pages Web individuelles, y compris celles utilisant l'interface CGI, qui nécessite normalement que l'utilisateur entre des données dans des zones. Il peut également surveiller le temps de téléchargement des éléments tels que les images sur une page Web.

Tableau 53. Récapitulatif des fichiers du moniteur HTTP	
Fichiers du moniteur	**Nom ou emplacement**
Exécutable du moniteur	`nco_m_http`
Fichier de propriétés	`$ISHOME/etc/props/http.props`
Fichier de règles	`$ISHOME/etc/rules/http.rules`
Fichier journal	`$ISHOME/log/http.log`

Consignes de configuration du moniteur HTTP

Les moniteurs HTTP et HTTPS vérifient la disponibilité et le temps de réponse des serveurs Web. Utilisez le moniteur HTTP dans les situations suivantes :

- Le site Web cible est statique.

  Pour les sites Web dynamiques, utilisez le moniteur TRANSX.
- Le site Web cible est pris en charge via le protocole HTTP.

  Pour les sites Web qui fournissent du contenu via le protocole HTTPS, sélectionnez le moniteur HTTPS.
- Pour effectuer la surveillance sur plusieurs plateformes.
- La vitesse est un facteur déterminant (le moniteur HTTP offre des performances élevées).

Types de requête HTTP

Le moniteur HTTP émule un navigateur Web qui prend en charge le protocole HTTP/1.0. Pour tester le serveur Web, le moniteur envoie une requête pour une page Web à l'aide des types de requête HTTP suivants :

- `HEAD`

  La commande `HEAD` tente d'accéder à une page Web et de renvoyer l'en-tête HTTP. L'émission de la commande `HEAD` permet de vérifier rapidement qu'une page Web est accessible.
- `GET`

La commande GET tente d'accéder à la page Web et de renvoyer l'ensemble de la page, notamment l'en-tête HTTP. Elle ne tente pas de renvoyer les fichiers associés à cette page, tels que les images.

- GETALL

  La commande GETALL tente d'accéder à la page Web et renvoie l'ensemble de la page, notamment l'en-tête HTTP, l'arrière-plan, les images, les applets, les cadres, les fichiers CSS et les scripts. Tout comme les commandes HEAD et GET, cette commande vérifie également qu'une page Web est accessible, mais étant donné que la commande GETALL renvoie l'ensemble de la page et tous ses fichiers associés, elle peut donner une indication plus réaliste de la durée nécessaire pour l'accès à la page. Le moniteur utilise également plusieurs unités d'exécution lors d'une commande GETALL pour une correspondance plus précise du comportement des navigateurs Web.

- POST

  La commande POST tente d'accéder à une page Web qui contient un formulaire HTTP et de compléter les zones de ce dernier. Ajoutez le corps de texte de la requête POST dans l'onglet **Corps** de la configuration d'Internet Service Monitoring agent ou utilisez le groupe @Body de la configuration d'Internet Service Monitoring agent ou ismbatch. Vous pouvez également utiliser les paramètres FORM. En revanche, vous ne pouvez pas utiliser les paramètres Corps de texte et FORM dans la demande POST.

Utilisation d'un serveur proxy

Vous pouvez tester la disponibilité des pages Web via un serveur proxy. Lorsque vous configurez le moniteur afin qu'il utilise un proxy, il envoie des demandes HTTP via le proxy. Si nécessaire, vous pouvez ignorer le cache de proxy. Vous pouvez configurer les paramètres pour le serveur proxy dans l'onglet **Détails du proxy**. Le moniteur HTTP prend en charge l'accès authentifié aux serveurs proxy. Cette authentification est indépendante de toute authentification requise pour la page Web cible.

Eléments du serveur proxy

Dans les versions antérieures, lorsque vous configuriez un élément de profil de sorte qu'il utilise un serveur proxy, le moniteur HTTP insérait par défaut le nom et le port du serveur proxy dans les éléments `$server` et `$port`, au lieu du nom et du port du serveur de destination prévu. Pour conserver la valeur du nom et du port du serveur de destination prévu dans les versions antérieures, définissez la propriété `generateProxyTokens` sur 1 ou démarrez le moniteur avec le paramètre de ligne de commande `-generateproxytokens`.

En plus de conserver les valeurs des éléments `$server` et `$port` lorsque cette propriété ou ce paramètre de ligne de commande est défini, le moniteur génère les éléments `$proxyServer`, `$proxyPort`, `$proxyAuthType`, `$proxyUsername` et `$proxyCache`.

Authentification

Si la page Web que vous souhaitez surveiller ou le serveur proxy que vous souhaitez tester nécessite une authentification, entrez les données d'identification permettant d'accéder à la page dans les zones de paramètre `authenticationtype`, `username` et `password` sur l'onglet Avancé ou Détails du proxy.

Pour désactiver l'authentification, attribuez la valeur `NONE` à `authenticationtype`.

Pour sélectionner l'authentification de base, procédez comme suit :

1. Attribuez la valeur `BASIC` à `authenticationtype`.
2. Attribuez la valeur `username` et `password` aux éléments requis par la page web ou le serveur proxy.

Pour sélectionner NTLM, procédez comme suit :

1. Attribuez la valeur `NTLMv1` ou `NTLMv2` à `authenticationtype`.
2. Attribuez la valeur `username` et `password` aux éléments requis par la page web ou le serveur proxy.

Remarque :

Le moniteur limite la longueur des requêtes HTTP à 4096 caractères. Si la longueur des données de formulaire supplémentaires est à l'origine d'une longueur de demande qui dépasse cette limite, le moniteur n'inclut pas les données de formulaire supplémentaires dans la demande.

Configuration du test de service du moniteur HTTP

Les paramètres de configuration du moniteur HTTP permettent de définir les tests de service HTTP.

Tableau 54. Configuration du moniteur HTTP

Zone	Description
server	Nom d'hôte du serveur à surveiller. Par exemple, `www.mycompany.com`
page	URL de la page à surveiller. Par exemple, `index.html`
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément. Par exemple, `surveillance via un serveur proxy`
port	Port du serveur HTTP à utiliser. Valeur par défaut : `80`
localip	Indique l'adresse IP de l'interface réseau utilisée par le moniteur pour le test. Si cette zone est vide, le moniteur utilise l'interface spécifiée par la propriété `IpAddress`.
version	Version de protocole HTTP à utiliser : • `1.0` • `1.1` Valeur par défaut : `1.0`
command	Type de requête HTTP : • `HEAD` • `GET` • `GETALL` • `POST` Valeur par défaut : `GET`
formname	Lorsqu'il est utilisé dans une transaction, le moniteur HTTP recherche dans le formulaire spécifié les valeurs par défaut. Toute valeur trouvée est automatiquement insérée dans l'étape HTTP suivante de la transaction.
authenticationtype	Spécifie le mécanisme d'authentification par stimulation/réponse des utilisateurs réseau : • `NONE` - Aucune authentification • `BASIC` • `NTLMv1` - Authentification par demande/réponse Windows NTLM version 1 • `NTLMv2` - Windows NTLM version 2 Valeur par défaut : `NONE`
username	Nom d'utilisateur (nom de compte) du moniteur à utiliser pour se connecter au serveur.
password	Mot de passe correspondant au nom d'utilisateur du moniteur à utiliser pour la connexion au serveur.

Tableau 54. Configuration du moniteur HTTP (suite)

Zone	Description
timeout	Délai d'attente, en secondes, avant une réponse du serveur. Valeur par défaut : `30`
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300` .
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`
verifycertificate	Désactivé par défaut.
Caractéristiques du proxy	
server	Nom d'hôte du serveur proxy.
port	Port du serveur proxy à utiliser. Valeur par défaut : `8080`
authenticationtype	Type d'authentification pour le serveur proxy. Pour plus d'informations, voir `authenticationtype`. Valeur par défaut : `NONE`
username	Elément utilisé par le moniteur avec le mot de passe pour établir la connexion au serveur proxy.
password	Elément utilisé par le moniteur avec le nom d'utilisateur pour établir la connexion au serveur proxy et dont le libellé est mot de passe.
useproxy	Configure le moniteur pour exécuter la demande en utilisant un serveur proxy. • `proxy` (utilisez `true` dans ismbatch) • `noproxy` (utilisez `false` dans ismbatch) Valeur par défaut : `noproxy`

Tableau 54. Configuration du moniteur HTTP (suite)	
Zone	**Description**
hostnamelookuppreference	Détermine la version IP (IPv6 ou IPv4) qui est appliquée au nom d'hôte fourni. Les options sont les suivantes : • `default` définit le moniteur pour utiliser les paramètres des propriétés du moniteur. Il s'agit de la valeur par défaut. • 4Then6 sélectionne IPv4, puis IPv6. Utilise les adresses IPv4 si elles sont disponibles. Si aucune adresse IPv4 n'est trouvée, les adresses IPv6 sont utilisées. • 6Then4 sélectionne IPv6, puis IPv4. Utilise les adresses IPv6 si elles sont disponibles. Si aucune adresse IPv6 n'est trouvée, les adresses IPv4 sont utilisées. • `4Only` sélectionne IPv4 uniquement. Utilise les adresses IPv4 uniquement. S'il n'existe aucune adresse IPv4, l'interrogation renvoie une erreur. • `6Only` sélectionne IPv6 uniquement. Utilise les adresses IPv6 uniquement. S'il n'existe aucune adresse IPv6, l'interrogation renvoie une erreur. • `6or4` sélectionne IPv4 ou IPv6. Utilise la première adresse renvoyée à partir du nom d'hôte.
nocache	Défini par défaut sur cache.

Expression régulière

Vous pouvez effectuer une recherche d'expression régulière sur les informations téléchargées en entrant jusqu'à 50 expressions régulières différentes. Le moniteur HTTP tente de faire correspondre le contenu extrait à chaque expression régulière. Si une correspondance à une expression régulière indiquée est trouvée, les lignes correspondantes (ou le nombre maximal de lignes correspondantes pouvant être stockées dans la mémoire tampon interne du moniteur) sont renvoyées dans l'élément `$regexpMatchn` correspondant. Si l'expression régulière a plusieurs correspondances dans les informations téléchargées, seule la première correspondance est renvoyée. L'état de chaque test d'expression régulière est indiqué par les éléments `$regexpStatusn`. Vous pouvez utiliser les correspondances d'expression régulière et les informations d'état en tant que critères pour les classifications de niveau de service. Pour plus d'informations sur la syntaxe des expressions régulières, voir Tableau 50, à la page 335.

Paramètre d'en-tête et de formulaire

Le moniteur HTTP peut envoyer des données supplémentaires dans les zones d'en-tête et dans le corps de message des requêtes HTTP.

Vous pouvez configurer les paramètres de ces données supplémentaires sur l'onglet Paramètres. Les paramètres sont Nom, Valeur et Type, et fonctionnent de la manière suivante :

- Les paires Nom/Valeur de type HEAD spécifient des zones d'en-tête supplémentaires, telles que `User-Agent` et `Referer`, incluses dans toutes les demandes HTTP envoyées par le moniteur. Les zones d'en-tête peuvent être définies pour tout type de méthode HTTP (`GET`, `GETALL`, `HEAD` ou `POST`).

  Pour ITCAM for Transactions version 7.4.0.1 et versions ultérieures, le paramètre HEAD de l'agent utilisateur par défaut `Mozilla/5.0 (ISM-MONITOR)` est ajouté à chaque nouvel élément HTTP ou HTTPS. L'en-tête de l'agent utilisateur par défaut est ajouté de sorte que les moniteurs HTTP et HTTPS puissent être utilisés avec les sites Web pour lesquels le contenu est fonction du client de navigation.
- Les paires Nom/Valeur de type FORM indiquent des informations supplémentaires contenues dans le corps du message des requêtes `POST` HTTP envoyées par le moniteur. Si la page cible contient un formulaire correspondant au nom spécifié dans la zone formname, le moniteur traite toute paire nom/valeur dans le formulaire comme si elle était configurée dans l'élément de profil.

Remarque :

Le moniteur limite la longueur des requêtes HTTP à 4096 caractères. Si la longueur des données de formulaire supplémentaires est à l'origine d'une longueur de demande qui dépasse cette limite, le moniteur n'inclut pas les données de formulaire supplémentaires dans la demande.

Eléments du moniteur

Outre les résultats de test communs à tous les éléments, le moniteur HTTP génère un ensemble de résultats de test contenant les données propres aux tests de service HTTP. Les éléments indiqués par un astérisque (*) sont disponibles en tant qu'attributs. Le nom des attributs est affiché entre parenthèses. L'absence d'astérisque indique qu'il n'existe aucun attribut équivalent. Les attributs entre parenthèses mais sans élément sont disponibles uniquement en tant qu'attributs, il n'existe aucun élément équivalent.

Tableau 55. Eléments du moniteur HTTP

Elément	Description
$bytesPerSec*(BytesPerSec)	Nombre moyen d'octets transférés par seconde.
$bytesTransfered*(BytesTransferred)	Nombre d'octets transférés ou téléchargés.
$checksum	Généralement, l'élément Checksum ne fournit pas de valeurs significatives pour les classifications de niveau de service car les valeurs de total de contrôle ne sont pas connues lorsque l'élément de profil est créé (le moniteur calcule les valeurs de total de contrôle lorsque les tests sont en cours). Les éléments de moniteur $checksum et $previousChecksum sont destinés à l'enrichissement des alertes à l'aide du fichier de règles du moniteur.
$command	Commande HTTP émise par le moniteur. Par exemple, HEAD, GET, GETALL ou POST.
$connectTime*(ConnectTime)	Temps mis pour se connecter au serveur.
$downloadTime*(DownloadTime)	Temps mis pour télécharger le fichier.
(Elements)	Nombre d'éléments de page reçus.
$formname	Nom du formulaire utilisé dans une action POST.
$lastStatus*(PageStatus)	Si un élément de profil extrait plusieurs pages, cet élément contient la chaîne de résultats de la dernière page extraite. Cette valeur est identique à celle de $urlResult*n* ,où *n* est égal à la valeur de $pageCount.
$lastModified	Valeur de la zone d'en-tête HTTP Last-Modified de la première page extraite.
$page*(Page)	Page accédée sur le serveur HTTP.

Tableau 55. Eléments du moniteur HTTP (suite)

Elément	Description
$pageCount	Nombre total de ressources téléchargées pendant un test GETALL, à l'exclusion de la page de test elle-même. Si la page testée ne se rapporte à aucune autre ressource, cet élément n'est pas généré.
$port*(Port)	Port utilisé pour l'accès au serveur HTTP. Si un serveur proxy a été utilisé pour le test, il s'agit de la valeur de port du serveur proxy auquel la demande a été envoyée. Pour préserver le port du serveur de destination prévu, définissez la propriété generateProxyTokens sur 1 ou démarrez le moniteur avec le paramètre de lancement -generateproxytokens.
$previousChecksum	Généralement, l'élément PreviousChecksum ne fournit pas de valeurs significatives pour les classifications de niveau de service car les valeurs de total de contrôle ne sont pas connues quand l'élément de profil est créé (le moniteur calcule les valeurs de total de contrôle lorsque les tests sont en cours). Les éléments de moniteur $previousChecksum et $checksum sont destinés à l'enrichissement des alertes à l'aide du fichier de règles du moniteur.
$proxyAuthType	Type d'authentification pour le serveur proxy.
$proxyCache	La valeur true indique que le serveur proxy a extrait la page Web du serveur, plutôt que de son propre cache.
$proxyPort	Numéro de port du serveur proxy auquel la demande a été envoyée.
$proxyServer	Nom d'hôte du serveur proxy.
$proxyUsername	Elément utilisé par le moniteur avec le mot de passe pour établir la connexion au serveur proxy.
$regexpMatch*n*	Contenu de la ligne correspondant à l'expression régulière.
$regexp*n*	Expression régulière.
$regexpMatch*n*	Contenu de la ligne correspondant à l'expression régulière.
$regexpStatus*n*	Etat de la correspondance des expressions régulières : NONE - Aucune vérification d'expression régulière n'est configurée MATCHED - une correspondance a été trouvée pour l'expression régulière FAILED - aucune correspondance n'a été trouvée pour l'expression régulière
$responsetime* (ResponseTime)	Durée entre la création d'une connexion et la réception du premier octet de la page.
$timeSinceModification	Durée écoulée depuis la dernière modification de la page. Il s'agit de la différence entre le moment du test et la valeur de la zone d'en-tête HTTP Last modified de la première page extraite.

Tableau 55. Eléments du moniteur HTTP (suite)	
Elément	**Description**
$urlDownloadTimes*n** (UrlDownloadTime)	Durée de téléchargement d'URL de chaque élément dans une demande GETALL. Chaque élément est numéroté, à partir de 000 ($urlDownloadTime000, $urlDownloadTime001, $urlDownloadTime002, etc.).
$url*n**(Url)	URL de chaque page d'un test GETALL. Chaque page est numérotée, à partir de 000 ($url000, $url001, $url002, etc.).
$urlResult*n** (UrlResultString)	Chaîne de résultat pour chaque page téléchargée dans une demande GETALL. Chaque est numéroté, à partir de 000 ($urlResult000, $urlResult001, $urlResult002, etc.).
$username	Nom utilisé pour accéder aux pages nécessitant une authentification de l'utilisateur.

Message d'état

Le moniteur HTTP fournit des messages d'état dans l'attribut ResultMessage lorsqu'IBM Application Performance Management est utilisé. Ces messages indiquent le résultat du test.

Tableau 56. Tableau 3. Messages d'état du moniteur HTTP	
Message	**Description**
OK	La demande émanant du moniteur a abouti.
Form not found	La page demandée est introuvable.
Initialise Fetch Page Failed	Mémoire insuffisante pour allouer de l'espace au mécanisme d'extraction de la page HTTP. Le message de la ligne précédente doit contenir plus d'informations.
Connection Failed	La connexion du moniteur a échoué pour d'autres raisons que la rupture du lien, la réinitialisation de la connexion, l'inaccessibilité du lien, le dépassement du délai de connexion, la fermeture de la connexion ou l'arrêt de l'hôte. Voir le fichier journal du moniteur HTTP pour plus d'informations.

Correspondance des expressions régulières et des paramètres de formulaire

Surveillez le fonctionnement du formulaire http://support.mycompany.com/cgi-bin/search.cgi en envoyant des demandes HTTP POST avec le paramètre de formulaire search=ism, et utilisez une expression régulière pour faire correspondre la chaîne Your search was successful dans la réponse. Si cette chaîne est renvoyée dans la réponse, attribuez le niveau de service Good et Failed dans les autres cas de figure.

Créez un élément de profil HTTP et définissez les zones comme indiqué dans le tableau ci-dessous.

Tableau 57. Exemple d'élément de profil de formulaire HTTP	
Zone de configuration d'élément de profil	**Valeur**
server	support.mycompany.com
page	/cgi-bin/search.cgi
description	Exemple - Expressions régulières et paramètres de formulaire

Tableau 57. Exemple d'élément de profil de formulaire HTTP (suite)	
Zone de configuration d'élément de profil	**Valeur**
Détails sur l'expression régulière	
match 1	`Votre recherche a abouti`
Détails sur la classification de niveau de service	
instruction	`Statut Regexp 1 = CORRESPONDANCE alors statut CORRECT`
Détails sur l'en-tête et le formulaire	
nom	`search`
valeur	`ism`
type	`FORM`

Propriétés

Les propriétés et les options de ligne de commande spécifiques au moniteur HTTP sont décrites dans le tableau suivant.

Tableau 58. Propriétés du moniteur HTTP		
Nom de la propriété	**Paramètre de la propriété**	**Description**
`AllowDuplicateDownload`	`0`|`1`	Déclenche le téléchargement des pages chaque fois qu'elles sont détectées. `0` - désactivé (un seul téléchargement) `1` - activé
`ForceHTMLParse`	`0`|`1`	Déclenche l'analyse HTML des pages dont le type de contenu n'est pas `text/html`. `0` - désactivé `1` - activé
`GenerateProxyTokens`	`0`|`1`	Indique si le moniteur génère des éléments supplémentaires contenant des informations sur le serveur proxy si un serveur proxy est utilisé dans un test. `0` - désactivé `1` - activé (les éléments supplémentaires `$server` et `$port` contiennent les valeurs du serveur proxy)
`GETALLThreadNum`	`1`|`2`|`3`|`4`|`5`	Spécifie le nombre d'unités d'exécution distinctes à utiliser lors d'une requête `GETALL`.

Tableau 58. Propriétés du moniteur HTTP (suite)

Nom de la propriété	Paramètre de la propriété	Description
GetLinkTags	0|1	Active le téléchargement de feuilles de style liées pour les requêtes GETALL : 0 - désactivé 1 - activé (si la page cible contient une balise link avec la valeur d'attribut rel=stylesheet, le moniteur tente de télécharger la ressource désignée par l'attribut href de la balise link)
HostnameLookupPreference	chaîne	Détermine la version IP (IPv6 ou IPv4) qui est appliquée au nom d'hôte fourni. Les valeurs admises sont : • 4Then6 sélectionne IPv4, puis IPv6. Utilise les adresses IPv4 si elles sont disponibles. Si aucune adresse IPv4 n'est trouvée, les adresses IPv6 sont utilisées. • 6Then4 sélectionne IPv6, puis IPv4. Utilise les adresses IPv6 si elles sont disponibles. Si aucune adresse IPv6 n'est trouvée, les adresses IPv4 sont utilisées. • 4Only sélectionne IPv4 uniquement. Utilise les adresses IPv4 uniquement. S'il n'existe aucune adresse IPv4, l'interrogation renvoie une erreur. • 6Only sélectionne IPv6 uniquement. Utilise les adresses IPv6 uniquement. S'il n'existe aucune adresse IPv6, l'interrogation renvoie une erreur. • 6Or4 sélectionne IPv4 ou IPv6. Utilise la première adresse renvoyée à partir du nom d'hôte. Par défaut : 4Then6
Ipv6Address	entier	Adresse locale à lier comme origine pour les requêtes HTTP lors de l'utilisation de HTTP IPv6. Par défaut : aucune adresse
NoParseExtensions	chaîne	Liste d'extensions de fichier séparées à l'aide de virgules indiquant les types de fichier non analysés, mais téléchargés, par le moniteur.
OutputDirectory	chaîne	Indique le répertoire de sortie à utiliser si OutputResult a la valeur true (défini sur 1). Par défaut : $ISHOME/var
OutputResult	0|1	Indique si le moniteur sauvegarde les données qu'il reçoit du service. 0 - désactivé 1 - activé

Tableau 58. Propriétés du moniteur HTTP (suite)		
Nom de la propriété	**Paramètre de la propriété**	**Description**
RelativeRedirects	0|1	Permet aux zones Emplacement des codes d'état HTTP 301/302 de contenir des URL relatives plutôt que des URL absolues. 0 - URL absolues 1 - URL relatives
RFCPOST	0|1	Indique que le moniteur doit suivre les RFC1945 et RFC2616, puis envoyer un deuxième POST après la redirection. De nombreux serveurs Web n'attendent pas un POST après une redirection et la plupart des navigateurs ne suivent pas les RFC. 0 - désactivé 1 - activé

Moniteur HTTPS

Le moniteur HTTPS vérifie la disponibilité et le temps de réponse des serveurs Web. Il peut surveiller des pages Web individuelles, y compris celles utilisant des formulaires HTML, qui nécessitent normalement que l'utilisateur entre des données dans des zones.

Remarque : Le moniteur HTTPS fonctionne de la même manière que le moniteur HTTP, mais il communique avec le serveur HTTP à l'aide de la version 2 ou 3 du protocole SSL (Secure Sockets Layer), qui chiffre toutes les communications entre le serveur et le moniteur.

Tableau 59. Récapitulatif du fichier de moniteur HTTPS	
Fichiers du moniteur	**Nom ou emplacement**
Exécutable du moniteur	nco_m_https
Fichier de propriétés	$ISHOME/etc/props/https.props
Fichier de règles	$ISHOME/etc/rules/https.rules
Fichier journal	$ISHOME/log/https.log

Consignes de configuration du moniteur HTTPS

Le moniteur HTTPS vérifie la disponibilité et le temps de réponse des serveurs Web. Utilisez le moniteur HTTPS dans les situations suivantes :

- Le site Web cible est statique.

  Pour les sites Web dynamiques, utilisez le moniteur TRANSX.
- Le site Web cible est pris en charge via le protocole HTTPS.

  Pour les sites Web qui fournissent du contenu via le protocole HTTP, sélectionnez le moniteur HTTP.
- Pour effectuer la surveillance sur plusieurs plateformes.
- La vitesse est un facteur déterminant (le moniteur HTTPS offre des performances élevées).

Certificat côté client

Le moniteur permet de surveiller les serveurs qui requièrent des certificats côté client pour une authentification mutuelle.

Spécifiez le fichier de certificats SSL, le fichier de clés et le mot de passe de clé lors de la création d'un élément de profil.

Les certificats doivent être au format PEM (Privacy Enhanced Mail). Si ce n'est pas le cas, vous devez convertir votre certificat au format PEM. Il est possible de convertir les certificats à l'aide d'un logiciel comme openSSL, lequel est disponible sur la page Web http://www.openssl.org.

Remarque : Si vous utilisez toujours les mêmes certificat, clé et mot de passe dans tous les éléments de profil, spécifiez-les en utilisant des propriétés de moniteur au lieu de les définir dans chaque élément de profil que vous créez.

Configuration des tests de service du moniteur HTTPS

Utilisez les paramètres de configuration du moniteur HTTPS pour définir les tests de service HTTPS.

Tableau 60. Configuration du moniteur HTTPS

Zone	Description
serveur	Nom d'hôte du serveur à surveiller. Par exemple : `www.myconpany.com`
page	URL de la page à surveiller. Exemple : `/secure/`
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément.
port	Port du serveur à utiliser. Port par défaut : 443
localip	Indique l'adresse IP de l'interface réseau utilisée par le moniteur pour le test. Si cette zone est vide, le moniteur utilise l'interface spécifiée par la propriété `IpAddress`.
version	Version du protocole HTTPS à utiliser : • `1.0` • `1.1` Valeur par défaut : `1.0`
command	Type de requête : • `HEAD` • `GET` • `GETALL` • `POST` Valeur par défaut : `GET`
formname	Lorsqu'il est utilisé dans une transaction, le moniteur HTTPS recherche les valeurs par défaut dans le formulaire spécifié. Toute valeur trouvée est automatiquement insérée dans l'étape HTTPS suivante de la transaction.
authenticationtype	Spécifie le mécanisme d'authentification par stimulation/réponse des utilisateurs réseau : • `NONE` - Aucune authentification. • `BASIC` • `NTLMv1` - Authentification par stimulation/réponse Windows NTLM version 1. • `NTLMv2` - Windows NTLM version 2. Valeur par défaut : `NONE`

Tableau 60. Configuration du moniteur HTTPS (suite)	
Zone	**Description**
username	Nom d'utilisateur (nom de compte) du moniteur à utiliser pour se connecter au serveur HTTPS.
password	Mot de passe correspondant au nom d'utilisateur du moniteur à utiliser pour se connecter au serveur HTTPS.
sslcertificatefile	Chemin d'accès et nom du fichier de certificat numérique qui est utilisé dans l'élément du moniteur. Si le chemin d'accès n'est pas absolu, il est interprété par le moniteur comme étant relatif par rapport au répertoire de travail (`$ISMHOME/platform/arch/bin`). Si vous ne spécifiez pas un fichier de certificat, le moniteur utilise le certificat indiqué par la propriété de moniteur `SSLCertificateFile`.
sslkeyfile	Chemin et nom du fichier contenant la clé privée SSL qui est utilisée pour identifier le serveur et signer les messages SSL.
sslkeypassword	Mot de passe utilisé pour chiffrer la clé privée SSL.
timeout	Délai d'attente, en secondes, d'une réponse du serveur. Valeur par défaut : `30`
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`
Détails du proxy	
serveur	Nom d'hôte du serveur proxy.
port	Port du serveur proxy à utiliser.
authenticationtype	Type d'authentification pour le serveur proxy HTTPS. Pour plus d'informations, voir authenticationtype.
username	Nom d'utilisateur du moniteur à utiliser pour se connecter au serveur proxy HTTPS.
password	Mot de passe du moniteur à utiliser pour se connecter au serveur proxy HTTPS.
useproxy	Configure le moniteur pour exécuter la demande en utilisant un serveur proxy. • `proxy` (utilisez `true` dans ismbatch) • `noproxy` (utilisez `false` dans ismbatch) Valeur par défaut : `noproxy`

Tableau 60. Configuration du moniteur HTTPS (suite)	
Zone	**Description**
hostnamelookuppreference	Détermine la version IP (IPv6 ou IPv4) qui est appliquée au nom d'hôte fourni. Les options sont les suivantes : • `default` définit le moniteur pour utiliser les paramètres des propriétés du moniteur. Il s'agit de la valeur par défaut. • 4Then6 sélectionne IPv4, puis IPv6. Utilise les adresses IPv4 si elles sont disponibles. Si aucune adresse IPv4 n'est trouvée, les adresses IPv6 sont utilisées. • 6Then4 sélectionne IPv6, puis IPv4. Utilise les adresses IPv6 si elles sont disponibles. Si aucune adresse IPv6 n'est trouvée, les adresses IPv4 sont utilisées. • `4Only` sélectionne IPv4 uniquement. Utilise les adresses IPv4 uniquement. S'il n'existe aucune adresse IPv4, l'interrogation renvoie une erreur. • `6Only` sélectionne IPv6 uniquement. Utilise les adresses IPv6 uniquement. S'il n'existe aucune adresse IPv6, l'interrogation renvoie une erreur. • `6or4` sélectionne IPv4 ou IPv6. Utilise la première adresse renvoyée à partir du nom d'hôte.

Correspondance d'expressions régulières

Vous pouvez effectuer une recherche d'expression régulière sur les informations téléchargées en entrant jusqu'à 50 expressions régulières différentes. Le moniteur HTTPS tente de faire correspondre le contenu extrait à chaque expression régulière.

Si une correspondance d'une expression régulière indiquée est trouvée, les lignes correspondantes (ou le nombre maximal de lignes correspondantes pouvant être stockées dans la mémoire tampon interne du moniteur) sont renvoyées dans l'élément `$regexpMatchn` correspondant. Si l'expression régulière a plusieurs correspondances dans les informations téléchargées, seule la première correspondance est renvoyée. L'état de chaque test d'expression régulière est indiqué par les éléments `$regexpStatusn`. Vous pouvez utiliser les correspondances d'expression régulière et les informations d'état en tant que critères pour les classifications de niveau de service.

Pour plus d'informations, voir Tableau 50, à la page 335.

Paramètre d'en-tête et de formulaire

Comme le moniteur HTTP, le moniteur HTTPS peut envoyer des données supplémentaires dans les zones d'en-tête et le corps du message de requêtes HTTP.

Pour des détails sur les paramètres d'en-être et de formulaire, voir Paramètre d'en-tête et de formulaire HTTP.

Eléments de moniteur

Tableau 61. Eléments du moniteur SSL HTTPS SSL	
Elément	**Description**
$SSLcertificateSerialNumber	Numéro de série du certificat X509 présenté par le serveur.
$SSLcipherSuiteCount	Nombre d'algorithmes de cryptographie disponibles sur la connexion.
$SSLcipherSuiteList	Liste des algorithmes de cryptographie disponibles sur la connexion.

Tableau 61. Eléments du moniteur SSL HTTPS SSL (suite)	
Elément	**Description**
$SSLcipherSuiteName	Suite de chiffrement sélectionné pour la connexion.
$SSLeffectiveSessionKeyBits	Nombre d'octets dans la clé de session. Il s'agit généralement de 128, 168, ou 40 pour les versions d'exportations.
$SSLHandshakeTime* (SslHandshakeTime)	Temps mis pour établir la connexion SSL.
$SSLissuerName	Nom d'émetteur pour la certification de format X509 du serveur.
$SSLprotocolVersion	Version de SSL utilisée, v2 ou v3.
$SSLpublicKeyLengthBits	Taille de la clé publique du serveur. Elle est généralement de 1024 octets, sauf lorsqu'un algorithme de cryptographie de spécification d'exportation est utilisé.
$SSLserverCertificateValidFrom	Date de début de validité du certificat du serveur.
$SSLserverCertificateValidTo	Date de fin de validité du certificat du serveur.
$SSLserverName	Nom du serveur SSL.
$SSLsubjectName	Nom de sujet de la certification de format X509. Il s'agit généralement du nom de l'organisation qui contrôle le serveur.

Les éléments indiqués par un astérisque (*) sont disponibles en tant qu'attributs. Le nom des attributs est affiché entre parenthèses. L'absence d'astérisque indique qu'il n'existe aucun attribut équivalent. Les attributs entre parenthèses mais sans élément sont disponibles uniquement en tant qu'attributs ; il n'existe aucun élément équivalent.

Le moniteur HTTPS produit les mêmes éléments supplémentaires que le moniteur HTTP, comme indiqué dans le Tableau 55, à la page 343. En outre, il produit les éléments liés à SSL si un certificat côté client est utilisé dans le test, comme décrit dans le Tableau 61, à la page 351.

En plus des résultats de test communs à tous les éléments, le moniteur HTTPS génère un ensemble de résultats de test contenant des données spécifiques aux tests de service HTTPS.

Message d'état

Le moniteur HTTPS fournit des messages d'état dans l'attribut `ResultMessage` lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

En plus des messages d'état HTTP, le moniteur HTTPS génère également les messages répertoriés dans le Tableau 62, à la page 352.

Tableau 62. Messages d'état du moniteur HTTPS	
Message	**Description**
OK	La connexion du moniteur au serveur a abouti.
`SSL handshake failed`	Le moniteur n'a pas réussi à initialiser la connectivité SSL, une fois la connexion au serveur établie.

Tableau 62. Messages d'état du moniteur HTTPS (suite)	
Message	**Description**
`Connection failed`	La connexion du moniteur a échoué pour d'autres raisons que la rupture du lien, la réinitialisation de la connexion, l'inaccessibilité du lien, le dépassement du délai de connexion, la fermeture de la connexion ou l'arrêt de l'hôte. Voir le fichier journal du moniteur HTTP pour plus d'informations.

Propriétés

Le moniteur HTTPS possède les mêmes propriétés que le moniteur HTTP.

Pour plus de détails sur les options de propriétés qui sont identiques à celles du moniteur HTTP, voir Tableau 58, à la page 346. Le tableau 5 répertorie les propriétés spécifiques de HTTPS.

Tableau 63. Propriétés spécifiques du moniteur HTTPS		
Nom de la propriété	**Paramètre de la propriété**	**Description**
SSLCertificate File	chaîne	Chemin et nom du fichier de certificats numériques utilisé si aucun certificat n'est explicitement spécifié pour un élément HTTPS lors de sa création. Si le chemin n'est pas absolu, il est interprété par le moniteur comme étant relatif au répertoire de travail (`$ISHOME/platform/arch/bin`).
SSLCipherSuite	chaîne	Suite de chiffrement à utiliser pour les opérations SSL. Valeur par défaut : `RC4:3DES:DES:+EXP`
SSLDisableTLS	entier	Désactive TLSv1 pour la prise en charge des éléments existants. Valeur par défaut : `0` - TLSv1 est activé. `1` - TLSv1 est désactivé.
SSLKeyFile	chaîne	Fichier contenant la clé privée SSL.
SSLKeyPassword	chaîne	Mot de passe utilisé pour chiffrer la clé privée SSL.

Algorithmes de chiffrement

La propriété `SSLCipherSuite` spécifie l'algorithme de cryptographie utilisé par le moniteur HTTPS. Pour plus d'informations sur les paramètres SSL, voir «Paramètre SSL dans Internet Service Monitoring», à la page 447.

Moniteur ICMP

Le moniteur ICMP teste les performances du service ICMP exécuté sur un réseau. Pour ce faire, le moniteur utilise la commande écho ICMP.

Le tableau ci-dessous répertorie les fichiers du moniteur ICMP.

Tableau 64. Fichiers du moniteur ICMP	
Fichiers du moniteur	**Nom ou emplacement**
Exécutable du moniteur	`nco_m_icmp`
Fichier de propriétés	`$ISHOME/etc/props/icmp.props`

Tableau 64. Fichiers du moniteur ICMP (suite)	
Fichiers du moniteur	**Nom ou emplacement**
Fichier de règles	`$ISHOME/etc/rules/icmp.rules`
Fichier journal	`$ISHOME/log/icmp.log`

Instructions de configuration du moniteur ICMP

Le moniteur ICMP envoie des demandes d'écho ICMP (généralement appelées `pings`) aux hôtes cible et attend des réponses d'écho. Il enregistre les temps de réponse, les durées de boucle et les mesures de taux de réussite qui fournissent une indication du fonctionnement du réseau. Lorsque le moniteur émet une demande d'écho, la demande peut passer par un ou plusieurs routeurs avant d'atteindre l'hôte cible. Ces routeurs peuvent répondre au moniteur avant que l'hôte cible ait reçu la demande d'écho. Si une demande d'écho émise par le moniteur passe par un routeur, ce routeur peut émettre une réponse destinée au moniteur. Cette réponse peut indiquer que le routeur n'a pas pu définir l'emplacement de l'hôte cible ou que le routeur est trop occupé pour traiter la demande. Il est possible que le moniteur reçoive des réponses de plusieurs routeurs avant qu'il ne reçoive une réponse d'écho de l'hôte cible. Si le moniteur reçoit une réponse d'écho de l'hôte cible, il enregistre la durée. S'il ne reçoit pas de réponse du serveur cible pendant la période définie, la demande est enregistrée comme un échec. Vous pouvez configurer le moniteur afin qu'il envoie plusieurs demandes d'écho ICMP vers la même cible dans chaque test. Le moniteur enregistre les statistiques de chaque demande envoyée.

Remarque : Le moniteur ICMP doit être exécuté en tant que superutilisateur `root` car il ouvre un socket brut pour envoyer des paquets ICMP.

Configuration des tests d'un service du moniteur ICMP

Utilisez les paramètres de configuration du moniteur ICMP pour définir les tests d'un service. Lorsque vous configurez le moniteur, des valeurs par défaut sont affichées pour les paramètres de délai et d'intervalle d'interrogation. Il s'agit respectivement des valeurs 30 et 300 secondes. D'autres valeurs par défaut répertoriées dans le tableau ne sont pas affichées pendant la configuration mais appliquées au moment de la sauvegarde des détails de la configuration si aucune valeur n'a été indiquée.

Le tableau suivant répertorie les configurations du moniteur ICMP.

Tableau 65. Configuration du moniteur ICMP	
Zone	**Description**
serveur	Nom d'hôte ou adresse IP du serveur auquel les demandes d'écho sont envoyées. Par exemple, `test.myconpany.com`
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément.
timeout	Délai d'attente, en secondes, d'une réponse du serveur à chaque demande d'écho. Valeur par défaut : `10`
numberofpings	Nombre de demandes d'écho à envoyer. Valeur par défaut : 5
packetinterval	Délai d'attente, en secondes, entre l'envoi de demandes d'écho. Valeur par défaut : `1`

Tableau 65. Configuration du moniteur ICMP (suite)	
Zone	**Description**
packetsize	Taille, en octets, de chaque demande d'écho envoyée. Valeur par défaut : 64
typeofservice	Définit la zone Type of Service dans la couche IP. Les valeurs des zones TOS (Type of Service) IPv4 et DSCP Differentiated Service doivent être entrées. Les valeurs admises sont comprises entre 0 et 255.
retries	Nombre de nouvelles tentatives du moniteur pour effectuer des demandes d'écho avant d'abandonner la procédure. Valeur par défaut : 0
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : 300
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : 0
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : 10
hostnamelookuppreference	Détermine la version IP (IPv6 ou IPv4) qui est appliquée au nom d'hôte fourni. Les options sont les suivantes : • default définit le moniteur pour utiliser les paramètres des propriétés du moniteur. Il s'agit de la valeur par défaut. • 4Then6 sélectionne IPv4, puis IPv6. Utilise les adresses IPv4 si elles sont disponibles. Si aucune adresse IPv4 n'est trouvée, les adresses IPv6 sont utilisées. • 6Then4 sélectionne IPv6, puis IPv4. Utilise les adresses IPv6 si elles sont disponibles. Si aucune adresse IPv6 n'est trouvée, les adresses IPv4 sont utilisées. • 4Only sélectionne IPv4 uniquement. Utilise les adresses IPv4 uniquement. S'il n'existe aucune adresse IPv4, l'interrogation renvoie une erreur. • 6Only sélectionne IPv6 uniquement. Utilise les adresses IPv6 uniquement. S'il n'existe aucune adresse IPv6, l'interrogation renvoie une erreur. • 6or4 sélectionne IPv4 ou IPv6. Utilise la première adresse renvoyée à partir du nom d'hôte.

Remarque : Surveillez la disponibilité de l'hôte `test.mycompany.com` en vérifiant les temps de réponse toutes les dix minutes. Tentez d'établir une connexion au serveur dans un intervalle de 30 secondes et si le délai est dépassé, faites deux nouvelles tentatives. Si ces tentatives n'aboutissent pas, répétez le test trois fois avec cinq secondes entre chaque tentative.

Eléments du moniteur

En plus des résultats de test communs à tous les éléments, le moniteur ICMP génère un ensemble de résultats de test contenant des données propres aux tests du service ICMP.

Le tableau ci-dessous décrit les éléments supplémentaires du moniteur ICMP.

Les éléments indiqués par un astérisque (*) sont disponibles en tant qu'attributs. Le nom des attributs est affiché entre parenthèses sous l'élément. L'absence d'astérisque indique qu'il n'existe aucun attribut équivalent. Les attributs entre parenthèses mais sans élément sont disponibles uniquement en tant qu'attributs, il n'existe aucun élément équivalent.

Tableau 66. Eléments du moniteur ICMP

Elément	Description
$averageRTT*(Average RTT)	Durée moyenne de la boucle, en secondes.
$endTime	Heure UNIX à laquelle la réponse a été reçue.
$jitter	Valeur absolue de la différence entre les heures d'arrivée de deux demandes d'écho ICMP adjacentes, moins leurs heures de départ. Cette valeur est calculée conformément à la formule spécifiée dans RFC2598. L'élément est créé uniquement si le nombre de demandes d'écho est supérieur à 1. Si plus de deux demandes d'écho sont utilisées, la valeur correspond à la gigue moyenne entre toutes les paires de demandes d'écho.
$lookupTime*(LookupTime)	Temps mis pour obtenir l'adresse IP du serveur hôte.
$maxRTT*(MaxRTT)	Durée maximale de la boucle, en secondes.
$minRTT* (MinRTT)	Durée minimale de la boucle, en secondes.
$numberPackets	Nombre de demandes d'écho ICMP envoyées, comme indiqué dans l'élément de profil.
$packetInterval	Temps d'attente entre l'envoi de chaque demande d'écho ICMP, comme indiqué dans l'élément de profil.
$packetRetries	Nombre de nouvelles tentatives effectuées par le moniteur pour renvoyer des demandes d'écho ICMP avant d'abandonner la procédure.
$packetSize	Taille (en octets) de chaque demande d'écho ICMP, comme indiqué dans l'élément de profil.
$pingAttempts Failed	Nombre de tentatives effectuées pour la première demande d'écho ICMP qui a échoué.
$pingAttempts Responded	Nombre de tentatives effectuées pour la première demande d'écho ICMP réussie.
$pingMessageFailed	Message renvoyé pour la première demande d'écho ICMP ayant échoué.
$pingMessage Responded	Message renvoyé pour la première demande d'écho ICMP réussie.
$pingReceivedTime Failed	Heure UNIX à laquelle la première réponse d'échec de l'écho a été reçue.
$pingReceivedTime Responded	Heure UNIX à laquelle la première réponse de réussite de l'écho a été reçue.
$pingRespondIP Failed	Adresse IP qui a répondu à la première demande d'écho ICMP ayant échoué.
$pingRespondIP Responded	Adresse IP qui a répondu à la première demande d'écho ICMP réussie.

Tableau 66. Eléments du moniteur ICMP (suite)	
Elément	**Description**
$pingRTTFailed	Durée de la boucle de la première demande d'écho ICMP ayant échoué, en secondes.
$pingRTTResponded	Durée de la boucle de la première demande d'écho ICMP réussie, en secondes.
$pingSentTime Failed	Heure UNIX à laquelle la première demande d'écho ICMP ayant échoué à été envoyée.
$pingSentTime Responded	Heure UNIX à laquelle la première demande d'écho ICMP réussie a été envoyée.
$pingsFailed	Nombre de demandes d'écho ICMP envoyées pour lesquelles il n'y a eu aucune réponse d'écho.
$pingsResponded	Nombre de réponses d'écho valides reçues.
$pingTime	Temps mis pour recevoir la réponse d'écho après l'envoi de la demande d'écho ICMP.
$respondPercent* (RespondPercent)	Pourcentage de demandes d'écho ICMP envoyées pour lesquelles il y a eu une réponse.
$responseTime	Temps mis pour que l'hôte cible réponde à une demande d'écho ICMP.
$sentTime	Heure UNIX à laquelle les demandes d'écho ICMP ont été envoyées.
$spreadRTT	Différence entre $maxRTT et $minRTT.
$startTime	Heure UNIX de début du test.
$totalHostTime	Temps mis pour recevoir la réponse d'écho après le début du test.
$typeOfService	Zone Type of Service de la couche IP, comme spécifié lors de l'ajout d'un nouvel élément ICMP. Pour plus d'informations, voir «Moniteur ICMP», à la page 353.

Le moniteur ICMP crée un ensemble distinct d'éléments $pingname pour enregistrer les résultats de chaque demande d'écho ICMP envoyée pendant le test. Le nombre de demandes envoyées est indiqué par $numberPackets. Par exemple, pour l'élément $pingRTT, si $numberPackets correspond à 3, le moniteur crée trois éléments ($pingRTT1, $pingRTT2 et $pingRTT3), qui contiennent les mesures de durée de la boucle des trois demandes d'écho ICMP envoyées.

Message d'état

Le moniteur ICMP fournit des messages d'état dans l'attribut ResultMessage lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Le tableau ci-dessous décrit les messages d'état ICMP.

Tableau 67. Messages d'état du moniteur ICMP	
Message	**Description**
Pings Complete	La demande d'écho ICMP a abouti.
ICMP echo failed	Le moniteur n'a pas pu émettre la demande d'écho ICMP en raison d'un problème avec l'hôte du moniteur ou avec sa connexion au réseau.
Timed out	La demande d'écho ICMP a dépassé le délai d'attente.

Tableau 67. Messages d'état du moniteur ICMP (suite)	
Message	**Description**
`Inaccessible`	Ce message est renvoyé par un routeur et n'est pas nécessairement correct.
`Source quench`	Un routeur est trop occupé pour traiter la demande d'écho ICMP.
`Time exceeded`	Ce message est renvoyé par un routeur. Il indique que la demande d'écho ICMP à été acheminée sur le réseau trop de fois.
`Parameter problem`	Ce message est renvoyé par un routeur. Il indique que le routeur ne peut pas traiter la demande d'écho ICMP. La cause peut être l'altération du message.

Propriétés

Les propriétés propres au moniteur ICMP sont décrites dans le tableau ci-dessous.

Tableau 68. Propriétés ICMP		
Nom de la propriété	**Paramètre de la propriété**	**Description**
`EventsPerSec`	non applicable	Cette propriété n'est pas prise en charge.
`IntraPingWait`	entier	L'intervalle de temps minimum, en millisecondes, entre toutes les commandes ping envoyées par le moniteur ICMP. Utilisez-le pour régler les paramètres de votre système afin de répartir le trafic réseau sur une période plus importante. Par exemple, dans un environnement comportant des milliers d'hôtes ICMP ciblés, affectez la valeur 3 à `IntraPingWait`. Valeur par défaut : `0`
`Ipv6Address`	entier	Adresse locale à lier comme origine pour les demandes d'écho ICMP lors de l'utilisation d'ICMP IPv6. Par défaut : aucune adresse
`MaxDNSResolvingThreads`	entier	Nombre maximal d'unités d'exécution qui doivent être utilisées par le programme de résolution DNS. Valeur par défaut : `20`
`MaxPacketSize`	entier	Taille maximale du paquet ICMP en octets.
`PingsPerSec`	entier	Nombre de demandes d'écho que le moniteur tente d'envoyer par seconde. Le nombre de demandes réellement envoyées dépend de la charge de l'unité centrale et du réseau. Valeur par défaut : `100`

Tableau 68. Propriétés ICMP (suite)		
Nom de la propriété	**Paramètre de la propriété**	**Description**
`SocketBufferSize`	entier	Taille de la mémoire tampon du socket de réception (en kilooctets). Valeur par défaut : 32

Moniteur LDAP

Le moniteur LDAP teste le fonctionnement des serveurs LDAP (Lightweight Directory Access Protocol).

Le tableau ci-dessous répertorie les fichiers du moniteur LDAP.

Tableau 69. Fichiers du moniteur LDAP	
Fichiers du moniteur	**Nom ou emplacement**
Exécutable du moniteur	`nco_m_ldap`
Fichier de propriétés	`$ISHOME/etc/props/ldap.props`
Fichier de règles	`$ISHOME/etc/rules/ldap.rules`
Fichier journal	`$ISHOME/log/ldap.log`

Consignes de configuration du moniteur LDAP

Le moniteur LDAP teste les services LDAP en établissant une connexion LDAP et en tentant de définir l'emplacement d'une entrée spécifique. Si le serveur arrive à effectuer cette action, il renvoie le contenu de l'entrée au moniteur. Le moniteur LDAP peut utiliser SSL pour authentifier le serveur LDAP et établir une connexion à ce dernier. Le moniteur LDAP peut utiliser SSL pour authentifier le serveur LDAP et établir une connexion à ce dernier.

Pour configurer le moniteur LDAP, il est nécessaire de comprendre le fonctionnement du protocole LDAP et du service d'annuaire surveillé. LDAP est un protocole Internet permettant d'accéder aux services d'annuaire et de les gérer. Un service d'annuaire est une application de base de données distribuée. Un annuaire est composé d'entrées. Ces entrées peuvent être liées aux employés ou aux ressources d'une organisation. Chaque entrée contient un ensemble d'attributs, par exemple, les entrées dans un annuaire

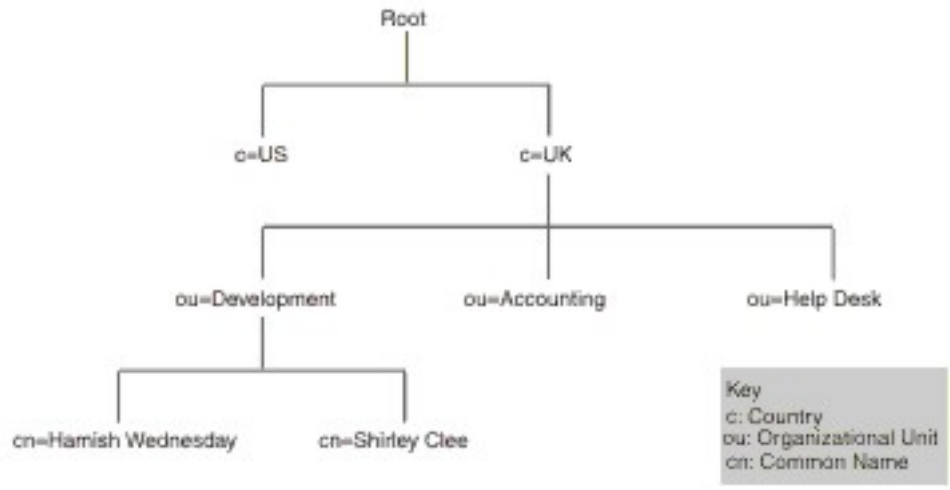
Des services d'annuaire individuels peuvent être construits différemment, et la procédure de surveillance peut également varier.

Versions LDAP

Le moniteur LDAP prend en charge les versions 2 et 3 de LDAP. Par défaut, il tente de se connecter au serveur LDAP cible qui utilise la version 3, puis revient automatiquement à la version 2 en cas d'échec. Vous pouvez forcer le moniteur à toujours utiliser la version en définissant la propriété **NOLDAPV3**.

Service d'annuaire exemple

Ce service d'annuaire exemple stocke des informations personnelles sur chaque employé. L'annuaire est divisé en pays puis en départements. Les employés et leurs attributs sont enregistrés sous chaque département.



L'image de la hiérarchie d'annuaire exemple présente un extrait d'annuaire. Cette figure présente une structure d'annuaire. Root apparaît au sommet. Les deux sous-répertoires représentent les pays et sont nommés UK et US. Le sous-répertoire UK se subdivise en trois sous-répertoires représentant les unités organisationnelles. Ils sont nommés Development, Accounting et Help Desk. Dans l'unité organisationnelle Development, il existe deux sous-répertoires, généralement nommés Shirley Clee et Hamish Wednesday.

Les entités sont référencées à l'aide de leurs noms distinctifs. Un nom distinctif désigne l'entité. Par exemple, les noms distinctifs du département Accounting et Hamish Wednesday sont :

```
dn="ou=accounting, c=UK"
dn="cn=Hamish Wednesday, ou=Development, c=UK"
```

L'entrée de chaque employé a plusieurs attributs. Par exemple, l'entrée d'Hamish Wednesday contient les détails ci-dessous.

```
cn: Hamish Wednesday
uid: ham
mail: HWednesday@development.mycompany.com
telephoneNumber: 88 88 55 44
```

Chaque entité dans la hiérarchie d'annuaire peut être protégée par un nom d'utilisateur (nom distinctif dans LDAP) et un mot de passe. Le moniteur utilise ce nom d'utilisateur et ce mot de passe pour accéder au serveur LDAP.

Lorsque le moniteur accède au serveur, il indique l'emplacement où commence la recherche de l'entité cible dans la hiérarchie d'annuaire. Ce paramètre est défini dans la zone searchBase en tant que nom distinctif. Par exemple, la recherche doit commencer au niveau du service :

```
ou=Accounting, c=UK
```

Remarque : Les entités qui constituent un nom distinctif se trouvent dans un ordre inversé. Elles commencent au point le plus bas dans la hiérarchie, puis listent chaque entité précédente.

L'entité cible est transmise au serveur dans la zone de filtre. Cette zone contient un attribut de l'entité cible. Par exemple, pour rechercher l'entité Hamish Wednesday's, le contenu de la zone de filtre peut être le suivant :

```
(uid=ham)
```

Le serveur LDAP utilise les zones fournies par le moniteur pour rechercher l'entité cible. Le résultat de la recherche est renvoyé au moniteur.

Si la recherche aboutit, le serveur renvoie également les attributs de l'entité cible. Le moniteur la convertit en éléments dont les noms sont créés dynamiquement. Par exemple, le moniteur convertit l'entrée d' Hamish Wednesday en :

```
$dnMatched = "cn=Hamish Wednesday, ou=Development, c=UK"
$cn = "Hamish Wednesday"
$uid = "ham"
$mail = "HWednesday@development.mycompany.com"
$telephoneNumber = "88 88 55 44"
```

Authentification LDAP

L'authentification du serveur LDAP SSL s'appuie sur les certificats de clé privés-publics signés par les autorités de certificat, comme Verisign et Thawte. Pour l'authentification SSL, le moniteur LDAP utilise la base de données Netscape cert7db des certificats publics afin de vérifier les signatures des certificats de serveur LDAP émises par les autorités de certification.

Si vous utilisez des certificats signés par une autorité de certification reconnue par Netscape, comme Verisign or Thawte, le moniteur LDAP les reconnaît automatiquement. Si vous utilisez des certificats signés par votre organisation ou par une organisation ne figurant pas dans la base de données Netscape, vous devez les ajouter à la base de données cert7db.

L'ajout des certificats à la base de données s'effectue par le biais de l'utilitaire certutil, disponible à partir de Netscape. La base de données cert7db du moniteur LDAP se trouve dans le fichier `$ISHOME/certificates/cert7.db`.

Pour surveiller les serveurs LDAP sécurisés via le chiffrement SSL ou TLS, définissez les variables d'environnement comme indiqué dans le tableau suivant :

Tableau 70. Variables d'environnement requises pour surveiller des serveurs LDAP sécurisés

Variable	Description	Paramètre
LDAPTLS_CACERT	Indique le fichier contenant les certificats de l'autorité de certification	Fichier contenant le certificat du serveur. Par exemple, `cacert.pem`.
LDAPTLS_REQCERT	Indique les vérifications à effectuer sur un certificat du serveur	Faites votre choix entre `never`|`allow`|`try`|`demand`.

Pour plus d'informations, voir http://www.openldap.org.

Propriétés

Les propriétés spécifiques du moniteur LDAP sont décrites dans le tableau suivant :

Tableau 71. Options des propriétés du moniteur LDAP

Nom de la propriété	Paramètre de la propriété	Description
NOLDAPV3	0|1	Oblige le moniteur à utiliser LDAP v2 au lieu de LDAP v3. 0 - utilise LDAP v3 1 - utilise LDAP v2

Suites de chiffrement

La propriété `SSLCipherSuite` spécifie l'algorithme de cryptographie utilisé par le moniteur LDAP. Pour plus d'informations sur les paramètres SSL, voir «Paramètre SSL dans Internet Service Monitoring», à la page 447.

Configuration des tests de service du moniteur LDAP

Utilisez les paramètres de configuration du moniteur LDAP pour définir les tests de service.

Lorsque vous configurez le moniteur, la valeur par défaut qui s'affiche pour le paramètres de délai est 30 secondes et 300 secondes pour le paramètre d'intervalle d'interrogation. D'autres valeurs par défaut répertoriées dans le tableau ne sont pas affichées pendant la configuration mais sont appliquées lors de la sauvegarde des détails de la configuration si aucune valeur n'a été indiquée.

Le tableau suivant décrit les configurations du moniteur LDAP :

Tableau 72. Configuration du moniteur LDAP

Zone	**Description**
server	Nom ou adresse IP du serveur LDAP à surveiller. Par exemple, `ldap.mycompany.in`.
searchbase	Nom distinctif de l'emplacement à partir duquel démarrer la recherche. Par exemple, `ou=Accounting, c=UK`.
filtre	Attribut de l'entité cible à rechercher. Par exemple, `(uid=ham)`.
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément. Par exemple, `moniteur LDAP`.
Rapports actifs	Sélectionne si l'élément de profil doit être activé après sa création. Par exemple, `Sélectionné`.
port	Port sur le serveur LDAP auquel se connecter. Vous devez spécifier le port SSL si vous utilisez l'authentification SSL. Par défaut : 389
username	Nom d'utilisateur pour la connexion au service d'annuaire. Le format du nom d'utilisateur dépend du Type d'authentification. Vous pouvez indiquer un domaine Windows, c'est-à-dire, `DOMAIN \username`. Par exemple, `jbloggs`.
password	Mot de passe utilisé pour se connecter au service d'annuaire, le cas échéant. Par exemple, `secret9`.
authenticationtype	Méthode d'authentification LDAP à utiliser : • SIMPLE (mot de passe anonyme ou en texte en clair) • SSL-SIMPLE • SASL-DIGEST-MD5 **Remarque :** L'authentification SASL-DIGEST-MD5 n'est pas disponible sur le système d'exploitation Linux. Si vous définissez le type d'authentification sur SIMPLE ou SSL-SIMPLE, entrez le nom d'hôte au format de nom distinctif. Si vous le définissez sur SASL-DIGEST-MD5, entrez le nom d'utilisateur sous la forme SASL bind-ids. Pour vous connecter au serveur LDAP en tant qu'utilisateur anonyme, définissez le type d'authentification sur SIMPLE et laissez à blanc les zones de nom d'utilisateur et de mot de passe. Par défaut : SIMPLE
saslrealm	Le domaine d'authentification du serveur LDAP ; généralement le nom de domaine complet du serveur. Pour partager des mots de passe entre plusieurs systèmes, vous pouvez utiliser un nom de domaine. Par exemple, `mycompany.com`.

Tableau 72. Configuration du moniteur LDAP (suite)	
Zone	**Description**
timeout	Délai d'attente, en secondes, d'une réponse du serveur. Par défaut : 30
poll	Délai, en secondes, entre chaque interrogation. Par défaut : 300
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Par défaut : 0
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Par défaut : 10

Classifications des niveaux de services

Les options de classification des niveaux de services disponibles pour le moniteur LDAP sont :

```
totalTime
connectTime
searchTime
initTime
dnMatched
message
```

Dans les classifications des niveaux de services :

- Spécifiez d'autres classifications des niveaux de services en entrant manuellement le nom de l'élément de moniteur. Ce nom doit correspondre à celui qui est indiqué pour l'élément dans la section des éléments Moniteurs.
- `message` peut correspondre à n'importe quel message transmis via l'élément **`$message`** au IBM Application Performance Management utilisé dans un widget. Pour obtenir une liste des valeurs possibles, voir Messages d'état.
- L'opérande est une chaîne ou un nombre positif.

Eléments du moniteur

Outre les résultats de test communs à tous les éléments, le moniteur LDAP génère un ensemble de résultats de test qui contient les données propres aux tests de service LDAP.

Le tableau suivant répertorie les éléments supplémentaires du moniteur LDAP.

Tableau 73. Eléments de moniteur LDAP	
Elément	**Description**
$authentication	Type de méthode d'authentification utilisateur requis par le serveur LDAP (standard ou CRAM-MD5).
$connectTime* (ConnectTime)	Durée nécessaire à la connexion au serveur LDAP.
$distinguishedName* (UserName)	Nom distinctif utilisé pour se connecter au service d'annuaire.
$dnMatched	L'entité a une correspondance dans la recherche.

Tableau 73. Eléments de moniteur LDAP (suite)	
Elément	**Description**
$filter* (SrchFilter)	Attribut permettant de définir l'emplacement de l'entité cible.
$initTime* (InitTime)	Durée nécessaire pour initialiser le client LDAP.
$port* (Port)	Port sur le serveur LDAP auquel le moniteur est connecté.
$saslRealm	Domaine SASL que vous avez indiqué après l'ajout d'un nouvel élément LDAP.
$searchBase* (SearchBase)	Nom distinctif de l'entité à partir de laquelle la recherche a été démarrée.
$searchTime* (SearchTime)	Durée nécessaire pour terminer la recherche.

Messages d'état

Le moniteur LDAP fournit des messages d'état dans l'attribut **ResultMessage** lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Le tableau ci-dessous décrit les messages d'état LDAP.

Tableau 74. Messages d'état du moniteur LDAP	
Message	**Description**
`Search successful`	Demande effectuée.
`Search failed`	La requête a échoué
`No match`	Le serveur n'a trouvé aucune entrée correspondante dans les critères de recherche.
`Connection timed out`	La connexion a abouti mais le serveur a cessé de répondre.
`Initialisation failed - an unrecognised authentication type was specified`	Se produit en cas d'utilisation d'un type d'authentification qui n'est pas pris en charge par le moniteur LDAP.
`Client initialisation failed`	L'initialisation des structures LDAP a échoué en raison d'une mémoire inadaptée.
`Bind (authentication) failed`	Le délai d'attente du serveur en attente de l'établissement de la liaison est dépassé.
`SASL bind is not possible because server does not support LDAPv3`	Le serveur doit prendre en charge LDAPv3 pour créer une liaison SASL.

Tableau 74. Messages d'état du moniteur LDAP (suite)	
Message	**Description**
`SASL bind is not possible because one of 'bind_id' (username), password or sasl_realm is blank`	Pour permettre une liaison, toutes les zones d'authentification doivent avoir une valeur. Ainsi une liaison SASL ne peut pas être établie si l'utilisateur est connecté de manière anonyme (en texte brut) à l'aide du type d'authentification SIMPLE.
`SASL bind error`	Le motif de l'échec de la fonction de liaison SASL ne peut pas être identifié.
`SASL bind authorisation error`	La liaison SASL a échoué en raison de justificatifs d'autorisation incorrects.

Moniteur IMAP4

Le moniteur IMAP4 fonctionne conjointement avec le moniteur SMTP pour tester la disponibilité et le temps de réponse d'un service de messagerie IMAP4.

Le tableau suivant répertorie les fichiers du moniteur IMAP4.

Tableau 75. Fichiers du moniteur IMAP4	
Fichiers du moniteur	**Nom ou emplacement**
Exécutable du moniteur	`nco_m_imap4`
Fichier de propriétés	`$ISHOME/etc/props/imap4.props`
Fichier de règles	`$ISHOME/etc/rules/imap4.rules`
Fichier journal	`$ISHOME/log/imap4.log`

Consignes de configuration du moniteur IMAP4

Le moniteur IMAP4 fonctionne conjointement avec le moniteur SMTP en surveillant la messagerie à laquelle le moniteur SMTP envoie les messages de test et en mesurant le temps nécessaire à la transmission de ces messages.

Remarque : Vérifiez que les horloges système de la machine hôte du moniteur et du serveur de messagerie sont synchronisées afin que le calcul de l'heure de remise fonctionne correctement.

Lorsque le moniteur IMAP4 a lu le contenu de la boîte aux lettres, il génère deux différents types d'événement :

- Evénements propres aux messages

  Le moniteur IMAP4 crée un événement propre aux messages pour chaque message électronique téléchargé à partir de la boîte aux lettres. Dans ce type d'événement, le moniteur attribue à l'élément `$message` la valeur `Message Successfully Downloaded`. L'élément `$timeToDeliver` est calculé en tant que durée nécessaire au transfert du message entre le moniteur SMTP qui l'a émis et la boîte aux lettres qui l'a reçu. L'élément `$hopCount` indique le nombre d'hôtes via lesquels le message a transité pour arriver à la boîte aux lettres.

- Evénements récapitulatifs

  Le moniteur crée un événement récapitulatif une fois qu'il a traité tous les messages dans la boîte aux lettres. Dans ce type d'événement, l'élément `message` indique le nombre total de messages téléchargés à partir de la boîte aux lettres et l'élément `totaltime` indique la durée nécessaire aux demandes. `$totaltime` est exprimé en secondes.

Messagerie sécurisée

Le moniteur IMAP4 prend en charge les connexions pour la sécurisation des services de messagerie. La connexion peut être effectuée à l'aide de SSL/TLS ou de la commande STARTTLS. Lors de la définition d'un élément de profil, utilisez la zone securitytype pour sélectionner la sécurité appropriée. Si le serveur de messagerie requiert un certificat côté client pour le chiffrement SSL, utilisez les propriétés SSL pour spécifier un fichier de certificats, un fichier de clés, un mot de passe de clé et une suite de chiffrement.

Certificats client

Le moniteur IMAP4 permet de surveiller les serveurs qui requièrent des certificats côté client pour une authentification mutuelle.

Spécifiez le fichier de certificats SSL, le fichier de clés et le mot de passe de clé lors de la création d'un élément de profil.

Les certificats doivent être au format PEM (Privacy Enhanced Mail). Si ce n'est pas le cas, vous devez convertir votre certificat au format PEM. Il est possible de convertir les certificats à l'aide d'un logiciel comme openSSL, lequel est disponible sur la page Web http://www.openssl.org.

Remarque : Si vous utilisez toujours les mêmes certificat, clé et mot de passe dans tous les éléments de profil, spécifiez-les en utilisant des propriétés de moniteur au lieu de les définir dans chaque élément de profil que vous créez.

Boîtes aux lettres

Une fois que le moniteur IMAP4 a traité les informations se trouvant dans un message électronique envoyé par le moniteur SMTP, il les supprime de la boîte aux lettres. Vous pouvez utiliser une boîte aux lettres existante pour stocker des messages électroniques entre les deux moniteurs même si la boîte aux lettres appartient à un utilisateur réel. Toutefois, il est recommandé de créer un compte de boîte aux lettres spécial pour le test de services.

Configuration des tests de service du moniteur IMAP4

Utilisez les paramètres de configuration du moniteur IMAP4 pour définir les tests de service.

Lorsque vous configurez le moniteur, des valeurs par défaut sont affichées pour les paramètres de délai et d'intervalle d'interrogation. Il s'agit respectivement des valeurs 30 et 300 secondes. D'autres valeurs par défaut répertoriées dans le tableau ne sont pas affichées pendant la configuration mais appliquées au moment de la sauvegarde des détails de la configuration si aucune valeur n'a été indiquée.

Tableau 76. Configuration du moniteur IMAP4

Zone	Description
server	Adresse IP du serveur de messagerie. Par exemple, `test.mycompany.com`
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément.
port	Port IP du serveur IMAP4. Valeur par défaut : 143

Tableau 76. Configuration du moniteur IMAP4 (suite)	
Zone	**Description**
securitytype	Type de connexion sécurisée ouverte avec le serveur de messagerie : • NONE - Connexion sans sécurité. • SSL - Envoi d'un message hello SSLv2, puis négociation SSLv2, SSLv3 ou TLSv1. • STARTTLS - Connexion sans sécurité, émission d'une commande STARTTLS, puis établissement d'une connexion via TLSv1. Valeur par défaut : NONE
username	Nom de boîte aux lettres.
password	Mot de passe utilisé pour se connecter à la boîte aux lettres, le cas échéant.
authenticationtype	Méthode d'authentification à utiliser (STANDARD ou CRAM_MD5) Valeur par défaut : STANDARD
sharedsecret	Secret partagé pour l'authentification CRAM_MD5, le cas échéant.
timeout	Délai d'attente, en secondes, avant une réponse du serveur. Valeur par défaut : 30
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : 300
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : 0
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : 10

Correspondance d'expressions régulières

Vous pouvez effectuer une recherche d'expression régulière sur les informations téléchargées en entrant jusqu'à 50 expressions régulières différentes. Le moniteur tente de faire correspondre le contenu extrait à chaque expression régulière.

Si une correspondance d'une expression régulière indiquée est trouvée, les lignes correspondantes (ou le nombre maximal de lignes correspondantes pouvant être stockées dans la mémoire tampon interne du moniteur) sont renvoyées dans l'élément $regexpMatchn correspondant. Si l'expression régulière a plusieurs correspondances dans les informations téléchargées, seule la première correspondance est renvoyée. L'état de chaque test d'expression régulière est indiqué par les éléments $regexpStatusn. Vous pouvez utiliser les correspondances d'expression régulière et les informations d'état en tant que critères pour les classifications de niveau de service.

Pour plus d'informations sur la syntaxe des expressions régulières, voir Tableau 50, à la page 335.

Eléments du moniteur

En plus des résultats de test communs à tous les éléments, le moniteur IMAP4 génère un ensemble de résultats de test contenant des données spécifiques aux tests de service IMAP4.

Le tableau suivant décrit les éléments supplémentaires du moniteur IMAP4.

Les éléments indiqués par un astérisque (*) sont disponibles en tant qu'attributs. Le nom des attributs est affiché entre parenthèses. L'absence d'astérisque indique qu'il n'existe aucun attribut équivalent. Les attributs entre parenthèses mais sans élément sont disponibles uniquement en tant qu'attributs, il n'existe aucun élément équivalent.

Tableau 77. Eléments du moniteur IMAP4

Elément	**Description**
$authentication	Type de méthode d'authentification requise par le serveur IMAP4 (Standard ou CRAM-MD5).
$bytesPerSec	Nombre moyen d'octets transférés par seconde.
$bytesTransferred	Nombre d'octets transférés ou téléchargés.
$connectTime	Temps mis pour se connecter au serveur IMAP4.
$downloadTime* (DownloadTime)	Temps mis pour télécharger le fichier.
$hopCount	Nombre d'hôtes via lesquels le message a transité pour arriver à la boîte aux lettres.
$inEvent	Indique que cet événement fait partie d'une série d'événements. 1 indique qu'il ne s'agit pas de l'événement final. 0 indique qu'il s'agit de l'événement final.
$lookupTime*(LookupTime)	Temps mis pour obtenir l'adresse IP du serveur hôte.
$port*(Port)	Port sur lequel le service est surveillé.
$responseTime* (ResponseTime)	Délai entre l'établissement de la connexion et la réception du premier octet de données.
$security	Type de connexion sécurisée ouverte avec le serveur de messagerie lors de l'ajout d'un élément IMAP (NONE, STARTTLS ou SSL).
$sentTo*(SentTo)	Adresse électronique utilisée par le moniteur SMTP pour envoyer le message d'origine.
$smtpServer	Nom du serveur SMTP à partir duquel le message électronique a été envoyé.
$SSLHandshakeTime* (SslHandshakeTime)	Temps mis pour établir la connexion SSL.
$timeToDeliver	Durée écoulée pour le transfert d'un message électronique entre un moniteur SMTP et la boîte aux lettres de destination.
$user*(ImapUser)	Nom d'utilisateur (nom de compte) utilisé par le moniteur pour la connexion au serveur IMAP4.

Message d'état

Le moniteur IMAP fournit des messages d'état dans l'attribut ResultMessage lorsqu'IBM Application Performance Management est utilisé. Ces messages indiquent le résultat du test.

Le tableau ci-dessous décrit les messages d'état IMAP4.

Tableau 78. Messages d'état du moniteur IMAP4	
Message	**Description**
`Message successfully downloaded`	Le téléchargement du message a réussi.
`Downloaded x messages`	Indique le nombre de messages dont le téléchargement à partir de la boîte aux lettres a réussi.
`Server not IMAP4rev1 compliant`	Le serveur IMAP4 ne respecte pas la spécification IMAP4 (RFC2060).
`Server does not support STARTTLS capability`	La configuration du serveur n'est pas correcte.
`Unable to log into server`	Le moniteur n'a pas pu se connecter au serveur IMAP.
`Unrecognised response to STATUS command`	Le moniteur ne reconnaît pas la valeur renvoyée par le serveur.
`Unrecognised response to FETCH INTERNALDATE command`	
`Failed to obtain Actual-Time-Sent header`	Le moniteur n'a pas obtenu la réponse attendue du serveur.
`Failed to obtain Actually-To header`	
`Failed to obtain SMTP-Server header`	

Propriétés

Les propriétés et les options de ligne de commande spécifiques au moniteur IMAP4 sont décrites dans le tableau suivant.

Tableau 79. Propriétés du moniteur IMAP4		
Nom de la propriété	**Paramètre de la propriété**	**Description**
`Originator`	chaîne	Spécifie la zone `From` qui doit correspondre lors de la récupération de messages électroniques envoyés par le moniteur SMTP. Le moniteur n'extrait que les messages dont la zone `From` correspond à la chaîne dans Originator (Emetteur). L'Emetteur IMAP4 doit correspondre à l'Emetteur dans le moniteur SMTP. Valeur par défaut : `SMTP-Monitor`
`SSLCertificate File`	chaîne	Chemin d'accès et nom du fichier de certificats numériques utilisé si aucun certificat n'est explicitement spécifié pour un élément HTTPS lors de sa création. Si le chemin n'est pas absolu, il est interprété par le moniteur comme étant relatif au répertoire de travail (`$ISHOME/platform/arch/bin`).

Tableau 79. Propriétés du moniteur IMAP4 (suite)		
Nom de la propriété	**Paramètre de la propriété**	**Description**
`SSLCipherSuite`	chaîne	Suite de chiffrement à utiliser pour les opérations SSL. Pour une description des valeurs possibles, voir Suites de chiffrement. Valeur par défaut : `RC4:3DES:DES:+EXP`
`SSLDisableTLS`	entier	Désactive TLSv1 pour la prise en charge des éléments existants. Valeur par défaut : `0` - TLSv1 est activé. `1` - TLSv1 est désactivé.
`SSLKeyFile`	chaîne	Fichier contenant la clé privée SSL.
`SSLKeyPassword`	chaîne	Mot de passe utilisé pour chiffrer la clé privée SSL.

Suites de chiffrement

La propriété `SSLCipherSuite` spécifie la suite de chiffrement utilisée par le moniteur IMAP4. Pour plus d'informations sur les paramètres SSL, voir «Paramètre SSL dans Internet Service Monitoring», à la page 447.

Moniteur NTP

Le moniteur NTP (Network Time Protocol) interroge un serveur NTP par le biais du protocole UDP (User Datagram Protocol) pour déterminer si le serveur indique l'heure correcte.

NTP utilise le format horaire UTC (temps universel coordonné) pour synchroniser les horloges des systèmes à la milliseconde près.

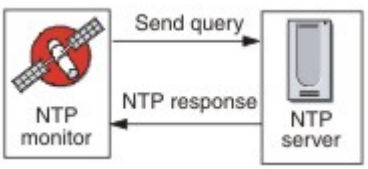
Le tableau ci-dessous répertorie les fichiers du moniteur NTP.

Tableau 80. Fichiers du moniteur NTP	
Fichiers du moniteur	**Nom et emplacement**
Exécutable du moniteur	`nco_m_ntp`
Fichier de propriétés	`$ISHOME/etc/props/ntp.props`
Fichier de règles	`$ISHOME/etc/ntp.rules`
Fichier journal	`$ISHOME/log/ntp.log`

Consignes de configuration du moniteur NTP

Le moniteur NTP acquiert des données en envoyant une requête à un serveur NTP, qui renvoie un paquet de réponses UDP avec l'heure en cours (telle qu'elle est vue par le serveur NTP).

L'image suivante présente un exemple des messages échangés entre le moniteur et le serveur NTP.



Configuration des tests de service du moniteur NTP

Les paramètres de configuration du moniteur NTP permettent de définir des tests de service.

Le tableau suivant décrit les configurations NTP :

Tableau 81. Configuration NTP

Zone	Description
server	Nom d'hôte du serveur NTP. Exemple : `ntp.mycompany.com`.
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément. Exemple : `NTP monitor`.
port	Port sur le serveur NTP à utiliser Par défaut : `123`
localip	Spécifie l'adresse IP de l'interface réseau sur le système hôte auquel le moniteur est associé lorsqu'il effectue le test. Si la propriété `IpAddress` du moniteur est définie, elle se substitue à la valeur de cette zone. Exemple : `102.168.n.n`.
version	Version du serveur NTP à utiliser (1, 2, 3 ou 4). Valeur par défaut : `1`
timeout	Délai d'attente, en secondes, d'une réponse du serveur. Valeur par défaut : `10`
retries	Nombre de nouvelles tentatives effectuées par le moniteur pour contacter le serveur NTP. Valeur par défaut : `0`
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`

Classification des niveaux des services

Les classifications des niveaux de services définissent les règles de détermination du niveau de service fourni via NTP.

Les options de classification des niveaux de services disponibles pour le moniteur NTP sont :

```
totalTime
responseTime
lookupTime
offset
adjustedOffset
message
```

Dans les classifications des niveaux de services :

- Spécifiez d'autres classifications des niveaux de services en entrant manuellement le nom de l'élément de moniteur. Ce nom doit correspondre à celui qui est indiqué pour l'élément dans la section des éléments Moniteurs.
- `message` peut correspondre à n'importe quel message transmis via l'élément `$message` au IBM Application Performance Management utilisé dans un widget. Pour obtenir une liste des valeurs possibles, voir Messages d'état.
- L'opérande est une chaîne ou un nombre positif.

Eléments du moniteur

Outre les résultats de test communs à tous les éléments, le moniteur NTP génère un ensemble de résultats de test qui contient les données propres aux tests de service NTP.

Le tableau suivant décrit les éléments supplémentaires du moniteur NTP.

Tableau 82. Eléments de moniteur NTP

Elément	**Description**
`$adjustedOffset`	Décalage de temps du serveur, en secondes.
`$localIP`	Adresse IP locale que le moniteur doit utiliser. Cet élément peut être vide sur un système n'ayant qu'une seule interface.
`$lookupTime*` (`LookupTime`)	Temps mis pour obtenir l'adresse IP du serveur hôte.
`$ntpVersionIn`	Version de protocole utilisée dans la réponse du serveur.
`$ntpVersionOut`	Version de protocole utilisée pour l'envoi.
`$offset`	Décalage de temps, en secondes, entre le serveur NTP et le système qui exécute le moniteur.
`$port*` (`Port`)	Port du serveur NTP à utiliser.
`$responseTime*` (`ResponseTime`)	Délai entre la connexion du moniteur au serveur NTP et la réception d'une réponse.
`$retries`	Nombre de nouvelles tentatives d'envoi d'une requête si aucun ID de réponse n'est reçu.

Messages d'état

Le moniteur NTP fournit des messages d'état dans l'attribut `ResultMessage` lorsque vous utilisez IBM Application Performance Management. Ces messages indiquent le résultat du test.

Le tableau ci-dessous décrit les messages d'état NTP.

Tableau 83. Messages d'état du moniteur NTP

Message	**Description**
`Successful query`	Le serveur NTP a donné la réponse attendue.
`Connection failed`	Impossible d'initialiser un socket UDP.

Tableau 83. Messages d'état du moniteur NTP (suite)	
Message	**Description**
`Failed to send request to NTP server`	Impossible d'écrire sur le socket UDP.
`No response from server`	Le serveur NTP n'a pas répondu.

Moniteur NNTP

Le moniteur NNTP teste la disponibilité d'un service NNTP en lisant et en postant des messages dans un forum.

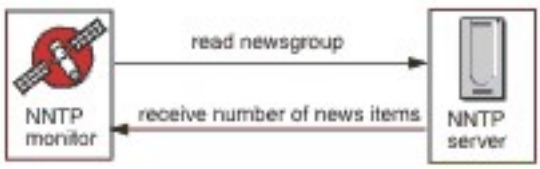
Le tableau ci-dessous répertorie les fichiers du moniteur NNTP.

Tableau 84. Fichiers du moniteur NNTP	
Fichiers du moniteur	**Nom ou emplacement**
Exécutable du moniteur	`nco_m_nntp`
Fichier de propriétés	`$ISHOME/etc/props/nntp.props`
Fichier de règles	`$ISHOME/etc/rules/nntp.rules`
Fichier journal	`$ISHOME/log/nntp.log`

Consignes de configuration du moniteur NNTP

Le moniteur NNTP teste les services NNTP en envoyant ou en lisant des données sur un serveur NNTP. Chaque élément de profil créé pour le moniteur effectue une opération de lecture ou d'envoi.

Dans une opération de lecture, le moniteur se connecte au service NNTP pour vérifier s'il existe un forum Internet particulier. Si c'est le cas, le moniteur enregistre le nombre de nouveaux éléments s'y trouvant. Il tente également d'enregistrer le dernier article ajouté au forum. L'image suivante illustre l'opération de lecture.



Dans une opération d'envoi (post), le moniteur vérifie qu'il existe un forum puis tente d'y écrire un message de test dont le sujet est `Message de test du moniteur NNTP`. L'image suivante illustre l'opération d'envoi (post).

Chaque élément de profil spécifie un `nomutilisateur` et un `motdepasse` fournis par le moniteur lorsqu'il accède à un serveur NNTP. Le moniteur utilise le système d'authentification en texte brut.

```
AUTHINFO USER nomutilisateur
AUTHINFO PASS motdepasse
```

Où `nomutilisateur` et `motdepasse` sont spécifiés dans l'élément de profil du moniteur.

Propriétés

Les options de propriétés spécifiques du moniteur NNTP sont décrites dans le tableau suivant.

Tableau 85. Options des propriétés du moniteur NNTP

Nom de la propriété	Paramètre de la propriété	Description
OutputDirectory	string	Indique le répertoire de sortie à utiliser si **`OutputResult`** a la valeur true (défini sur 1). Par défaut : `$ISHOME/var`
OutputResult	0|1	Indique que le moniteur peut sauvegarder les données reçues du service. 0 - désactivé 1 - activé

Configuration des tests de service du moniteur NNTP

Utilisez les paramètres de configuration du moniteur NNTP pour définir les tests de service.

Le tableau ci-dessous répertorie les configurations du moniteur NNTP.

Tableau 86. Configuration du moniteur NNTP

Zone	Description
server	Adresse IP du serveur NNTP. Par exemple, `news.mycompany.com`.
forum	Nom du forum utilisé par le moniteur pour envoyer et lire des messages de test. Par exemple, `mycompany.test`.
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément. Par exemple, READ.
port	Numéro du port du serveur NNTP. Par défaut : `119`
username	Nom d'utilisateur utilisé pour l'authentification sur le serveur NNTP.
password	Mot de passe du nom d'utilisateur utilisé pour l'authentification sur le serveur NNTP.
action	Indique si un article doit être envoyé ou récupéré. Peut être READ ou POST. Par défaut : POST
timeout	Délai d'attente, en secondes, d'une réponse du serveur. Valeur par défaut : `30`
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`

Correspondance d'expression régulière

Vous pouvez rechercher jusqu'à 50 expressions régulières parmi les informations téléchargées. Le moniteur NNTP tente de trouver une correspondance pour chaque expression régulière dans le contenu.

Si une correspondance d'une expression régulière indiquée est trouvée, les lignes correspondantes (ou le nombre maximal de lignes correspondantes pouvant être stockées dans la mémoire tampon interne du moniteur) sont renvoyées dans l'élément `$regexpMatchn` correspondant. Si l'expression régulière a plusieurs correspondances dans les informations téléchargées, seule la première correspondance est renvoyée. L'état de chaque test d'expression régulière est indiqué par les éléments `$regexpStatusn`. Vous pouvez utiliser les correspondances d'expression régulière et les informations d'état en tant que critères pour les classifications de niveau de service.

Pour plus d'informations, voir Tableau 50, à la page 335.

Classifications des niveaux de services

Les classifications des niveaux de services définissent les règles de détermination du niveau de service fourni via NNTP.

Les options de classification des niveaux de services disponibles pour le moniteur NNTP sont :

```
totalTime
lookupTime
connectTime
transferTime
responseTime
statut
bytesTransferred
bytesPerSec
newsItems
expected
lastLineReceived
checksum
previousChecksum
regexpMatch1 to 3
regexpStatus1 to 3
message
```

Dans les classifications des niveaux de services :

- Spécifiez d'autres classifications des niveaux de services en entrant manuellement le nom de l'élément de moniteur. Ce nom doit correspondre à celui qui est indiqué pour l'élément dans la section des éléments Moniteurs.
- `message` peut correspondre à n'importe quel message transmis via l'élément `$message` au IBM Application Performance Management utilisé dans un widget. Pour obtenir une liste des valeurs possibles, voir Messages d'état.
- L'opérande est une chaîne ou un nombre positif.
- Les codes de `status` `220` et `240` indiquent le succès. Voir le protocole NNTP pour les autres codes d'état renvoyés par l'opération.
- `egexpStatus`*n* peut avoir les valeurs suivantes :
  - `NONE` : aucune vérification d'expression régulière n'est configurée
  - `MATCHED` : une correspondance a été trouvée pour l'expression régulière
  - `FAILED` : aucune correspondance n'a été trouvée pour l'expression régulière
- Evaluez les correspondances d'expression régulière qui utilisent les expressions de test au format suivant :

  ```
  regexpMatchn [contains|!contains] expression
  ```

  Utilisez les opérateurs `contains` et `!contains` à la place de = et `!=` car `regexpMatch`*n* contient normalement la ligne entière qui correspond à l'expression régulière et non à une partie seulement de celle-ci, de sorte que les opérateurs = et `!=` ne correspondent souvent pas à l'expression.

- Les éléments Checksum et PreviousChecksum ne fournissent normalement pas de valeurs significatives pour les classifications des niveaux de services car les valeurs de somme de contrôle sont inconnues au moment de la création de l'élément de profil (ces valeurs sont calculées par le moniteur lors l'exécution des tests). Les éléments de moniteur $checksum et $previousChecksum sont destinés à l'enrichissement des alertes par le biais du fichier de règles du moniteur.

Eléments du moniteur

Outre les résultats de test communs à tous les éléments, le moniteur NNTP génère un ensemble de résultats de test qui contient les données propres aux tests de service NNTP.

Le tableau suivant décrit les éléments supplémentaires du moniteur NNTP.

Tableau 87. Eléments du moniteur NNTP

Elément	**Description**
$action* (NntpAction)	Action effectuée par le moniteur. Peut être READ ou POST.
$bytesPerSec	Nombre moyen d'octets transférés par seconde.
$bytesTransferred	Nombre d'octets transférés ou téléchargés.
$checksum	L'élément Checksum ne fournit normalement pas de valeurs significatives pour les classifications des niveaux de services car les valeurs de somme de contrôle sont inconnues au moment de la création de l'élément de profil (ces valeurs sont calculées par le moniteur lors de l'exécution des tests). Les éléments de moniteur $checksum et $previousChecksum sont destinés à l'enrichissement des alertes par le biais du fichier de règles du moniteur.
$connectTime* (ConnectTime)	Durée nécessaire à l'établissement d'une connexion au serveur NNTP.
$downloadTime	Temps mis pour télécharger le fichier.
$group* (NntpGroup)	Nom du groupe de discussion surveillé.
$lastLineReceived	Cet élément est uniquement défini si l'élément $message contient le message Expect Failed. Si c'est le cas, il contient la réponse du serveur NNTP.
$lookupTime* (LookupTime)	Durée nécessaire à la recherche de l'adresse IP du serveur.
$newsItems	Nombre d'articles de forum dans le forum.
$password	Mot de passe utilisé pour authentifier le moniteur.

Tableau 87. Eléments du moniteur NNTP (suite)	
Elément	**Description**
$previousChecksum	L'élément PreviousChecksum ne fournit normalement pas de valeurs significatives pour les classifications des niveaux de services car les valeurs de somme de contrôle sont inconnues au moment de la création de l'élément de profil (ces valeurs sont calculées par le moniteur lors de l'exécution des tests). Les éléments de moniteur $previousChecksum et $checksum sont destinés à l'enrichissement des alertes par le biais du fichier de règles du moniteur.
$responseTime* (ResponseTime)	Délai entre la création d'une connexion et la réception du premier octet de l'article cible.
$status	Code d'état renvoyé par le serveur NNTP.
$transferTime* (TransferTime)	Définit la valeur sur $uploadTime ou $downloadTime.
$uploadTime	Temps mis pour charger le fichier.
$username	Nom d'utilisateur utilisé pour authentifier le moniteur.
Si $message contient $ExpectFailed	
$expected	Texte dans la connexion que le moniteur attendait lors de l'échec de la connexion.
$lastLineReceived	Dernière ligne du texte dans la connexion que le moniteur a reçu du serveur NNTP.

Messages d'état

Le moniteur NNTP fournit des messages d'état dans l'attribut ResultMessage lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Le tableau ci-dessous décrit les messages d'état NNTP.

Tableau 88. Messages d'état du moniteur NNTP	
Message	**Description**
Article Posted	L'action NNTP POST a abouti.
Article Retrieved	L'action NNTP READ a abouti.
Not Found	L'article n'a peut-être pas été localisé.
Expect failed	La requête NNTP a échoué.
Timed out waiting to read	Une connexion de données a été établie avec le serveur, mais ce dernier ne répond plus.

Tableau 88. Messages d'état du moniteur NNTP (suite)	
Message	**Description**
`Connection failed`	Le moniteur n'a pas pu se connecter au serveur. Pour plus d'informations, consultez le fichier journal.
`Connection closed by foreign host`	L'hôte distant a fermé la connexion avant que le moniteur ne le prévoit.

Moniteur POP3

Le moniteur POP3 fonctionne conjointement avec le moniteur SMTP pour tester la disponibilité et le temps de réponse d'un service de messagerie POP3.

Le tableau suivant répertorie les fichiers du moniteur POP3.

Tableau 89. Fichiers du moniteur POP3	
Fichiers du moniteur	**Nom ou emplacement**
Exécutable du moniteur	`nco_m_pop3`
Fichier de propriétés	`$ISHOME/etc/props/pop3.props`
Fichier de règles	`$ISHOME/etc/rules/pop3.rules`
Fichier journal	`$ISHOME/log/pop3.log`

Consignes de configuration du moniteur POP3

Le moniteur POP3 fonctionne conjointement au moniteur SMTP en surveillant la messagerie à laquelle le moniteur SMTP envoie les messages de test et en mesurant la durée nécessaire à la transmission de ces messages.

Remarque : Vérifiez que les horloges système de la machine hôte du moniteur et du serveur de messagerie sont synchronisées afin que le calcul de l'heure de remise fonctionne correctement.

Lorsque le moniteur POP3 a lu le contenu de la boîte aux lettres, il génère deux différents types d'événement :

- Evénements propres aux messages

  Le moniteur POP3 crée un événement propre aux message pour chaque message électronique téléchargé à partir de la boîte aux lettres. Dans ce type d'événement, le moniteur attribue à l'élément `$message` la valeur `Message Successfully Downloaded`. L'élément `$timeToDeliver` est calculé en tant que durée nécessaire au transfert du message entre le moniteur SMTP qui l'a émis et la boîte aux lettres qui l'a reçu. L'élément `$hopCount` indique le nombre d'hôtes via lesquels le message a transité pour arriver à la boîte aux lettres.

- Evénements récapitulatifs

  Le moniteur crée un événement récapitulatif une fois qu'il a traité tous les messages dans la boîte aux lettres. Dans ce type d'événement, l'élément `message` indique le nombre total de messages téléchargés à partir de la boîte aux lettres et l'élément `totaltime` indique la durée nécessaire aux demandes. `$totaltime` est exprimé en secondes.

Messagerie sécurisée

Le moniteur POP3 prend en charge les connexions pour la sécurisation des services de messagerie. La connexion peut être effectuée à l'aide de SSL/TLS ou de la commande STARTTLS. Lors de la définition d'un élément de moniteur POP3, utilisez la zone Type de sécurité pour sélectionner la sécurité appropriée. Si le serveur de messagerie requiert un certificat côté client pour le chiffrement SSL, utilisez les propriétés `SSLname` ou les options de ligne de commande pour spécifier un fichier de certificats, un fichier de clés, un mot de passe de clé et une suite de chiffrement.

Certificat côté client

Le moniteur POP3 permet de surveiller les serveurs qui requièrent des certificats côté client pour une authentification mutuelle. Spécifiez le fichier de certificats SSL, le fichier de clés et le mot de passe de clé lors de la création d'un élément de profil. Les certificats doivent être au format PEM (Privacy Enhanced Mail). Si ce n'est pas le cas, vous devez convertir votre certificat au format PEM. Il est possible de convertir les certificats à l'aide d'un logiciel comme openSSL, lequel est disponible sur la page Web http://www.openssl.org.

Remarque : Si vous utilisez toujours les mêmes certificat, clé et mot de passe dans tous les éléments de profil, spécifiez-les en utilisant des propriétés de moniteur au lieu de les définir dans chaque élément de profil que vous créez.

Configuration des tests du moniteur POP3

Remarque : Surveillez le fonctionnement du serveur de messagerie `mail.mycompany.com` en configurant le moniteur SMTP de telle sorte qu'il envoie des messages à une boîte aux lettres test et en configurant le moniteur POP3 de telle pour l'extraction des messages. L'adresse de la boîte aux lettres est `ismtest@mycompany.com` et ses données d'identification sont `ismtest/secret1`. Utilisez un délai de connexion de 20 secondes, 2 nouvelles tentatives en cas d'échec et un intervalle de cinq secondes, et testez les services toutes les dix minutes. Utilisez les classifications de niveau de service par défaut fournis par les éléments de profil.

Tableau 90. Configuration du moniteur POP3

Zone	Description
server	Adresse IP du serveur de messagerie. Par exemple, `mail.mycompany.com`
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément.
port	Numéro du port du serveur de messagerie. Valeur par défaut : `110`
securitytype	Type de connexion sécurisée ouverte avec le serveur de messagerie : • `NONE` - Connexion sans sécurité • `SSL` - Envoi d'un message `hello` SSLv2, puis négociation SSLv2, SSLv3 ou TLSv1 • `STARTTLS` - Connexion sans sécurité, émission d'une commande STLS, puis établissement d'une connexion via TLSv1. Il s'agit du type de sécurité le plus sûr. • `NONE` - Connexion sans sécurité Valeur par défaut : `NONE`
username	Nom de boîte aux lettres.
password	Mot de passe utilisé pour se connecter à la boîte aux lettres, le cas échéant.

Tableau 90. Configuration du moniteur POP3 (suite)	
Zone	**Description**
authenticationtype	Méthode d'authentification à utiliser et dont le libellé est Type d'authentification : • STANDARD - Utilise un échange nom d'utilisateur/mot de passe où le mot de passe n'est pas chiffré. Cette méthode est appropriée pour une utilisation intermittente du protocole POP3. • APOP - Utilisez cette méthode quand le client POP3 se connecte régulièrement au serveur. Elle offre un niveau de sécurité plus élevé que la méthode standard. Assurez-vous de spécifier un secret partagé APOP si vous sélectionnez APOP. Notez que tous les serveurs ne prennent pas en charge APOP. Valeur par défaut : STANDARD.
sharedsecret	Secret partagé pour l'authentification APOP. Applicable uniquement si vous utilisez le type d'authentification APOP. La chaîne doit comporter au moins huit caractères et est masquée dans l'interface utilisateur.
timeout	Délai d'attente, en secondes, avant une réponse du serveur. Valeur par défaut : 30
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : 300
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : 0
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : 10
verifycertificate	Certificat de vérification du serveur. Valeur par défaut : Disabled

Utilisez les paramètres de configuration du moniteur POP3 pour définir les tests de service.

Correspondance d'expressions régulières

Vous pouvez effectuer une recherche d'expression régulière sur les informations téléchargées en entrant jusqu'à 50 expressions régulières différentes. Le moniteur tente de faire correspondre le contenu extrait à chaque expression régulière.

Si une correspondance d'une expression régulière indiquée est trouvée, les lignes correspondantes (ou le nombre maximal de lignes correspondantes pouvant être stockées dans la mémoire tampon interne du moniteur) sont renvoyées dans l'élément `$regexpMatchn` correspondant. Si l'expression régulière a plusieurs correspondances dans les informations téléchargées, seule la première correspondance est renvoyée. L'état de chaque test d'expression régulière est indiqué par les éléments `$regexpStatusn`. Vous pouvez utiliser les correspondances d'expression régulière et les informations d'état en tant que critères pour les classifications de niveau de service.

Pour plus d'informations sur la syntaxe des expressions régulières, voir Tableau 50, à la page 335.

Eléments du moniteur

En plus des résultats de test communs à tous les éléments, le moniteur POP3 génère un ensemble de résultats de test contenant des données spécifiques aux tests de service POP3.

LeTableau 1 décrit les éléments supplémentaires du moniteur POP3.

Les éléments indiqués par un astérisque (*) sont disponibles en tant qu'attributs. Le nom des attributs est affiché entre parenthèses. L'absence d'astérisque indique qu'il n'existe aucun attribut équivalent. Les attributs entre parenthèses mais sans élément sont disponibles uniquement en tant qu'attributs, il n'existe aucun élément équivalent.

Tableau 91. Eléments du moniteur IMAP4

Elément	Description
$authentication	Type de méthode d'authentification requise par le serveur IMAP4 (Standard ou CRAM-MD5).
$bytesPerSec	Nombre moyen d'octets transférés par seconde.
$bytesTransferred	Nombre d'octets transférés ou téléchargés.
$connectTime	Temps mis pour se connecter au serveur IMAP4.
$downloadTime* (DownloadTime)	Temps mis pour télécharger le fichier.
$hopCount	Nombre d'hôtes via lesquels le message a transité pour arriver à la boîte aux lettres.
$inEvent	Indique que cet événement fait partie d'une série d'événements. 1 indique qu'il ne s'agit pas de l'événement final, 0 indique qu'il s'agit de l'événement final.
$lookupTime*(LookupTime)	Temps mis pour obtenir l'adresse IP du serveur hôte.
$port*(Port)	Port sur lequel le service est surveillé.
$responseTime* (ResponseTime)	Délai entre l'établissement de la connexion et la réception du premier octet de données.
$security	Type de connexion sécurisée ouverte avec le serveur de messagerie lors de l'ajout d'un élément IMAP (NONE, STARTTLS ou SSL).
$sentTo*(SentTo)	Adresse électronique utilisée par le moniteur SMTP pour envoyer le message d'origine.
$smtpServer	Nom du serveur SMTP à partir duquel le message électronique a été envoyé.
$SSLHandshakeTime* (SslHandshakeTime)	Temps mis pour établir la connexion SSL.
$timeToDeliver	Durée écoulée pour le transfert d'un message électronique entre un moniteur SMTP et la boîte aux lettres de destination.
$user*(ImapUser)	Nom d'utilisateur (nom de compte) utilisé par le moniteur pour la connexion au serveur IMAP4.

Message d'état

Le moniteur POP3 fournit des messages d'état dans l'attribut ResultMessage lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Le tableau suivant décrit les messages d'état POP3.

Tableau 92. Messages d'état du moniteur POP3	
Message	**Description**
`Message successfully downloaded`	La requête POP3 a abouti.
`Downloaded` *x* `messages`	Indique le nombre de messages téléchargés à partir de la boîte aux lettres.
`Timed out waiting to read/write`	Une connexion de données a été établie avec le serveur, mais il a cessé de répondre.
`Connection closed by foreign host`	L'hôte distant a fermé la connexion plus tôt que prévu par le moniteur.
`Connection failed`	Le moniteur n'a pas pu se connecter au serveur. Pour plus d'informations, reportez-vous au fichier journal.
`APOP not supported by the server`	La méthode d'authentification APOP n'est pas prise en charge par le serveur. Utilisez le type d'authentification Standard à la place.
`APOP service not available`	L'implémentation du serveur APOP n'est pas prise en charge par le moniteur. Utilisez le type d'authentification Standard à la place.
`Server does not support STLS capability`	Le serveur ne prend pas en charge STARTTLS. Utilisez un autre type de sécurité.

Propriétés

Les propriétés spécifiques au moniteur POP3 sont décrites dans le tableau suivant.

Tableau 93. Propriétés et options de ligne de commande du moniteur POP3		
Nom de la propriété	**Paramètre de la propriété**	**Description**
`SSLCertificate File`	chaîne	Chemin et nom du fichier de certificats numériques utilisé si aucun certificat n'est explicitement spécifié pour un élément POP3 lors de sa création. Si le chemin d'accès n'est pas absolu, il est interprété par le moniteur comme étant relatif par rapport au répertoire de travail (`$ISHOME/platform/`*`arch`*`/bin`).
`SSLCipherSuite`	chaîne	Suite de chiffrement à utiliser pour les opérations SSL. Valeur par défaut : `RC4:3DES:DES:+EXP`. Pour une description des valeurs possibles, voir Suites de chiffrement.
`SSLDisableTLS`	entier	Désactive TLSv1 pour la prise en charge des éléments existants. Valeur par défaut : `0` - TLSv1 est activé. Définir sur `1` pour désactiver TLSv1.
`SSLKeyFile`	chaîne	Fichier contenant la clé privée SSL.
`SSLKeyPassword`	chaîne	Mot de passe utilisé pour chiffrer la clé privée SSL.

Suites de chiffrement

La propriété `SSLCipherSuite` spécifie la suite de chiffrement utilisée par le moniteur POP3. Pour plus d'informations sur les paramètres SSL, voir «Paramètre SSL dans Internet Service Monitoring», à la page 447.

Moniteur RADIUS

RADIUS (Remote Authentication Dial-In User Service, service utilisateur d'accès téléphonique pour une authentification à distance) fournit une authentification pour l'accès distant aux services. Le moniteur RADIUS simule un système client qui accède à un service RADIUS et renvoie les données sur les performances du service.

Le tableau ci-dessous répertorie les fichiers du moniteur RADIUS.

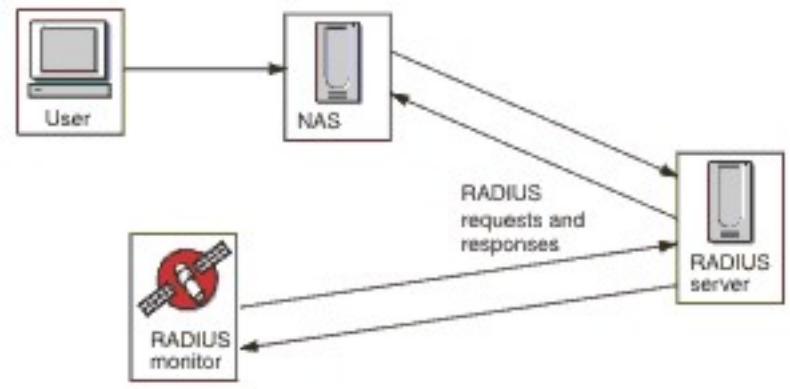
Tableau 94. Fichiers du moniteur RADIUS

Fichiers du moniteur	**Nom et emplacement**
Exécutable du moniteur	`nco_m_radius`
Fichier de propriétés	`$ISHOME/etc/props/radius.props`
Fichier de règles	`$ISHOME/etc/rules/radius.rules`
Fichier journal	`$ISHOME/log/http.log`

Consignes de configuration du moniteur Radius

Le moniteur RADIUS simule le fonctionnement d'un serveur NAS (Network Access Server), en envoyant des demandes à un serveur RADIUS.

Le moniteur RADIUS utilise UDP pour envoyer des demandes au serveur RADIUS et génère ensuite des événements qui contiennent les résultats de ces demandes et les données sur les performances du serveur. L'image suivante illustre le fonctionnement du moniteur.



Le moniteur peut tester les opérations d'authentification et de compatibilité des serveurs RADIUS :

- Demandes d'accès par le biais du protocole d'authentification de mot de passe (PAP)
- Demandes d'accès par le biais du protocole CHAP (Challenge-Handshake Authentication Protocol)
- Demandes de comptabilité : Start, Stop, Accounting On et Accounting Off

Propriétés

Les options de propriétés spécifiques du moniteur RADIUS sont décrites dans le tableau ci-dessous.

Tableau 95. Options des propriétés du moniteur RADIUS		
Nom de la propriété	**Paramètre de la propriété**	**Description**
FramedServiceRequest	0|1	Lorsque cette propriété est définie sur 1, le moniteur sélectionne le type de service encadré défini dans les demandes d'accès. 0 - désactivé 1 - activé

Configuration des tests de service du moniteur Radius

Les paramètres de configuration du moniteur RADIUS permettent de définir des tests de service.

Le tableau suivant décrit les configurations du moniteur Radius :

Tableau 96. Configuration du moniteur RADIUS	
Zone	**Description**
server	Adresse IP du serveur RADIUS.
sharedsecret	Secret partagé permettant l'authentification du moniteur.
username	Nom d'utilisateur fourni par le moniteur pour authentifier le serveur RADIUS.
password	Mot de passe fourni par le moniteur pour authentifier le serveur RADIUS.
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément.
requesttype	Spécifie le type de requête envoyé au serveur RADIUS : • Authenticate (CHAP) • Authenticate (PAP) • Accounting Par défaut : Authenticate(CHAP)
port	Port permettant de se connecter au serveur RADIUS. Par défaut : 1812
localip	Spécifie l'adresse IP de l'interface réseau sur le système hôte auquel le moniteur est associé lorsqu'il effectue le test. Si la propriété IpAddress du moniteur est définie, elle se substitue à la valeur de cette zone.
loginhost	Définit la valeur de l'attribut Login-IP-Host dans la requête d'accès.
calledstation	Définit la valeur de l'attribut Called-Station-Id dans la requête d'accès.

Tableau 96. Configuration du moniteur RADIUS (suite)	
Zone	**Description**
callingstation	Définit la valeur de l'attribut `Calling-Station-Id` dans la requête d'accès.
accountsessionid	Définit la valeur de l'attribut `Acct-Session-Id` dans les paquets de demande de comptabilité envoyés au serveur de comptabilité. **Remarque :** Cette zone s'applique uniquement au type de requête `Accounting`.
accountstatustype	Définit la valeur de l'attribut `Acct-Status-Type` dans les paquets de demande de comptabilité envoyés au serveur de comptabilité. • `Start` • `Stop` • `Accounting On` • `Accounting Off` **Remarque :** Cette zone s'applique uniquement au type de requête `Accounting`. Par défaut : `Start`
accountsessiontime	Définit la valeur de l'attribut `Acct-Session-Time` (en secondes) dans les paquets de demande de comptabilité envoyés au serveur de comptabilité. **Remarque :** Cette zone s'applique uniquement au type de requête `Accounting`.
nasip	Attribut `NAS-IP-Address` envoyé par le moniteur RADIUS comme partie intégrante d'un paquet de demande d'accès.
nasport	Attribut `NAS-Port` envoyé par le moniteur RADIUS comme partie intégrante d'un paquet de demande d'accès.
timeout	Délai d'attente, en secondes, d'une réponse du serveur. Valeur par défaut : `10`
retries	Nombre de nouvelles tentatives de connexion au serveur RADIUS en cas de problème. Valeur par défaut : `0`
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`

Classification des niveaux de services

Les classifications des niveaux de services définissent les règles de détermination du niveau de service fourni par le service RADIUS.

Les options de classification des niveaux de services disponibles pour le moniteur RADIUS sont :

```
totalTime
lookupTime
responseTime
message
```

Dans les classifications des niveaux de services :

- Spécifiez d'autres classifications des niveaux de services en entrant manuellement le nom de l'élément de moniteur. Ce nom doit correspondre à celui qui est indiqué pour l'élément dans la section des éléments Moniteurs.
- `message` peut correspondre à n'importe quel message transmis via l'élément `$message` au IBM Application Performance Management utilisé dans un widget. Pour obtenir une liste des valeurs possibles, voir Messages d'état.
- L'opérande est une chaîne ou un nombre positif.

Eléments du moniteur

Outre les résultats de test communs à tous les éléments, le moniteur RADIUS génère un ensemble de résultats de test contenant les données propres aux tests de service RADIUS.

Le tableau suivant décrit les éléments supplémentaires du moniteur RADIUS.

Tableau 97. Eléments de moniteur RADIUS

Elément	**Description**
`$accountSessionId`	Identificateur unique utilisé pour faire correspondre les enregistrements de début et de fin.
`$accountSessionTime`	Lorsque `accountStatusType` est défini sur `Stop`, cette zone indique, en secondes, la durée pendant laquelle l'utilisateur reçoit le service.
`$accountStatusType`	Indique si le service de l'utilisateur commence (`start`) ou s'arrête (`stop`).
`$calledStationId`	Le moniteur RADIUS envoie calledStationId comme partie intégrante du paquet de demande d'accès. Cet élément est utilisé s'il est requis par le serveur RADIUS ; il ne l'est pas si `callingStationId` est utilisé.
`$callingStationId`	Le moniteur RADIUS envoie `callingStationId` comme partie intégrante d'un paquet de demande d'accès. Cet élément est utilisé s'il est requis par le serveur RADIUS ; il ne l'est pas si `calledStationId` est utilisé.
`$localIP`	Adresse IP locale que le moniteur doit utiliser. Cet élément peut être vide sur un système n'ayant qu'une seule interface.
`$loginIPHost*` (`LoginIpHost`)	Le moniteur RADIUS envoie loginIPHost comme partie intégrante d'un paquet de demande d'accès. Cet élément peut être requis par les serveurs surveillés.

Tableau 97. Eléments de moniteur RADIUS (suite)	
Elément	**Description**
$lookupTime* (LookupTime)	Temps mis pour obtenir l'adresse IP du serveur hôte.
$nasPort* (NasPort)	Le paramètre NAS Port envoyé par le moniteur RADIUS comme partie intégrante d'un paquet de demande d'accès. Valeur par défaut : 0.
$password	Mot de passe utilisé pour authentifier le moniteur.
$port* (Port)	Port sur lequel le service est surveillé.
$requestType	Indique le type de demande sélectionné pour l'élément, soit PAP, CHAP ou Accounting.
$responseTime	Durée écoulée entre l'envoi d'une demande au serveur RADIUS et la réception d'une réponse.
$retries	Nombre maximum de nouvelles tentatives.
$secret	Mot de passe du secret partagé issu du fichier de configuration.
$username* (RadiusUser)	Nom d'utilisateur utilisé pour authentifier le moniteur.

Messages d'état

Le moniteur RADIUS fournit des messages d'état dans l'attribut ResultMessage lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Le tableau suivant décrit les messages d'état du moniteur RADIUS

Tableau 98. Messages d'état du moniteur RADIUS	
Message	**Description**
CHAP authentication - Access granted	Le moniteur a été authentifié (en utilisant CHAP). Cet élément est renvoyé uniquement si le type de demande CHAP a été utilisé.
PAP authentication - Access granted	Le moniteur a été authentifié (en utilisant PAP). Cet élément est renvoyé uniquement si le type de demande PAP a été utilisé.
Accounting response received	Une réponse de comptabilité a été reçue du serveur. La transaction se poursuit.
Connection failed	Le nom du serveur spécifié n'est pas valide.
Failed to send request to RADIUS server	Un paquet UDP n'a peut-être pas été enregistré sur le réseau. Aucune information supplémentaire sur l'erreur n'est disponible.

Tableau 98. Messages d'état du moniteur RADIUS (suite)	
Message	**Description**
`No response from server`	Le serveur RADIUS ne répond pas.
`Incorrect identifier returned`	Le serveur a envoyé une réponse à une requête qui n'a pas été envoyée par le moniteur.
`Invalid response authenticator`	La réponse contenait une autorisation imprévue. Cela peut être dû à un secret partagé ou mot de passe incorrect.
`Unrecognized response`	Le serveur n'a pas reconnu le paquet envoyé.
`PAP authentication - Access denied`	Le moniteur n'a pas été authentifié (en utilisant PAP).
`CHAP authentication - Access denied`	Le moniteur n'a pas été authentifié (en utilisant CHAP).

Moniteur RPING

Le moniteur RPING teste la disponibilité des périphériques réseau en lançant une commande ping distante à partir d'un routeur. Il fournit les données de performance sur la durée maximale, minimale et moyenne de la boucle.

Le moniteur prend en charge les routeurs Cisco et Juniper, et les routeurs compatibles RFC2925.

Le tableau suivant répertorie les fichiers du moniteur RPING.

Tableau 99. Fichiers du moniteur RPING	
Fichiers du moniteur	**Nom ou emplacement**
Exécutable du moniteur	`nco_m_rping`
Fichier de propriétés	`$ISHOME/etc/ims/props/rping.props`
Fichier de règles	`$ISHOME/etc/ims/rules/rping.rules`
Fichier journal	`$ISHOME/log/rping.log`
Fichiers script	`$ISHOME/scripts/rping/cisco.s` (script SNMP pour les routeurs Cisco) `$ISHOME/scripts/rping/juniper.s` (script SNMP pour les routeurs Juniper) `$ISHOME/scripts/rping/rfc2925` (script SNMP pour les routeurs compatibles RFC2925)

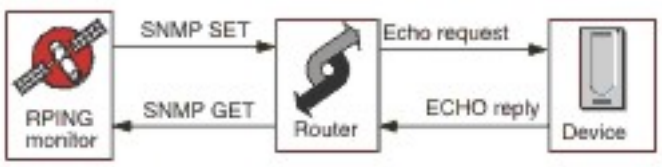
Consignes de configuration du moniteur RPING

Le moniteur RPING acquiert des données en configurant le routeur pour qu'il émette une commande ping sur une unité réseau et en l'interrogeant régulièrement afin d'obtenir les résultats de ces commandes.

Il configure les tests ping à l'aide d'une commande SNMP SET pour créer une ligne de contrôle dans la commande ping de la base d'informations de gestion du routeur, et extrait ensuite de celle-ci les

données ping par le biais des commandes SNMP GET. Toutes les communications avec le routeur s'effectuent via SNMP.

L'image suivante présente un exemple des messages échangés entre le moniteur et le périphérique réseau.



Activation de demande Ping éloignée sur des routeurs Cisco

Par défaut, les demandes SNMP ping éloignées sur les routeurs Cisco sont désactivées. Toutefois, pour que le moniteur RPING effectue une demande SNMP SET et commence à lancer une commande ping, il convient d'activer cette demande.

Pour activer la demande, connectez-vous au routeur Cisco et entrez les commandes suivantes :

```
enable
config terminal
snmp-server community communitystring rw
write mem
logout
```

La chaîne communitystring configurée dans le routeur doit correspondre à celle que vous avez saisie dans la zone R/W Community String des éléments de profil RPING créés pour ce routeur. La ligne write mem garantit que les paramètres sont sauvegardés lors de la réinitialisation du routeur.

Activation de demande Ping éloignée sur des routeurs Juniper

Par défaut, les demandes SNMP ping éloignées sur les routeurs Juniper sont désactivées. Pour que le moniteur RPING puisse fonctionner avec le routeur Juniper, vous devez activer les demandes SNMP.

Pour activer la demande SNMP sur le routeur, vérifiez que la section SNMP de la configuration JUNOS correspond à :

```
[edit snmp]
view ping-mib-view {
  oid .1.3.6.1.2.1.80 include; # pingMIB
  oid jnxPingMIB include; # jnxPingMIB
}
community communitystring {
  authorization read-write;
  view ping-mib-view;
}
```

La chaîne communitystring configurée dans le routeur doit correspondre à celle que vous avez saisie dans la zone communitystring des éléments de profil RPING qui sont configurés pour ce routeur.

Propriétés

Les options de propriétés spécifiques du moniteur RPING sont décrites dans le tableau suivant.

Tableau 100. Options des propriétés RPING

Nom de la propriété	Paramètre de la propriété	Description
MibDir	chaîne	Répertoire qui contient les fichiers MIB utilisés par le moniteur. Par défaut : `$ISHOME/mibs`.

Configuration des tests de service du moniteur RPING

Les paramètres de configuration du moniteur RPING permettent de définir des tests de service.

Tableau 101. Configuration du moniteur RPING	
Zone	**Description**
server	Nom ou adresse IP du routeur. Par exemple, `rt1.mycompany.com`.
routertype	Type de routeur : • CISCO • Juniper • RFC2925
host	Nom ou adresse IP du serveur pour lequel vous souhaitez qu'une commande ping soit émise par le routeur.
communitystring	Indique la chaîne de communauté SNMP utilisée pour communiquer avec le routeur. Par exemple, `server1.mycompany.com`.
description	Zone de texte dans laquelle placer des informations descriptives sur l'élément. Par exemple, `RPING monitor`.
vpn	Nom facultatif d'un réseau VPN à utiliser pour l'envoi de commandes ping. Le routeur utilise le réseau VPN spécifié à la place de la route par défaut configurée.
version	Version SNMP à utiliser : 1 - SNMPv1 2 - SNMPv2c 3 - SNMPv3 La valeur par défaut est 2
numberofpings	Nombre de commandes ping à envoyer. La valeur par défaut est 5.
packetsize	Taille des paquets à envoyer, en octets. Par défaut : 64
packettimeout	Durée d'attente, en secondes, entre les commandes ping. Par défaut : 500
securityname†	Nom d'utilisateur pour la session SNMP.
authenticationphrase†	Mot de passe d'authentification pour l'utilisateur.
privacyphrase†	Mot de passe de confidentialité pour l'utilisateur.
authenticationprotocol†	Protocole à utiliser pour authentifier l'utilisateur : • MD5 • SHA1 Par défaut : MD5

Tableau 101. Configuration du moniteur RPING (suite)	
Zone	**Description**
privacyprotocol†	Protocole à utiliser pour chiffrer la session. Par défaut : DES
timeout	Délai, en secondes, entre chaque interrogation. Par défaut : 10
retries	Nombre de nouvelles tentatives effectuées par le moniteur pour contacter le serveur. Par défaut : 3
poll	Durée d'attente, en secondes, entre les commandes ping. Par défaut : 300
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Par défaut : 0
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Par défaut : 10
† s'applique uniquement pour SNMPv3.	

Classification des niveaux de services

Les classifications des niveaux de services définissent les règles de détermination du niveau de service fourni via RPING.

Les options de classification des niveaux de services disponibles pour le moniteur RPING sont :

```
totalTime
lookupTime
numPacketSent
numPacketsRecv
maxRTT
minRTT
averageRTT
respondPercent
message
```

Dans les classifications des niveaux de services :

- Spécifiez d'autres classifications des niveaux de services en entrant manuellement le nom de l'élément de moniteur. Ce nom doit correspondre à celui qui est indiqué pour l'élément dans la section des éléments Moniteurs.
- `message` peut correspondre à n'importe quel message transmis via l'élément **$message** au IBM Application Performance Management utilisé dans un widget. Pour obtenir une liste des valeurs possibles, voir Messages d'état.
- L'opérande est une chaîne ou un nombre positif.

Eléments du moniteur

Outre les résultats de test communs à tous les éléments, le moniteur RPING génère un ensemble de résultats de test contenant les données propres aux tests de service RPING.

Le tableau suivant répertorie les éléments supplémentaires du moniteur RPING.

Tableau 102. Eléments de moniteur RPING	
Elément	**Description**
$authProto	Protocole d'authentification spécifié lors de la création de l'élément.
(AverageRTT)	Durée moyenne de la boucle, en secondes.
$community	Chaîne de communauté SNMP pour le routeur.
$communityString	Chaîne de communauté SNMP utilisée pour communiquer avec le routeur.
(MaxRTT)	Durée maximale de la boucle, en secondes.
(MinRTT)	Durée minimale de la boucle, en secondes.
$numPacketSent	Nombre de paquets envoyés par le moniteur.
$numPings	Nombre de commandes PING envoyées, comme spécifié lors de l'ajout de l'élément RPING.
$packetSize	Taille des paquets à envoyer.
$packetTimeout	Délai d'attente entre les envois de paquets.
$privProto	Protocole de confidentialité spécifié lors de la création de l'élément.
$remoteHost* (RemoteHost)	Nom ou adresse IP du serveur pour lequel vous souhaitez qu'une commande ping soit émise par le routeur.
(RespondPercent)	Pourcentage des demandes ping envoyées ayant reçu une réponse.
$routerMan* (RouterName)	Type de routeur sélectionné lors de l'ajout de l'élément RPING : • CISCO • Juniper • RFC2925
$securityName	Nom d'utilisateur sécurisé spécifié lors de la création de l'élément.
(SnmpVersion)	Version du protocole SNMP utilisée pour envoyer les paquets SNMP (version 1, 2c ou 3).
(SourceRouter)	Nom ou adresse IP du routeur.
$timeout	Délai de réponse du serveur, en secondes. Extrait du fichier de configuration.
$vpn* (Vpn)	Nom du réseau privé virtuel spécifié dans la zone **vpn** de l'élément de profil RPING.

Messages d'état

Le moniteur RPING fournit des messages d'état dans l'attribut **ResultMessage** lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Le tableau ci-dessous décrit les messages d'état RPING.

Tableau 103. Messages d'état du moniteur RPING	
Message	**Description**
`Got Response`	Le moniteur a reçu une réponse du périphérique Cisco.
`Error in packet - exiting thread`	Une erreur est survenue dans un des paquets.
`Timed out while trying initial sets`	Aucune réponse n'a été obtenue du routeur lors de la tentative de création de la zone `rowEntry`.
`Internal Error`	Erreur dans le routeur.
`Host poll did not finish`	Le périphérique réseau n'a pas terminé les commandes PING.
`Response Failed` `Operation Failed`	Le routeur n'est pas parvenu à envoyer de commande PING au périphérique réseau.
`Timed out on Get requests`	Le moniteur a dépassé le délai d'attente lors de la tentative d'obtention des résultats depuis le routeur.

Moniteur RTSP

Le moniteur RTSP (Real Time Streaming Protocol) teste la diffusion des flux vidéo et audio sur les serveurs de flot de données. Il réunit des informations sur les fichiers média et lance la lecture, la pause et l'arrêt d'une session de flot de données.

Le tableau ci-dessous répertorie les fichiers du moniteur RTSP.

Tableau 104. Fichiers du moniteur RTSP	
Fichiers du moniteur	**Nom ou emplacement**
Exécutable du moniteur	`nco_m_rtsp`
Fichier de propriétés	`$ISHOME/etc/props/rtsp.props`
Fichier de règles	`$ISHOME/etc/rules/rtsp.rules`
Fichier journal	`$ISHOME/log/rtsp.log`

Consignes de configuration du moniteur RTSP

Le moniteur RTSP se connecte au serveur de flot de données en mode DESCRIBE ou PLAY. Il télécharge les informations ou les statistiques fournies pour les serveurs RTSP authentiques, tels que Darwin.

Mode DESCRIBE

En mode DESCRIBE, le moniteur RTSP se connecte au serveur de diffusion en flux et demande les informations sur les fichiers audio et vidéo et les flux.

Le serveur renvoie un code d'état où la valeur `200` indique un fichier téléchargeable, et où les autres valeurs indiquent la raison pour laquelle le fichier demandé n'a pas pu être lu.

Cependant, les statistiques liées à la lecture ne sont pas signalées dans ce mode. La fonction de base des serveurs qui prennent en charge RTSP peut être testée.

Mode PLAY

En mode PLAY, le moniteur RTSP se connecte au serveur de diffusion en flux de la même manière qu'en mode DESCRIBE puis lit le fichier en continu pour fournir des statistiques sur les téléchargements demandés.

Propriétés

Les options de propriétés spécifiques du moniteur RTSP sont décrites dans le tableau suivant.

Tableau 105. Options des propriétés du moniteur RTSP

Nom de la propriété	Paramètre de la propriété	Description
StreamingSocket BufferSize	entier	Taille de la mémoire tampon du socket de flux de données, comprise entre 8 et 64 ko. Valeur par défaut : 8

Configuration des tests de service du moniteur RTSP

Les paramètres de configuration du moniteur RTSP permettent de définir des tests de service.

Le tableau ci-dessous répertorie les configurations du moniteur RTSP :

Tableau 106. Configuration du moniteur RTSP

Zone	Description
server	Système cible qui exécute le serveur de diffusion en flux. Par exemple, `rtsp.mymusic.com`.
remotefile	Fichier qui est téléchargé. Par exemple, `singalong.mp3`.
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément. Par exemple, `RTSP monitor`.
port	Port auquel se connecte le moniteur sur le système cible. Par défaut : 554
action	Action effectuée par le serveur sur le flot : • DESCRIBE • PLAY Par défaut : DESCRIBE
duration	Portion du flux, en secondes, exécutée par le serveur. La valeur par défaut est 5.

Tableau 106. Configuration du moniteur RTSP (suite)	
Zone	**Description**
maxbandwidth	Bande passante maximale, n bits par seconde, utilisée pour le flot de données. Par défaut : 1500000
timeout	Durée d'attente d'une réponse du serveur RSTP, en secondes. Par défaut : 10
poll	Délai, en secondes, entre chaque interrogation. Par défaut : 300
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Par défaut : 0
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Par défaut : 10

Classifications de niveau de service

Les classifications des niveaux de services définissent les règles de détermination du niveau de service fourni via RTSP.

Les options de classification des niveaux de services disponibles pour le moniteur RTSP sont :

```
totalTime
lookupTime
connectTime
responseTime
sdpDownloadTime
playbackTime
status
percentPacketsLost
message
```

Dans les classifications des niveaux de services :

- Spécifiez d'autres classifications des niveaux de services en entrant manuellement le nom de l'élément de moniteur. Ce nom doit correspondre à celui qui est indiqué pour l'élément dans la section des éléments Moniteurs.
- `message` peut correspondre à n'importe quel message transmis via l'élément **$message** au IBM Application Performance Management utilisé dans un widget. Pour obtenir une liste des valeurs possibles, voir Messages d'état.
- L'opérande est une chaîne ou un nombre positif.
- Le code d'état 200 indique la réussite. Voir le protocole RTSP pour les autres codes d'état renvoyés par l'opération.

Eléments du moniteur

Outre les résultats de test communs à tous les éléments, le moniteur RTSP génère un ensemble de résultats de test contenant les données propres aux tests de service RTSP.

Le tableau suivant décrit les éléments supplémentaires du moniteur RTSP.

Tableau 107. Eléments du moniteur RTSP	
Elément	**Description**
$action	Action effectuée par le moniteur.
$averageBandwidth	Bande passante totale moyenne, en octets.
$bytesReceived	Nombre total d'octets reçus.
$connectTime* (`ConnectTime`)	Temps mis pour établir une connexion au serveur cible.
$describeStageStatus	Code d'état pour une étape de la conversation RTSP.
`$filename`	Nom du fichier multimédia.
$lookupTime* (`LookupTime`)	Temps mis pour obtenir l'adresse IP du serveur hôte.
$maxBandwidth	Bande passante maximale utilisant l'interface de configuration.
$mediaResponseTime	Durée nécessaire au serveur pour démarrer le flot de données du fichier requis.
$numberOfStreams	Nombre de flots imbriqués dans le média.
$percentPacketsLost	Pourcentage de paquets perdus.
$playbackTime* (`PlaybackTime`)	Durée qui représente la somme de `setupResponseTime` et de `mediaResponseTime`.
$playStageStatus	Code d'état pour une étape de la conversation RTSP.
$port	Port utilisé pour l'accès au serveur du moniteur.
$responseTime* (ResponseTime)	Durée entre l'établissement de la connexion et la réception du premier octet de données.
$sdpDownloadTime* (SdpDownloadTimed)	Durée nécessaire au téléchargement de données concernant le fichier multimédia.
$setupResponseTime	Durée qui représente une partie de `playbackTime`. **Remarque :** L'élément est généré uniquement lorsque le moniteur RTSP fonctionne en mode PLAY.
$setupStageStatus	Code d'état pour une étape de la conversation RTSP.
$status	Code d'état renvoyé par le serveur RTSP.
$streamingTime	Durée nécessaire au serveur pour terminer le flot de données du fichier requis.

Tableau 107. Eléments du moniteur RTSP (suite)	
Elément	**Description**
$streamLength	Longueur du plus long flot du fichier multimédia.
$teardownStageStatus	Code d'état pour une étape de la conversation RTSP.
$totalBandwidthRequired	Bande passante totale, en kilooctets par seconde.
$totalPacketsLost	Nombre total de paquets perdus.
$totalPacketsReceived	Nombre de paquets reçus.

Messages d'état

Le moniteur RTSP fournit des messages d'état dans l'attribut **ResultMessage** lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Tableau 108. Messages d'état du moniteur RTSP	
Message	**Description**
OK	Demande effectuée.
Connection failed	Le moniteur n'a pas pu se connecter au serveur. Pour plus d'informations, consultez le fichier journal.
Connection closed by foreign host	La connexion au serveur RTSP a été interrompue.
Timed out waiting to read/write	Une connexion de données a été établie avec le serveur RTSP, mais un incident est apparu.
Play failed - no streams	Le moniteur a reçu une réponse, mais aucun élément audio ni vidéo n'était disponible pour la lecture.
select() failed on RTSP socket (PLAY stage)	Le socket a été fermé par le serveur distant, ou il a dépassé le délai en attendant une réponse.
RTSP Server response not in expected format	La réponse du serveur était dans un format que le moniteur ne prend pas en charge.
Redirection requested by server not supported by client	La réponse du serveur n'est pas prise en charge par le client.
Server cannot fulfill client request	La demande a échoué et aucune autre information n'est disponible.
Server Error	Un incident est apparu sur le serveur et la requête a échoué. Le code 500 ou supérieur a été renvoyé par le serveur. Pour plus d'informations, voir le protocole RTSP (RFC 2326).

Tableau 108. Messages d'état du moniteur RTSP (suite)	
Message	**Description**
RTSP response header CSeq doesn't match request CSeq	La configuration du serveur RTSP est incorrecte et ce dernier ne fonctionne pas correctement.
Corrupted RTSP server response	
Corrupted session description	
RTSP SETUP response CSeq doesn't match request CSeq	
RTSP SETUP response, incomplete Session string	
RTSP SETUP response, Session ID has changed within the same session	
RTSP SETUP response does not contain server ports to connect to	
RTSP SETUP response does not contain server port pair to connect to	
RTSP PLAY response CSeq doesn't match request CSeq	
RTSP PLAY response, incomplete Session string	
RTSP PLAY response, Session ID has changed within the same session	
RTSP PLAY response, incomplete RTP-Info string	
RTSP PLAY response does not valid RTP seqnum in RTP-Info response	
RTSP PLAY response does not valid RTP time in RTP-Info response	

Moniteur SAA

Service Assurance Agent (SAA) Cisco est un agent de surveillance des performances des produits Cisco pour IOS version 12.2(2) et ultérieure.

Le moniteur SAA utilise la fonction Service Assurance Agent Cisco pour tester les différents délais entre les routeurs Cisco.

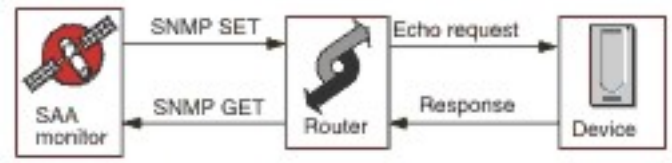
Tableau 109. Récapitulatif du moniteur SAA	
Fichiers du moniteur	**Nom ou emplacement**
Nom de l'exécutable	`nco_m_saa`
Fichier de propriétés	`$ISHOME/etc/props/saa.props`

Tableau 109. Récapitulatif du moniteur SAA (suite)	
Fichiers du moniteur	**Nom ou emplacement**
Fichier de règles	`$ISHOME/etc/rules/saa.rules`
Fichier journal	`$ISHOME/log/saa.log`
Répertoire de scripts	`$ISHOME/scripts/saa/`

Consignes de configuration du moniteur SAA

Le moniteur SAA configure un agent SAA du routeur pour tester la disponibilité d'un autre périphérique réseau ou service en utilisant une demande d'écho temporisée ou des réponses qui sont définies dans la base d'informations de gestion (MIB) du moniteur de temps de réponse Cisco. Il utilise le protocole SNMP (Simple Network Management Protocol) pour communiquer avec Service Assurance Agent.

L'image suivante illustre le fonctionnement du moniteur SAA.



Fonctionnement

Le moniteur SAA configure l'Service Assurance Agent de sorte qu'il exécute des test d'écho, appelés sondes, sur d'autres périphériques réseau. Vous pouvez configurer plusieurs sondes qui utilisent chacune un protocole différent.

Toutes les sondes peuvent fonctionner sur toute cible activée IP, à l'exception de Jitter, qui requiert un autre routeur de canal répondeur Cisco compatible SAA.

Chaque élément de profil du moniteur lance une sonde Service Assurance Agent sur un routeur lors du démarrage et, lors de chaque interrogation, il collecte les informations de résultats et reprogramme la sonde. Si une sonde s'arrête de manière imprévue, le moniteur la redémarre immédiatement. Une fois les tests terminés, la sonde passe à l'état inactif jusqu'à l'interrogation suivante du moniteur. Les données de résultats sont alors collectées et un autre cycle de test commence. Au cours de chaque interrogation, le moniteur vérifie l'état de la sonde. Si cette dernière est encore en cours d'exécution, le moniteur l'arrête puis interroge la base d'informations de gestion (Management Information Base - MIB) pour obtenir les données de résultats et les informations d'erreur du cycle précédent. Il reprogramme ensuite la sonde, réinitialise les données statistiques et réactive la sonde qui s'exécute sans intervention jusqu'à l'interrogation suivante du moniteur.

Pour éviter que des processus incontrôlés restent sur le routeur, le moniteur démarre les sondes avec une durée de vie prédéfinie qui est étendue à chaque interrogation du moniteur. Si le moniteur est arrêté, son exécution continue jusqu'à la fin de son cycle de vie. Il passe alors à l'état inactif jusqu'à ce qu'il atteigne le délai d'expiration fixé et le routeur arrête le processus.

Il n'est pas nécessaire de préconfigurer IOS et Service Assurance Agent car le moniteur effectue automatiquement les opérations de configuration, de contrôle et de nettoyage après l'utilisation des sondes au cours de la phase d'exécution. Ces opérations comprennent la configuration des routeurs de réponse nécessaires à certains types de sonde.

Persistance de sonde

La propriété de moniteur ProbePersist contrôle la persistance de sonde au cours des interrogations du moniteur. Si cette fonction n'est pas activée, les sondes sont lancées à chaque interrogation et se terminent immédiatement après avoir produit les résultats de test.

Charge de routeur

Les opérations de sonde peuvent parfois être affectées par la charge de routeur. La propriété StatusWait fournit des sondes avec la durée autorisée pour le passage d'un état à un autre avant que l'opération soit considérée comme ayant échoué.

Types de sonde

Les types de sonde disponibles avec le moniteur SAA sont les suivants :

- DHCP
- DLSW
- DNS
- FTP
- Requêtes HTTP Get
- ICMP Echo
- ICMP Path Echo
- Jitter
- UDP Echo
- SNA-Echo
- VOIP

Les sondes Echo effectuent des tests basés sur un délai, tandis que les sondes Jitter, VOIP et HTTP les effectuent sur des opérations distinctes.

Propriétés SAA

Vous devez définir les propriétés du moniteur SAA.

Le tableau ci-dessous décrit les propriétés du moniteur SAA.

Tableau 110. Propriétés du moniteur SAA

Nom de la propriété	Paramètre de la propriété	Description
AgeOut	entier	Durée maximale, en secondes, pendant laquelle une sonde est inactive avant de s'arrêter. Par défaut : 600.
MibDir	chaîne	Répertoire utilisé pour les fichiers MIB. Le chemin d'accès par défaut est `$ISHOME/mibs`
ProbeLife	entier	Durée maximale, en secondes, pendant laquelle une sonde est active lorsqu'elle s'exécute sans intervention de l'utilisateur. Par défaut : 600.
ProbePersist	0|1	Les sondes peuvent être exécutées dans deux modes. Elles suivent un seul cycle de test pour chaque interrogation du moniteur ou elles démarrent une première fois et sont reprogrammées à chaque interrogation. • 0 indique un cycle de test unique • 1 indique une reprogrammation à chaque interrogation
StatusWait	entier	Durée, en secondes, pendant laquelle un moniteur attend qu'une sonde termine son exécution avant d'échouer.

Configuration des tests de service du moniteur SAA

Vous devez configurer les paramètres du moniteur SAA pour définir des tests de service.

Le tableau suivant décrit les zones de configuration du moniteur SAA.

Tableau 111. Configuration du moniteur SAA	
Zone	**Description**
server	Nom ou adresse IP du routeur Cisco.
communitystring	Chaîne de communauté SNMP pour le routeur.
probetype	Type de sonde SAA applicable à l'élément de profil.
description	Zone de texte dans laquelle placer des informations descriptives sur l'élément.
Active	Indique si l'élément de profil est actif.
port	Port utilisé pour accéder au routeur. Par défaut : 161.
version	Version SNMP à utiliser : • 1 est utilisé pour SNMPv1 • 2 est utilisé pour SNMPv2c • 3 est utilisé pour SNMPv3 La valeur par défaut est 1.
probeid	Indique une valeur permettant de générer l'index de ligne de contrôle de sonde.
securityname†	Nom d'utilisateur pour la session SNMP.
authenticationphrase†	Mot de passe d'authentification pour l'utilisateur.
privacyphrase†	Mot de passe de confidentialité pour l'utilisateur.
authenticationprotocol†	Les protocoles utilisés pour authentifier les utilisateurs sont les suivants : • MD5 • SHA1 Par défaut : MD5.
privacyprotocol†	Protocole à utiliser pour le chiffrement de la session. Il s'agit du protocole DES.
timeout	Durée d'attente, en secondes, d'une réponse du routeur. Par défaut : 5.
retries	Nombre de nouvelles tentatives du moniteur pour contacter le routeur avant d'abandonner. Par défaut : 0.
poll	Délai, en secondes, entre chaque interrogation. Par défaut : 300
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Par défaut : 0.

Tableau 111. Configuration du moniteur SAA (suite)	
Zone	**Description**
retestinterval	Durée, en secondes, à attendre entre chaque nouvelle tentative de test en cas d'erreur. Par défaut : 10.

Remarque : † s'applique uniquement pour SNMPv3.

Configuration du type de sonde

Chaque type de sonde possède une configuration spécifique et un ensemble de zones de configuration spécifique fourni par Internet Service Monitoring. Pour créer un élément de profil, sélectionnez un type de sonde, puis fournissez la configuration appropriée pour ce dernier. Pour obtenir des informations sur les éléments de configuration individuels, voir le document Cisco Response Time Monitor MIB.

Classification des niveaux des services

La classification des niveaux de services définit les règles permettant de définir le niveau de service fourni par un périphérique réseau.

Les options de classification de niveau de service disponibles pour le moniteur SAA sont les suivantes :

```
totalTime
errTotal
numRTT
minRTT
maxRTT
avgRTT
minPosJitterSD
maxPosJitterSD
minNegJitterSD
maxNegJitterSD
minPosJitterDS
maxPosJitterDS
minNegJitterDS
maxNegJitterDS
packetLossSD
packetLossDS
packetOutOfSequence
packetMIA
packetLateArrival
minDelaySD
maxDelaySD
minDelayDS
maxDelayDS
avgPosJitterSD
avgPosJitterDS
avgNegjitterSD
avgNegJitterDS
avgDelaySD
avgDelayDS
devPosJitterSD
devPosJitterDS
devNegJitterSD
devNegJitterDS
devDelaySD
devDelayDS
MOS
ICPIF
mMinRTT
httpRTT
dnsRTT
tcpConnectRTT
transactionRTT
message
```

Dans les classifications des niveaux de services :

- Spécifiez d'autres classifications des niveaux de services en entrant manuellement le nom de l'élément de moniteur. Ce nom doit correspondre à celui qui est indiqué pour l'élément dans la section des éléments Moniteurs.
- `message` peut correspondre à n'importe quel message transmis via l'élément **$message** au IBM Application Performance Management utilisé dans un widget. Pour obtenir une liste des valeurs possibles, voir «Messages d'état», à la page 414.
- L'opérande est une chaîne ou un nombre positif.

Eléments du moniteur
Outre les résultats de test communs à tous les éléments, le moniteur SAA génère un ensemble de résultats de test qui contient les données propres au type de sonde utilisé.

Sondes DHCP
Les sondes DHCP génèrent plusieurs éléments.

Le tableau ci-dessous décrit les éléments de sonde DHCP.

Tableau 112. Eléments de sonde DHCP	
Elément	**Description**
$authProto	Protocole d'authentification spécifié lors de la création de l'élément.
$community	Communauté utilisée pour envoyer des requêtes SNMP à SAA.
$port	Port utilisé pour se connecter à SAA.
$privProto	Protocole de confidentialité spécifié lors de la création de l'élément.
$probeType	dhcp
$securityName	Nom d'utilisateur sécurisé spécifié lors de la création de l'élément.
$snmpVersion (SnmpVersion)	Version du protocole SNMP utilisée pour envoyer les paquets SNMP (version 1, 2c ou 3).
(SourceRouter)	Nom du routeur utilisé pour envoyer des requêtes DHCP.
$totalRTT † (TotalRTT)	Durée totale de la boucle, en secondes, en vue de l'obtention d'une adresse IP du serveur DHCP.

Remarque : † indique que l'élément est disponible pour les classifications des niveaux de services.

Sondes DLSW
Les sondes DLSW génèrent plusieurs éléments.

Le tableau ci-dessous décrit les éléments de sonde DLSW.

Tableau 113. Eléments de sonde DLSW	
Elément	**Description**
$authProto	Protocole d'authentification spécifié lors de la création de l'élément.
$avgRTT* † (AverageRTT)	Durée moyenne de la boucle, en secondes.
$community	Communauté utilisée pour envoyer des requêtes SNMP à SAA.
$errTotal* † (ErrorTotal)	Nombre total de paquets transmis avec des erreurs.

Tableau 113. Eléments de sonde DLSW (suite)	
Elément	**Description**
$maxRTT* † (MaximumRTT)	Durée la plus élevée de la boucle, en secondes.
$minRTT* † (MinimumRTT)	Durée la plus faible de la boucle, en secondes.
$numRTT†	Nombre d'allers-retours ayant abouti.
$port	Port utilisé pour se connecter à SAA.
$privProto	Protocole de confidentialité spécifié lors de la création de l'élément.
$probeType †	dlsw
$securityName	Nom d'utilisateur sécurisé spécifié lors de la création de l'élément.
$snmpVersion (SnmpVersion)	Version du protocole SNMP utilisée pour envoyer les paquets SNMP (version 1, 2c ou 3).
(SourceRouter)	Routeur utilisé pour exécuter le test SAA.
$sumOfRTT (TotalRTT)	Somme de tous les allers-retours en secondes.
(TargetHost)	Nom ou adresse IP de l'hôte sur lequel le SAA cible est en cours d'exécution.

Remarque : † indique que l'élément est disponible pour les classifications des niveaux de services.

Sondes DNS
Les sondes DNS génèrent plusieurs éléments.

Le tableau ci-dessous décrit les éléments de sonde DNS.

Tableau 114. Eléments de sonde DNS	
Elément	**Description**
$authProto	Protocole d'authentification spécifié lors de la création de l'élément.
$community	Communauté utilisée pour envoyer des requêtes SNMP à SAA.
$dnsHost (Host)	Hôte à résoudre à partir du serveur.
$dnsServer	Adresse IP du serveur DNS.
(HostLookup)	Adresse IP de l'hôte.
$port	Port utilisé pour se connecter à SAA.
$privProto	Protocole de confidentialité spécifié lors de la création de l'élément.
$probeType	dns
$securityName	Nom d'utilisateur sécurisé spécifié lors de la création de l'élément.

Tableau 114. Eléments de sonde DNS (suite)	
Elément	**Description**
$snmpVersion (SnmpVersion)	Version du protocole SNMP utilisée pour envoyer les paquets SNMP (version 1, 2c ou 3).
(SourceRouter)	Nom du routeur utilisé pour envoyer des requêtes DNS.
$totalRTT † (TotalRTT)	Durée totale de la boucle, en secondes, pour la recherche DNS.

Remarque : † indique que l'élément est disponible pour les classifications des niveaux de services.

Sondes FTP
Les sondes FTP génèrent plusieurs éléments.

Le tableau ci-dessous décrit les éléments de sonde FTP.

Tableau 115. Eléments de sonde FTP	
Elément	**Description**
$activePassive	Type de connexion utilisé dans le test, `Active` ou `Passive`. Valeur par défaut : `Passive`
$authProto	Protocole d'authentification spécifié lors de la création de l'élément.
$community	Communauté utilisée pour envoyer des requêtes SNMP à SAA.
$errorStatus	Chaîne de résultat indiquant l'état du test (de l'objet MIB `rttMonLatestRttOperSense`).
$ftpFile	Nom du fichier de test extrait lors du test.
$ftpUrl (FtpUrl)	Adresse URL utilisée pour le test FTP.
$port	Port utilisé pour se connecter à SAA.
$privProto	Protocole de confidentialité spécifié lors de la création de l'élément.
$securityName	Nom d'utilisateur sécurisé spécifié lors de la création de l'élément.
$snmpVersion (SnmpVersion)	Version du protocole SNMP utilisée pour envoyer les paquets SNMP (version 1, 2c ou 3).
(SourceRouter)	Nom du routeur utilisé pour envoyer des requêtes FTP.
$totalRTT (TotalRTT)	Durée d'exécution du test (de l'objet MIB `rttMonLatestRttOperCompletionTime`), en secondes.

Sondes HTTP-Get
Les sondes HTTP-Get génèrent plusieurs éléments.

Le tableau ci-dessous décrit les éléments de sonde HTTP-Get.

Tableau 116. Eléments de sonde HTTP-Get	
Elément	**Description**
$authProto	Protocole d'authentification spécifié lors de la création de l'élément.
$community	Communauté utilisée pour envoyer des requêtes SNMP à SAA.
$dnsRTT † (DnsRTT)	Durée de la boucle, en secondes, pour l'exécution de la requête DNS.
$httpRTT † (HttpRTT)	Durée de la boucle, en secondes, pour l'exécution de l'opération HTTP.
(HttpUrl)	Adresse URL surveillée.
$messageBodyBytes	Taille du corps de message reçu.
$numRTT†	Nombre d'allers-retours ayant abouti.
$port	Port utilisé pour se connecter à SAA.
$privProto	Protocole de confidentialité spécifié lors de la création de l'élément.
$probeType	http-get
$securityName	Nom d'utilisateur sécurisé spécifié lors de la création de l'élément.
(SourceRouter)	Nom du routeur utilisé pour envoyer des requêtes HTTP.
$snmpVersion (SnmpVersion)	Version du protocole SNMP utilisée pour envoyer les paquets SNMP (version 1, 2c ou 3).
$targetHost	Nom de l'hôte pour le service testé.
$tcpConnectRTT † (TcpConnectRTT)	Durée de la boucle, en secondes, pour la connexion au serveur HTTP.
$transactionRTT † (TransactionRTT)	Durée de la boucle, en secondes, pour le téléchargement de l'objet indiqué par l'adresse URL.

Remarque : † indique que l'élément est disponible pour les classifications des niveaux de services.

Sondes ICMP-Echo
Les sondes ICMP-Echo génèrent plusieurs éléments.

Le tableau ci-dessous décrit les éléments de sonde ICMP-Echo.

Tableau 117. Eléments de sonde ICMP-Echo	
Elément	**Description**
$authProto	Protocole d'authentification spécifié lors de la création de l'élément.
$avgRTT † (AverageRTT)	Durée moyenne de la boucle, en secondes.
$community	Communauté utilisée pour envoyer des requêtes SNMP à SAA.
$errBusies	Nombre de commandes ping ayant échoué en raison de l'exécution incomplète d'un ping précédent.

Tableau 117. Eléments de sonde ICMP-Echo (suite)	
Elément	**Description**
$errDisconnects	Nombre de commandes ping ayant échoué pour cause de déconnexions.
$ErrDrops	Nombre de commandes ping ayant échoué en raison de l'indisponibilité d'une ressource interne.
$errNoConnects	Nombre de commandes ping ayant échoué en raison de l'impossibilité d'établir une connexion à la cible.
$errSequences	Nombre de commandes ping ayant échoué en raison de la réception d'un ID séquence imprévu.
$errTimeouts	Nombre de commandes ping ayant échoué en raison d'un dépassement de délai.
$errTotal † (ErrorTotal)	Nombre total de paquets transmis avec des erreurs.
$errVerifies	Nombre de commandes ping ayant échoué car les données reçues n'étaient pas identiques à celles attendues.
$maxRTT † (MaximumRTT)	Durée la plus élevée de la boucle, en secondes.
$minRTT † (MinimumRTT)	Durée la plus faible de la boucle, en secondes.
$numRTT †	Nombre d'allers-retours ayant abouti.
$port	Port utilisé pour se connecter à SAA.
$privProto	Protocole de confidentialité spécifié lors de la création de l'élément.
$probeType	Le type de sonde doit être le suivant : • icmp-echo • icmp-echo-path • udp-echo
$securityName	Nom d'utilisateur sécurisé spécifié lors de la création de l'élément.
$snmpVersion (SnmpVersion)	Version du protocole SNMP utilisée pour envoyer les paquets SNMP (version 1, 2c ou 3).
(SourceRouter)	Nom du routeur utilisé pour envoyer des requêtes ICMP.
$sumOfRTT	Somme de tous les allers-retours en secondes.
$targetHost (Host)	Nom d'hôte du service surveillé.
$tos (Tos)	Type de la valeur de service.

Tableau 117. Eléments de sonde ICMP-Echo (suite)	
Elément	**Description**
$vpn (Vpn)	Nom du réseau privé virtuel.

Remarque : † indique que l'élément est disponible pour les classifications des niveaux de services.

Sondes ICMP-Path-Echo
Les sondes ICMP-Patch-Echo génèrent plusieurs éléments.

Le tableau ci-dessous décrit les éléments de sonde ICMP-Patch-Echo.

Tableau 118. Eléments de sonde ICMP-Path-Echo	
Elément	**Description**
$authProto	Protocole d'authentification spécifié lors de la création de l'élément.
$avgRTT † (AverageRTT)	Durée moyenne de la boucle, en secondes.
$community	Communauté utilisée pour envoyer des requêtes SNMP à SAA.
(HopHost*Un à Huit*)	Du premier au huitième hôte qui visite à l'aide de la sonde ICMP Echo ICMP.
$maxRTT † (MaximumRTT)	Durée la plus élevée de la boucle, en secondes.
$minRTT † (MinimumRTT)	Durée la plus faible de la boucle, en secondes.
$numRTT †	Nombre d'allers-retours ayant abouti.
$port	Port utilisé pour se connecter à SAA.
$privProto	Protocole de confidentialité spécifié lors de la création de l'élément.
$probeType	Le type de sonde est le suivant : • icmp-echo • icmp-echo-path
$securityName	Nom d'utilisateur sécurisé spécifié lors de la création de l'élément.
$snmpVersion (SnmpVersion)	Version du protocole SNMP utilisée pour envoyer les paquets SNMP (version 1, 2c ou 3).
(SourceRouter)	Nom du routeur utilisé pour envoyer des requêtes ICMP.
$sumOfRTT	Somme de tous les allers-retours en secondes.
$targetHost	Nom de l'hôte pour le service testé.
$tos (Tos)	Type de la valeur de service.

Tableau 118. Eléments de sonde ICMP-Path-Echo (suite)	
Elément	**Description**
$vpn (Vpn)	Nom du réseau privé virtuel.

Remarque : † indique que l'élément est disponible pour les classifications des niveaux de services.

Sondes Jitter
Les sondes Jitter génèrent plusieurs éléments.

Le tableau ci-dessous décrit les éléments de sonde Jitter.

Tableau 119. Eléments de sonde Jitter	
Elément	**Description**
$authProto	Protocole d'authentification spécifié lors de la création de l'élément.
$avgDelayDS†	Retard moyen de la destination à la source (en secondes).
$avgDelaySD†	Retard moyen de la source à la destination (en secondes).
$avgNegJitterDS†	Gigue négative moyenne de la destination à la source (en secondes).
$avgNegJitterSD†	Gigue négative moyenne de la source à la destination (en secondes).
$avgPosJitterDS†	Gigue positive moyenne de la destination à la source (en secondes).
$avgPosJitterSD†	Gigue positive moyenne de la source à la destination (en secondes).
$avgRTT † (AverageRTT)	Durée moyenne de la boucle, en secondes.
$community	Communauté utilisée pour envoyer des requêtes SNMP à SAA.
$devDelayDS†	Ecart-type standard du retard de la destination à la source.
$devDelaySD†	Ecart-type standard du retard de la source à la destination.
$devNegJitterDS†	Ecart-type standard de la gigue négative de la destination à la source.
$devNegJitterSD†	Ecart-type standard de la gigue négative de la source à la destination.
$devPosJitterDS†	Ecart-type standard de la gigue positive de la destination à la source.
$devPosJitterSD†	Ecart-type standard de la gigue positive de la source à la destination.
$errDescription	Description de l'erreur.
$errTotal (ErrorTotal)	Nombre total de paquets transmis avec des erreurs.
$maxDelayDS †	Retard maximum de la destination à la source (en secondes).
$maxDelaySD †	Retard maximum de la source à la destination (en secondes).
$maxNegJitterDS †	Gigue négative maximum de la destination à la source (en secondes).
$maxNegJitterSD †	Gigue négative maximum de la source à la destination (en secondes).
$maxPosJitterDS †	Gigue positive maximum de la destination à la source (en secondes).
$maxPosJitterSD †	Gigue positive maximum de la source à la destination (en secondes).

Tableau 119. Eléments de sonde Jitter (suite)	
Elément	**Description**
$maxRTT † (MaximumRTT)	Durée la plus élevée de la boucle, en secondes.
$minDelayDS †	Retard minimum de la destination à la source (en secondes).
$minDelaySD †	Retard minimum de la source à la destination (en secondes).
$minNegJitterDS †	Gigue négative minimum de la destination à la source (en secondes).
$minNegJitterSD †	Gigue négative minimum de la source à la destination (en secondes).
$minPosJitterDS †	Gigue positive minimum de la destination à la source (en secondes).
$minPosJitterSD †	Gigue positive minimum de la source à la destination (en secondes).
$minRTT † (MinimumRTT)	Durée la plus faible de la boucle, en secondes.
$numNegJitterDS	Nombre de gigues négatives de la destination à la source.
$numNegJitterSD	Nombre de gigues négatives de la source à la destination.
$numOW	Nombre d'opérations undirectionnelles pour le retard.
$numPosJitterDS	Nombre de gigues positives de la destination à la source.
$numPosJitterSD	Nombre de gigues positives de la source à la destination.
$numRTT †	Nombre d'allers-retours ayant abouti.
$packetLateArrival †	Nombre de paquets arrivés après le délai d'attente.
$packetLossDS †	Nombre de paquets perdus de la destination à la source.
$packetLossSD †	Nombre de paquets perdus de la source à la destination.
$packetMIA†	Nombre de paquets perdus pour lesquels la direction est inconnue.
$packetOutOfSequence†	Nombre de paquets renvoyés dans le désordre.
$port	Port utilisé pour se connecter à SAA.
$privProto	Protocole de confidentialité spécifié lors de la création de l'élément.
$probeType†	Jitter
(ResponderRouter)	Nom du routeur utilisé pour répondre aux requêtes Jitter.
$securityName	Nom d'utilisateur sécurisé spécifié lors de la création de l'élément.
(SourceRouter)	Nom du routeur utilisé pour envoyer des requêtes Jitter.
$snmpVersion (SnmpVersion)	Version du protocole SNMP utilisée pour envoyer les paquets SNMP (version 1, 2c ou 3).
$sum2DelayDS	Somme des carrés des retards de la destination à la source.
$sum2DelaySD	Somme des carrés des retards de la source à la destination.
$sum2NegJitterDS	Somme des carrés de toutes les gigues négatives.

Tableau 119. Eléments de sonde Jitter (suite)	
Elément	**Description**
$sum2NegJitterSD	Somme des carrés de toutes les gigues négatives.
$sum2PosJitterDS	Somme des carrés de toutes les gigues positives.
$sum2PosJitterSD	Somme des carrés de toutes les gigues positives.
$sum2Rtt†	Somme des carrés de toutes les valeurs d'allers-retours en secondes.
$sumDelayDS	Somme des retards de la destination à la source (en secondes).
$sumDelaySD	Somme des retards de la source à la destination (en secondes).
$sumNegJitterDS	Somme de toutes les gigues négatives (en secondes).
$sumNegJitterSD	Somme de toutes les gigues négatives (en secondes).
$sumPosJitterDS	Somme de toutes les gigues positives (en secondes).
$sumPosJitterSD	Somme de toutes les gigues positives (en secondes).
$sumRTT	Somme de tous les allers-retours en secondes.
$targetHost	Nom de l'hôte pour le service testé.
$tos (Tos)	Type de la valeur de service.
$vpn (\Vpn)	Nom du réseau privé virtuel.

Remarque : † indique que l'élément est disponible pour les classifications des niveaux de services.

Sondes SNA-Echo
Les sondes SNA-Echo (SNA-RU-Echo, SNA-LU0-Echo, SNA-LU2-Echo, SNA-LU62-Echo et SNA-LU62Native-Echo) génèrent les éléments répertoriés dans le tableau ci-dessous.

Le tableau ci-dessous décrit les éléments de sonde JSNA-Echo.

Tableau 120. Eléments de sonde SNA-Echo	
Elément	**Description**
$authProto	Protocole d'authentification spécifié lors de la création de l'élément.
$avgRTT † (AverageRTT)	Durée moyenne de la boucle, en secondes.
$community	Communauté utilisée pour envoyer des requêtes SNMP à SAA.
$errTotal †	Nombre total de paquets transmis avec des erreurs.
$maxRTT † (MaximumRTT)	Durée la plus élevée de la boucle, en secondes.
$minRTT † (MinimumRTT)	Durée la plus faible de la boucle, en secondes.
$numRTT†	Nombre d'allers-retours ayant abouti.

Tableau 120. Eléments de sonde SNA-Echo (suite)	
Elément	**Description**
$port	Port utilisé pour se connecter à SAA.
$privProto	Protocole de confidentialité spécifié lors de la création de l'élément.
$probeType (ProbeType)	sna-*nom*-echo
$securityName	Nom d'utilisateur sécurisé spécifié lors de la création de l'élément.
(SourceRouter)	Nom du routeur utilisé pour envoyer des requêtes SNA.
$snmpVersion (SnmpVersion)	Version du protocole SNMP utilisée pour envoyer les paquets SNMP (version 1, 2c ou 3).
$sumOfRTT (TotalRTT)	Somme de tous les allers-retours en secondes.
(TargetHost)	Hôte cible de la demande d'écho SNA.

Remarque : † indique que l'élément est disponible pour les classifications des niveaux de services.

Sondes UDP-Echo
Les sondes UDP-Echo génèrent les éléments répertoriés dans le tableau suivant.

Le tableau ci-dessous décrit les éléments de sonde UDP-Echo.

Tableau 121. Eléments de sonde UDP-Echo	
Elément	**Description**
$authProto	Protocole d'authentification spécifié lors de la création de l'élément.
$avgRTT † (AverageRTT)	Durée moyenne de la boucle, en secondes.
$community	Communauté utilisée pour envoyer des requêtes SNMP à SAA.
$errBusies	Nombre de commandes ping ayant échoué en raison de l'exécution incomplète d'un ping précédent.
$ErrDrops	Nombre de commandes ping ayant échoué car une ressource interne était indisponible.
$errTimeouts	Nombre de commandes ping ayant échoué pour cause de dépassement de délai.
$errTotal † (ErrorTotal)	Nombre total de paquets transmis avec des erreurs.
$errVerifies	Nombre de commandes ping ayant échoué car les données reçues n'étaient pas identiques à celles attendues.
$maxRTT † (MaximumRTT)	Durée la plus élevée de la boucle, en secondes.

Tableau 121. Eléments de sonde UDP-Echo (suite)	
Elément	**Description**
$minRTT † (MinimumRTT)	Durée la plus faible de la boucle, en secondes.
$numRTT †	Nombre d'allers-retours ayant abouti.
$port	Port utilisé pour se connecter à SAA.
$privProto	Protocole de confidentialité spécifié lors de la création de l'élément.
$probeType	udp-echo
$securityName	Nom d'utilisateur sécurisé spécifié lors de la création de l'élément.
$snmpVersion* (SnmpVersion)	Version du protocole SNMP utilisée pour envoyer les paquets SNMP (version 1, 2c ou 3).
$sumOfRTT	Somme de tous les allers-retours (en secondes).
$targetHost (Host)	Nom d'hôte du service surveillé.
$tos (Tos)	Type de la valeur de service.
$vpn (Vpn)	Nom du réseau privé virtuel.

Remarque : † indique que l'élément est disponible pour les classifications des niveaux de services.

Sondes VOIP
Les sondes VOIP génèrent les mêmes éléments que les sondes Jitter, auxquels s'ajoutent ceux répertoriés dans le tableau ci-dessous.

Le tableau ci-dessous décrit les éléments de sonde VOIP.

Tableau 122. Eléments de sonde VOIP	
Elément	**Description**
$authProto	Protocole d'authentification spécifié lors de la création de l'élément.
$avgRTT † (AverageRTT)	Durée moyenne de la boucle, en secondes.
$community	Communauté utilisée pour envoyer des requêtes SNMP à SAA.
$errTotal † (ErrorTotal)	Nombre total de paquets transmis avec des erreurs.
$ICPIF †	Valeur ICPIF.
$maxRTT † (MaximumRTT)	Durée la plus élevée de la boucle, en secondes.

Tableau 122. Eléments de sonde VOIP (suite)	
Elément	**Description**
$minRTT † (MinimumRTT)	Durée la plus faible de la boucle, en secondes.
$MOS †	Valeur Mean Opinion Score (MOS) du test.
$port	Port utilisé pour se connecter à SAA.
$privProto	Protocole de confidentialité spécifié lors de la création de l'élément.
$probeType †	voip
(ResponderRouter)	Nom du routeur utilisé pour répondre aux requêtes VOIP.
$securityName	Nom d'utilisateur sécurisé spécifié lors de la création de l'élément.
$snmpVersion (SnmpVersion)	Version du protocole SNMP utilisée pour envoyer les paquets SNMP (version 1, 2c ou 3).
(SourceRouter)	Nom du routeur utilisé pour envoyer les requêtes VOIP.
(Tos)	Type de la valeur de service.
(Vpn)	Nom du réseau privé virtuel.

Remarque : † indique que l'élément est disponible pour les classifications des niveaux de services.

Messages d'état
Le moniteur SAA fournit des messages d'état dans l'attribut **ResultMessage** lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Le tableau ci-dessous décrit les messages d'état des moniteurs SAA.

Tableau 123. Messages d'état du moniteur SAA	
Message	**Description**
`Success`	L'opération de sonde a abouti.
`Operation failed`	L'opération de sonde a échoué.
`Invalid status`	L'opération de sonde a échoué avec un état invalide.

Moniteur SIP
Le moniteur SIP vérifie la disponibilité des serveurs SIP (Session Initiation Protocol), notamment la durée nécessaire à l'enregistrement et à l'authentification des noeuds finaux. Il initie une session SIP de manière à pouvoir surveiller les demandes et les réponses SIP.

Le tableau ci-dessous répertorie les fichiers du moniteur SIP.

Tableau 124. Récapitulatif des fichiers du moniteur SIP	
Fichiers du moniteur	**Nom ou emplacement**
Exécutable du moniteur	`nco_m_sip`
Fichier de propriétés	`$ISHOME/etc/props/sip.props`
Fichier de règles	`$ISHOME/etc/rules/sip.rules`
Fichier journal	`$ISHOME/log/sip.log`

Consignes de configuration du moniteur SIP

Le moniteur SIP teste la disponibilité d'un serveur SIP en envoyant une demande à l'URI d'une unité activée SIP, via le serveur SIP et la réception des réponses provenant de l'unité SIP, via le serveur SIP également.

Il agit en tant que client UAC (User Agent Client) et initie les connexions utilisées pour tester les services SIP. Le serveur UAS (User Agent Server), le récepteur ou la cible de l'appel peut être un périphérique SIP, comme un ordinateur qui exécute un logiciel de téléphonie ou une banque de messages.

Lorsqu'il teste un serveur SIP, le moniteur exécute la séquence d'opérations suivante :

1. Enregistrement auprès du serveur SIP à l'aide des données d'identification fournies dans l'élément de profil.
2. Envoi d'une demande OPTIONS au serveur UAS.
3. Envoi d'une demande INVITE au serveur UAS.

   Enregistrement d'un résultat de test ayant abouti si le serveur UAS accepte la demande.
4. Envoi d'une demande BYE au serveur UAS et clôture de la connexion au serveur UAS.
5. Annulation de l'enregistrement auprès du serveur SIP, avec expiration immédiate.

Le moniteur enregistre la durée de chaque opération effectuée au cours du test.

Propriétés

Les options de propriétés spécifiques du moniteur SIP sont décrites dans le tableau ci-dessous.

Tableau 125. Options de propriétés du moniteur SIP

Nom de la propriété	Paramètre de la propriété	Description
ShowZeroes	0|1	Spécifie l'affichage de statistiques SIP avec des valeurs zéro. 0 - désactivé 1 - activé
Transports	chaîne	Répertorie les ports de transport de protocole local, séparés par un espace, c'est-à-dire TCP ou UDP pour le protocole. Les numéros de ports génériques sont autorisés. Par défaut : UDP:*.

Suites de chiffrement

La propriété **SSLCipherSuite** spécifie l'algorithme de cryptographie utilisé par le moniteur SIP. Pour plus d'informations, voir «Paramètre SSL dans Internet Service Monitoring», à la page 447.

Configuration des tests de service du moniteur SIP

Les paramètres de configuration du moniteur SIP permettent de définir des tests de service.

Tableau 126. Configuration du moniteur SIP

Zone	Description
server	Spécifie le nom du serveur à tester. Par exemple, `sip1.mycompany.com`.
port serveur	Port via lequel le moniteur SIP peut atteindre le serveur à tester.

Tableau 126. Configuration du moniteur SIP (suite)	
Zone	**Description**
username	Indique le numéro d'extension ou l'identité de compte du moniteur SIP qui appelle. Par exemple, `jblogg`.
target	Indique le numéro d'extension d'un périphérique SIP utilisé pour effectuer un appel. Par exemple, `5551234`.
password	Spécifie le mot de passe du nom d'utilisateur.
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément. Par exemple, `SIP monitor`.
proxy	Nom d'hôte du serveur proxy. Par exemple, `proxy.mycompany.com`.
port proxy	Port via lequel le moniteur SIP peut atteindre le serveur proxy.
timeout	Délai d'attente, en secondes, d'une réponse du serveur. Par défaut : 30
poll	Délai, en secondes, entre chaque interrogation. Par défaut : 300
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Par défaut : 0
retestinterval	Durée, en secondes, à attendre entre chaque nouvelle tentative de test en cas d'erreur. Par défaut : 10

Classification des niveaux des services

Les classifications des niveaux de services définissent les règles de détermination du niveau de service fourni via SIP.

Les options de classification des niveaux de services disponibles pour le moniteur SIP sont :

```
totalTime
message
```

Dans les classifications des niveaux de services :

- Spécifiez d'autres classifications des niveaux de services en entrant manuellement le nom de l'élément de moniteur. Ce nom doit correspondre à celui qui est indiqué pour l'élément dans la section des éléments Moniteurs.
- `message` peut correspondre à n'importe quel message transmis via l'élément **`$message`** au IBM Application Performance Management utilisé dans un widget. Pour obtenir une liste des valeurs possibles, voir Messages d'état.
- L'opérande est une chaîne ou un nombre positif.

Eléments du moniteur

Outre les résultats de test communs à tous les éléments, le moniteur SIP génère un ensemble de résultats de test contenant les données propres aux tests de service SIP.

Le tableau suivant décrit les éléments supplémentaires du moniteur SIP.

Tableau 127. Eléments du moniteur SIP	
Elément	**Description**
$AcceptReg	Nombre de demandes d'enregistrement SIP acceptées.
$AuthTime* (AuthenticationTime)	Durée nécessaire à l'autorisation du moniteur SIP et du périphérique activé pour SIP.
$authAttempts	Nombre de nouveaux envois d'une requête nécessaires au moniteur pour inclure ses droits d'accès.
(CallSetupTime)	Durée nécessaire pour établir un appel.
$Invalid	Nombre de requêtes envoyées et reçues invalides.
$InvalidReg	Nombre de demandes d'enregistrement SIP invalides.
$lastMethod	Dernière méthode vue par le moniteur, autre que BYE ou ACK.
$lastSequence [METHOD]	Dernière séquence reçue pour une méthode.
$lastStatus [METHOD]	Dernier statut reçu pour une méthode ou au niveau global.
$method *METHOD*	Compte les messages émis pour une méthode.
$optionsTime* (OptionsTime)	Durée nécessaire à la négociation d'une modification d'options (OPTIONS sur 200 OK).
$postDialTime* (PostDialTime)	Durée nécessaire à la réception d'une sonnerie après la numérotation (INVITE sur 180 Ringing).
$RegTime* (RegistrationTime)	Durée nécessaire à l'enregistrement du moniteur SIP et du périphérique activé pour SIP.
$registrationTime	Durée nécessaire à l'enregistrement auprès du serveur (REGISTER sur 200 OK).
$Requests	Nombre de messages de demande SIP reçus et envoyés.
($RequestsSent)	Nombre de messages de demande SIP envoyés.

Tableau 127. Eléments du moniteur SIP (suite)	
Elément	**Description**
`${request|response}[Sent| Received|Transmitted|Total] [METHOD][STATUS]`	Compte des messages vus pour différentes catégories, par exemple, `requestSentINVITE = 1`, `responseReceived = 10` et `responseReceivedBYE200 = 1`.
$Responses	Nombre de messages de réponse SIP reçus et envoyés.
($ResponseReceived)	Nombre de messages de réponse SIP reçus.
$sessionAnswered	• 1 - si l'appel reçoit une réponse • 0 - si l'appel ne reçoit pas de réponse
$sessionCreated	• 1 - si une session est établie • 0 - si une session n'est pas établie
$sessionTerminated	• 1 - si la session se termine • 0 - si la session ne se termine pas.
$shutdownTime* (`ShutdownTime`)	Durée nécessaire pour terminer la connexion (BYE sur 200 OK).
$terminatedReason* (TerminatedReason)	Raison de la fermeture de la connexion.
(Username)	Nom d'utilisateur utilisé pour la connexion au serveur SIP.
(Target)	Cible vers laquelle ouvrir la session.

Messages d'état

Le moniteur SIP fournit des messages d'état dans l'attribut **`ResultMessage`** lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Le tableau ci-dessous décrit les messages d'état du moniteur SIP.

Tableau 128. Messages d'état du moniteur SIP	
Message	**Description**
`Register timed out`	Echec de l'enregistrement du moniteur sur le serveur.
`Invite timed out`	Le message INVITE a dépassé le délai d'attente.
OK	Réussite de la requête et de la réponse.

Tableau 128. Messages d'état du moniteur SIP (suite)	
Message	**Description**
`n operation status description`	• *n* correspond à la séquence de numérotation des messages. • operation est le type du message. • status est le code d'état. • description est une description de l'état en texte brut. Par exemple, `1 INVITE 200 OK`.

Réponses SIP

Le moniteur SIP prend en charge les types de réponse suivants. Chaque séquence possède un compte à 3 chiffres :

- Réponses informatives (100 à 199)
- Réponses réussies (200 à 299)
- Réponse de redirection (300 à 399)
- Réponses d'échecs du client (400 à 499)
- Réponses d'échecs du serveur (500 à 599)
- Réponses d'échecs généraux (600 à 699)

Le tableau ci-dessous répertorie les réponses SIP courantes.

Tableau 129. Réponses SIP courantes	
Response	**Description**
100 Trying (Essai)	Le message est reçu par le périphérique SIP mais n'est pas encore traité.
180 Ringing (Sonnerie)	Le message est reçu et traité par le périphérique SIP. Le périphérique sonne pour avertir l'utilisateur.
200 OK	Ce code est renvoyé en cas de réussite d'une méthode. Par exemple, l'appel est enregistré sur le serveur ou l'utilisateur y a répondu.
401 Unauthorized (Non autorisé)	L'utilisateur n'est pas autorisé.
407 Proxy Authentication Required (Authentification proxy nécessaire)	Ce code est similaire au code 401, mais indique que l'utilisateur doit d'abord s'authentifier.
408 Request Timeout (Délai de demande écoulé)	L'utilisateur n'a pas répondu à l'appel.

Pour une liste complète des réponses SIP, voir RFC3261.

Moniteur SMTP

Le moniteur SMTP fonctionne conjointement avec les moniteurs IMAP4 ou POP3 pour tester les performances d'un service de messagerie.

Le tableau suivant répertorie les fichiers du moniteur SMTP.

Tableau 130. Fichiers du moniteur SMTP	
Fichiers du moniteur	**Nom ou emplacement**
Exécutable du moniteur	`nco_m_smtp`

Tableau 130. Fichiers du moniteur SMTP (suite)	
Fichiers du moniteur	**Nom ou emplacement**
Fichier de propriétés	`$ISHOME/etc/props/smtp.props`
Fichier de règles	`$ISHOME/etc/rules/smtp.rules`
Fichier journal	`$ISHOME/log/smtp.log`

Consignes de surveillance du moniteur SMTP

Le moniteur SMTP fonctionne conjointement avec les moniteurs POP3 ou IMAP4. Il envoie régulièrement un message électronique à une boîte aux lettres sur le serveur cible et enregistre la durée nécessaire à l'émission d'une demande de courrier électronique. Le moniteur POP3 ou IMAP4 lit ensuite les messages dans la boîte aux lettres et les utilise pour calculer le temps de réponse et la disponibilité du service de messagerie électronique.

Remarque : Le moniteur SMTP fonctionne conjointement avec les moniteurs POP3 ou IMAP4. Il envoie régulièrement un message électronique à une boîte aux lettres sur le serveur cible et enregistre la durée nécessaire à l'émission d'une demande de courrier électronique. Le moniteur POP3 ou IMAP4 lit ensuite les messages dans la boîte aux lettres et les utilise pour calculer le temps de réponse et la disponibilité du service de messagerie électronique.

Boîtes aux lettres

Vous pouvez configurer le moniteur afin qu'il envoie des messages électroniques à une boîte aux lettres existante même si la boîte aux lettres appartient à un utilisateur réel. Toutefois, il est recommandé de créer un compte de boîte aux lettres spécial pour le test de services. Le paramètre de messagerie indique la boîte aux lettres du destinataire. Par défaut, le moniteur envoie des messages de test avec la ligne d'objet `SMTP Monitor Test Message`. Le cas échéant, vous pouvez configurer des éléments de profil SMTP avec un nom de boîte aux lettres. Dans cette configuration, le moniteur vérifie tout simplement que le service SMTP accepte les connexions.

Messageries sécurisées

Le moniteur SMTP prend en charge les connexions pour la sécurisation des services de messagerie. La connexion peut être effectuée à l'aide de SSL/TLS ou de la commande STARTTLS. Lors de la définition d'un élément de moniteur SMTP, utilisez la zone Security Type pour sélectionner la sécurité appropriée. Si le serveur de messagerie requiert un certificat côté client pour le chiffrement SSL, utilisez les propriétés SSLname ou les options de ligne de commande pour spécifier un fichier de certificats, un fichier de clés, un mot de passe de clé et une suite de chiffrement.

Certificat côté client

Le moniteur SMTP vous permet de surveiller des serveurs qui requièrent des certificats côté client pour l'authentification mutuelle. Vous spécifiez le fichier de certificats SSL, le fichier de clés et le mot de passe de clé lors de la création d'un élément de profil. Les certificats doivent être au format PEM (Privacy Enhanced Mail). Si ce n'est pas le cas, vous devez convertir votre certificat au format PEM. Il est possible de convertir les certificats à l'aide d'un logiciel comme openSSL, lequel est disponible sur la page Web http://www.openssl.org.

Remarque : Si vous utilisez toujours les mêmes certificat, clé et mot de passe dans tous les éléments de profil, spécifiez-les en utilisant des propriétés de moniteur au lieu de les définir dans chaque élément de profil que vous créez.

Configuration des tests de service du moniteur SMTP

Utilisez les paramètres de configuration du moniteur SMTP pour définir les tests de service. Lorsque vous configurez le moniteur, des valeurs par défaut sont affichées pour les paramètres de délai et d'intervalle d'interrogation. Il s'agit respectivement des valeurs 30 et 300 secondes. D'autres valeurs par défaut répertoriées dans le tableau ne sont pas affichées pendant la configuration mais appliquées au moment de la sauvegarde des détails de la configuration si aucune valeur n'a été indiquée.

Tableau 131. Configuration du moniteur SMTP

Zone	Description
server	Adresse IP du serveur de messagerie. Par exemple : `mail.mycompany.com`
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément.
port	Numéro du port du serveur de messagerie. Valeur par défaut : `25` Si vous utilisez un autre serveur que le serveur SMTP, mettez à jour son port de connexion. Par exemple, si vous utilisez un serveur IMAP4 via SSL for Microsoft Exchange, spécifiez le port `465`.
securitytype	Type de connexion sécurisée ouverte avec le serveur de messagerie : • `NONE` - Connexion sans sécurité • `SSL` - Envoi d'un message `hello` SSLv2, puis négociation SSLv2, SSLv3 ou TLSv1 • `STARTTLS` - Connexion sans sécurité, émission d'une commande `STARTTLS`, puis établissement d'une connexion via TLSv1 Valeur par défaut : `NONE`
username	Nom d'utilisateur utilisé pour se connecter au serveur SMTP. Utilisé avec l'authentification `PLAIN` ou `CRAM-MD5`.
password	Mot de passe utilisé pour se connecter au serveur SMTP. Utilisé avec l'authentification `PLAIN` ou `CRAM-MD5`.
authenticationtype	Méthode d'authentification du moniteur sur le serveur SMTP. Les options disponibles sont les suivantes : • `NONE` - Aucune tentative d'authentification • `PLAIN` - Authentification du nom d'utilisateur et du mot de passe en clair • `CRAM-MD5`- L'authentification CRAM-MD5 est utilisée La valeur par défaut est `NONE`.
sharedsecret	Clé secrète partagée pour l'authentification CRAM-MD5.
email	Adresse électronique de la boîte aux lettres utilisée par les moniteurs SMTP et POP3.
timeout	Délai d'attente, en secondes, d'une réponse du serveur SMTP. Valeur par défaut : `30`
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`

Tableau 131. Configuration du moniteur SMTP (suite)	
Zone	**Description**
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`

Remarque : Surveillez la disponibilité du serveur de messagerie `mail.mycompany.com` en tentant d'y établir une connexion toutes les dix minutes. Utilisez un délai de connexion de trente secondes et si cette tentative n'aboutit pas, faites trois nouvelles tentatives avec cinq secondes entre chaque tentative.

Elément de moniteur

En plus des résultats de test communs à tous les éléments, le moniteur SMTP génère un ensemble de résultats de test contenant des données spécifiques aux tests de service SMTP.

Le tableau suivant décrit les éléments supplémentaires pour le moniteur SMTP.

Tableau 132. Eléments de moniteur SMTP	
Elément	**Description**
`$authentication`	Type de méthode d'authentification utilisateur requis par le serveur SMTP (`Standard` ou `APOP`).
`$bytesPerSec`	Nombre moyen d'octets transférés par seconde.
`$bytesTransferred`	Nombre d'octets transférés ou téléchargés.
`$connectTime*` (`ConnectTime`)	Temps mis pour se connecter au serveur SMTP.
`$email*` (`EmailAddress`)	Adresse électronique de la boîte aux lettres à laquelle le moniteur envoie un courrier électronique de test.
`$lookupTime*` (`LookupTime`)	Temps mis pour obtenir l'adresse IP du serveur hôte.
`$port*` (`Port`)	Port sur lequel le service est surveillé.
`$responseTime*` (`ResponseTime`)	Durée entre la création d'une connexion et l'envoi du premier octet du message test au serveur SMTP.
`$security`	Type de connexion sécurisée ouverte avec le serveur de messagerie (`NONE`, `STARTTLS` ou `SSL`), défini dans la zone **type_sécurité** de l'élément de profil.
`$SSLHandshakeTime*` (`SslHandshakeTime`)	Temps mis pour établir la connexion SSL.
`$status*` (`ResultStatus`)	Code d'état renvoyé par le serveur SMTP.

Tableau 132. Eléments de moniteur SMTP (suite)	
Elément	**Description**
$uploadTime* (UploadTime)	Temps mis pour charger le fichier.
$user* (SmtpUser)	Nom d'utilisateur (nom de compte) utilisé par le moniteur pour la connexion au serveur SMTP.

Message d'état

Le moniteur SMTP fournit des messages d'état dans l'élément $message lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Propriétés

Les propriétés spécifiques du moniteur SMTP sont décrites dans le tableau suivant.

Tableau 133. Propriétés et options de ligne de commande du moniteur SMTP		
Nom de la propriété	**Paramètre de la propriété**	**Description**
MailMessage Path	chaîne	Chemin d'accès à un fichier contenant le texte à envoyer dans le courrier électronique de test. Un message par défaut est envoyé si cette propriété n'est pas définie.
Originator	chaîne	Spécifie la zone From à définir lors de l'envoi d'un courrier électronique de test. Assurez-vous qu'elle corresponde à la chaîne équivalente du moniteur IMAP4. Valeur par défaut : SMTP-Monitor
SSLCertificate File	chaîne	Chemin et nom du fichier de certificats numériques utilisé si aucun certificat n'est explicitement spécifié pour un élément SMTP lors de sa création. Si le chemin n'est pas absolu, il est interprété par le moniteur comme étant relatif au répertoire de travail ($ISHOME/platform/arch/bin).
SSLCipherSuite	chaîne	Suite de chiffrement à utiliser pour les opérations SSL. Pour une description des valeurs possibles, voir Algorithmes de cryptographie. Valeur par défaut : RC4:3DES:DES:+EXP
SSLDisableTLS	entier	Désactive TLSv1 pour la prise en charge des éléments existants. Valeur par défaut : 0 - TLSv1 est activé. 1 TLSv1 est désactivé.
SSLKeyFile	chaîne	Fichier contenant la clé privée SSL.
SSLKeyPassword	chaîne	Mot de passe utilisé pour chiffrer la clé privée SSL.

Tableau 133. Propriétés et options de ligne de commande du moniteur SMTP (suite)		
Nom de la propriété	**Paramètre de la propriété**	**Description**
UseBody	entier	Indique l'endroit où le moniteur écrit les informations de suivi dans le courrier électronique (en-tête ou corps de texte). Par défaut : `0` - les informations sont incluses dans l'en-tête du courrier électronique. 1 - consigne des informations dans le corps du message.

Suites de chiffrement

La propriété `SSLCipherSuite` spécifie l'algorithme de cryptographie utilisé par le moniteur SMTP. Pour plus d'informations sur les paramètres SSL, voir «Paramètre SSL dans Internet Service Monitoring», à la page 447.

Moniteur SNMP

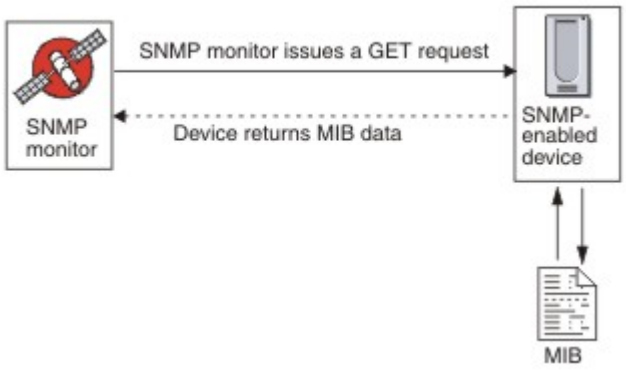
Le moniteur SNMP teste les périphériques SNMP afin d'obtenir des données sur les performances et les erreurs.

Le tableau ci-dessous répertorie les fichiers du moniteur SNMP.

Tableau 134. Récapitulatif du moniteur SNMP	
Fichiers du moniteur	**Nom ou emplacement**
Exécutable du moniteur	`nco_m_snmp`
Fichier de propriétés	`$ISHOME/etc/props/snmp.props`
Fichier de règles	`$ISHOME/etc/rules/snmp.rules`
Fichier journal	`$ISHOME/log/snmp.log`

Consignes de configuration du moniteur SNMP

Le moniteur SNMP acquiert les données des périphériques SNMP en envoyant des requêtes GET SNMP sur un ou plusieurs objets contenus dans la base d'informations de gestion (MIB) d'un périphérique. Ce dernier renvoie ensuite les données MIB au moniteur SNMP, lequel prend en charge SNMP versions 1, 2c et 3.



Propriétés

Les options de propriétés spécifiques du moniteur SNMP sont décrites dans le tableau suivant.

Tableau 135. Options des propriétés du moniteur SNMP		
Nom de la propriété	**Paramètre de la propriété**	**Description**
Valeur InvalidBps	entier	Spécifie une valeur d'entier qui remplace les calculs de valeur en bits par seconde (Bps) lorsqu'un seul point de données est disponible.
MibDir	chaîne	Répertoire qui contient les documents MIB utilisés par le moniteur. Par défaut : `$ISHOME/mibs`.
StripQuotes	`0|1`	Supprime les guillemets des données d'entier. `0` - désactivé `1` - activé
Rollover Threshold	entier	La valeur qu'un delta doit atteindre ou excéder si une remise à zéro se produit avant qu'un routeur soit réinitialisé. Par défaut : `0` (ne jamais remettre à zéro)

Configuration des tests de service du moniteur SNMP

Les paramètres de configuration du moniteur SNMP permettent de définir des tests de service.

Tableau 136. Configuration du moniteur SNMP	
Zone	**Description**
server	Serveur auquel envoyer les requêtes SNMP GET.
nom objet groupe	Nom au format texte du groupe d'ID objet à inclure dans la requête GET.
nom communauté	Chaîne de communauté d'écriture/lecture SNMP pour le serveur SNMP sur le client. **Remarque :** Pour insérer un accent circonflexe (^) dans les noms de communauté, il faut respecter certaines règles ; pour plus d'informations, voir Noms de communauté.
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément.
port	Port du serveur à utiliser. Par défaut : 161
version	Version SNMP à utiliser : 1 - SNMPv1 2 - SNMPv2c 3 - SNMPv3 Valeur par défaut : 1
securityname†	Nom d'utilisateur pour la session SNMP.

Tableau 136. Configuration du moniteur SNMP (suite)	
Zone	**Description**
authenticationphrase†	Mot de passe d'authentification pour l'utilisateur.
privacyphrase†	Mot de passe de confidentialité pour l'utilisateur.
authenticationprotocol†	Protocole à utiliser pour authentifier l'utilisateur : • MD5 • SHA1 Par défaut : MD5
privacyprotocol†	Protocole à utiliser pour le chiffrement de la session. Par défaut : DES
timeout	Délai d'attente, en secondes, d'une réponse du serveur. Par défaut : 20
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : 300
retries	Nombre de nouvelles tentatives du moniteur pour contacter le serveur avant d'abandonner. Par défaut : 0
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Par défaut : 0
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Par défaut : 10
hostnamelookuppreference	Détermine la version IP (IPv6 ou IPv4) qui est appliquée au nom d'hôte fourni. Les options sont les suivantes : • default définit le moniteur pour utiliser les paramètres des propriétés du moniteur. Il s'agit de la valeur par défaut. • 4Then6 sélectionne IPv4, puis IPv6. Utilise les adresses IPv4 si elles sont disponibles. Si aucune adresse IPv4 n'est trouvée, les adresses IPv6 sont utilisées. • 6Then4 sélectionne IPv6, puis IPv4. Utilise les adresses IPv6 si elles sont disponibles. Si aucune adresse IPv6 n'est trouvée, les adresses IPv4 sont utilisées. • 4Only sélectionne IPv4 uniquement. Utilise les adresses IPv4 uniquement. S'il n'existe aucune adresse IPv4, l'interrogation renvoie une erreur. • 6Only sélectionne IPv6 uniquement. Utilise les adresses IPv6 uniquement. S'il n'existe aucune adresse IPv6, l'interrogation renvoie une erreur. • 6or4 sélectionne IPv4 ou IPv6. Utilise la première adresse renvoyée à partir du nom d'hôte.

Tableau 136. Configuration du moniteur SNMP (suite)	
Zone	**Description**
† s'applique uniquement pour SNMPv3.	

Noms de communauté

Internet Service Monitoring utilise le caractère accent circonflexe (^) comme caractère d'échappement lors de l'envoi d'informations au périphérique cible. Si un nom de communauté contient un accent circonflexe, vous devez en saisir deux (^^) pour que le nom soit correct au niveau du routeur. Par exemple, pour que le nom de communauté a$^&b soit correct lorsqu'il est envoyé au périphérique, utilisez a$^^&b.

Classifications des niveaux de services

Les classifications des niveaux de services définissent les règles de détermination du niveau de service.

Les options de classification des niveaux de services disponibles pour le moniteur SNMP sont :

```
totalTime
message
```

Dans les classifications des niveaux de services.

- Spécifiez d'autres classifications des niveaux de services en entrant manuellement le nom de l'élément de moniteur. Ce nom doit correspondre à celui qui est indiqué pour l'élément dans la section des éléments Moniteurs.
- `message` peut correspondre à n'importe quel message transmis via l'élément **$message** au IBM Application Performance Management utilisé dans un widget. Pour obtenir une liste des valeurs possibles, voir Messages d'état.
- L'opérande est une chaîne ou un nombre positif.
- oidName est le nom affecté à un objet MIB dans la zone OID Name définie dans le groupe d'ID objet.

Eléments du moniteur

Outre les résultats de test communs à tous les éléments, le moniteur SNMP génère un ensemble de résultats de test contenant les données propres aux tests de service SNMP.

Le tableau suivant décrit les éléments supplémentaires du moniteur SNMP.

Tableau 137. Eléments de moniteur SNMP	
Elément	**Description**
$community	Chaîne de communauté SNMP pour le serveur SNMP sur le client.
$numOids	Nombre d'ID objet utilisés dans la requête.
$oidGroupName* (OidGroup)	Nom du groupe d'ID objet. Le groupe d'ID objet contient les ID objet interrogés par le moniteur.
$oidName*0 à n** (OIDName*Zéro à Neuf*)	Noms du premier au dernier objet MIB dans le groupe d'ID objet. Ils sont indiqués par un numéro lors de l'utilisation de Netcool/OMNIbus et par un texte alphabétique (zéro à neuf) lors de l'utilisation d'IBM Application Performance Management.
$oidNames	Noms de chaque ID objet séparés par une barre verticale (|).

Tableau 137. Eléments de moniteur SNMP (suite)	
Elément	**Description**
$oidReturnValues*0 à n** ($snmpResult*Zéro à Neuf*)	Données renvoyées par la commande SNMP GET pour le premier au dernier objet MIB dans le groupe d'ID objet. Elles sont indiquées par un numéro lors de l'utilisation de Netcool/OMNIbus et par un texte alphabétique (zéro à neuf) lors de l'utilisation d'IBM Application Performance Management.
$oidUnit*0 à n*	Unités du premier au dernier objet MIB dans le groupe d'ID objet, indiquées par un numéro.
$oidUnits	Unités pour chaque ID objet, séparées par une barre verticale (|).
$port	Port sur lequel le service est surveillé.
$snmpVersion* (SnmpVersion)	Version de SNMP utilisée pour envoyer des paquets SNMP configurés dans le profil (version 1, 2c ou 3).

Message d'état

Le moniteur SNMP fournit des messages d'état dans l'attribut `ResultMessage` lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Le tableau ci-dessous décrit les messages d'état du moniteur SNMP.

Tableau 138. Messages d'état du moniteur SNMP	
Message	**Description**
`Successful Get`	La requête de l'agent SNMP a abouti.
`Failed to open snmp sessions` `SNMP session - start failed`	Initialisation de la session SNMP impossible.
`Error in packet`	Impossible de créer un paquet SNMP valide.
`Timed out while waiting for response`	Aucune réponse reçue de l'agent SNMP.
`Internal Error`	Une erreur interne s'est produite dans le moniteur. Pour plus d'informations, contactez le support technique d'IBM.
`Error Processing OID`	Une erreur est survenue lors du traitement de l'un des `ID objet`.
`ERROR: Too Many OIDs`	En raison de sa configuration, le moniteur demande un trop grand nombre d'`ID objet` à la fois. Le nombre maximal est de `100`.
`ERROR: PDU received mismatch with PDU sent`	L'unité de données de protocole (PDU) reçue par le moniteur ne correspond pas à celle qui a été envoyée par le serveur.

Moniteur SOAP

Le moniteur SOAP vérifie la disponibilité et le temps de réponse de l'interface SOAP (SOAP 1.0 et 1.1). Il peut également surveiller la validité des entrées SOAP (demandes) et des sorties SOAP (réponses).

Le moniteur SOAP prend en charge les styles de codage de message suivants :

- RPC - codé
- Document - littéral non encapsulé
- Document - littéral encapsulé

Le tableau ci-dessous répertorie les fichiers du moniteur SOAP.

Tableau 139. Récapitulatif des fichiers du moniteur SOAP

Fichiers du moniteur	**Nom ou emplacement**
Exécutable du moniteur	`nco_m_soap`
Fichier de propriétés	`$ISHOME/etc/props/soap.props`
Fichier de règles	`$ISHOME/etc/rules/soap.rules`
Fichier journal	`$ISHOME/log/soap.log`

Consignes de configuration du moniteur SOAP

Le moniteur SOAP teste le fonctionnement d'un service SOAP en envoyant à l'interface SOAP cible une demande contenant un ensemble d'entrées et en recevant et analysant ensuite les sorties contenues dans la réponse reçue de l'interface. Lorsqu'une demande est envoyée à l'interface SOAP, elle peut aboutir ou échouer. Une demande aboutit si une réponse est reçue et que les valeurs du message de réponse correspondent aux valeurs de sortie spécifiées. Elle échoue si aucune réponse n'est reçue ou si une réponse est reçue mais que les valeurs du message ne correspondent pas aux valeurs de sortie.

Les entrées et sorties SOAP contenues dans les demandes et les réponses dépendent des fonctions du service SOAP testé. Lorsque vous concevez un test pour un service SOAP, vous devez donc spécifier les entrées et sorties adaptées à celui-ci. Les entrées se composent des noms des données à envoyer et leurs valeurs d'entrée attribuées. Les sorties se composent des noms des données à recevoir et leurs valeurs de sortie attendues. Ces noms de données proviennent d'un fichier WSDL (Web Service Description Language) local que vous spécifiez lors de la configuration du moniteur SOAP. Les noms de données d'entrée et de sortie doivent correspondre aux noms et aux types de données dans le fichier WSDL. Les noms de données doivent également être dans le même ordre que dans le fichier WSDL. Si les noms ne correspondent pas ou si l'ordre est incorrect, un message d'erreur est généré lorsque le moniteur tente d'interroger l'interface SOAP.

Le format de l'entrée est :

```
nomdonnées:typedonnées=valeur_attribuée, nomdonnées:typedonnées=valeur_attribuée, ...
```

Le format des sorties est :

```
nomdonnées:typedonnées=valeur_attendue, nomdonnées:typedonnées=valeur_attendue, ...
```

Types de données SOAP

Le moniteur SOAP prend en charge les types de données simples, de tableau et définis par l'utilisateur. Les types de données simples sont entier, chaîne et booléen. Les tableaux peuvent contenir des types de données simples et d'autres données de type tableau définies par l'utilisateur.

Tableau 140. Types de données simples			
Types de données simples			
anyURI	float	language	Qname
boolean	gDay	long	short
byte	gMonth	Name	chaîne
date	gMonthDay	NCName	time
dateTime	gYear	negativeInteger	token
decimal	gYearMonth	NMTOKEN	unsignedByte
double	ID	NMTOKENS	unsignedInt
duration	IDREFS	nonNegativeInteger	unsignedLong
ENTITIES	int	nonPostiveInteger	unsignedShort
ENTITY	integer	normalizedString	

Authentification SOAP

Si l'interface SOAP à surveiller requiert une authentification HTTP de base, spécifiez les données d'identification permettant d'accéder à l'interface dans l'élément de profil SOAP par le biais de l'outil de configuration d'Internet Service Monitoring.

Pour définir les paramètres d'authentification SOAP requis :

1. Dans l'outil de configuration d'Internet Service Monitoring, sélectionnez l'élément de profil auquel vous voulez ajouter les informations d'authentification.
2. Dans l'onglet **Avancé**, cliquez sur la zone **Valeur** du paramètre `username` et entrez la valeur requise.
3. Cliquez sur la zone **Valeur** du paramètre `password` et entrez la valeur requise. Le mot de passe est chiffré.
4. Cliquez sur **OK**.

Si l'authentification n'est plus requise, supprimez les valeurs des paramètres **`username`** et **`password`**.

Propriétés

Les options de propriétés spécifiques du moniteur SOAP sont décrites dans le tableau ci-dessous.

Tableau 141. Options de propriétés du moniteur SOAP			
Nom de la propriété	**Paramètre de la propriété**	**Description**	**Valeur par défaut**
SoapParser	chaîne	Bibliothèque d'analyse XML.	`$ISHOME/platform/$ARCH/bin/AxisXMLParserXerces.dll`
SoapTransport	chaîne	Bibliothèque de transport SOAP.	`$ISHOME/platform/$ARCH/bin/HTTPTransport.dll`

Tableau 141. Options de propriétés du moniteur SOAP (suite)			
Nom de la propriété	**Paramètre de la propriété**	**Description**	**Valeur par défaut**
SoapChannel	chaîne	Bibliothèque de canal SOAP	`$ISHOME/platform/$ARCH/bin/HTTPChannel.dll`
SoapSecureChannel	chaîne	Bibliothèque de canal sécurisé SOAP.	`$ISHOME/platform/$ARCH/bin/HTTPSSLChannel.dll`
SoapClientLog	chaîne	Nom du fichier journal du client SOAP.	`$ISHOME/log/SoapClient.log`

Suites de chiffrement

La propriété `SSLCipherSuite` spécifie l'algorithme de cryptographie utilisé par le moniteur SOAP.

Pour plus d'informations, voir «Paramètre SSL dans Internet Service Monitoring», à la page 447.

Configuration des tests de service du moniteur SOAP

Les paramètres de configuration du moniteur SOAP permettent de définir des tests de service.

Tableau 142. Configuration du moniteur SOAP	
Elément	**Description**
wsdl	Chemin d'accès d'une copie locale du fichier WSDL.
operation	Nom de l'opération SOAP.
operationnamespace	Espace de nom de l'opération SOAP.
location	URL du service SOAP à surveiller.
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément.
timeout	Durée d'attente, en secondes, d'une réponse du service SOAP. Valeur par défaut : `10`
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`
Paramètres Soap	

Tableau 142. Configuration du moniteur SOAP (suite)	
Elément	**Description**

inputs	Permet d'accéder aux zones de nom, de type et de valeur, y compris les attributs, des entrées SOAP. Utilisez des paramètres SOAP simple, complexe ou de tableau. Exemple :
	• Simple : `symbol:string="IBM"`
	• Complexe :
	`outer:{item1:string,item2:string}(aaa:string='bbb')`
	`={item1(attr:string='ccc')='',`
	`item2(attr:string='ddd',attr2:string='eee')='fff'}`
	Dans cet exemple, les attributs entre parenthèses, en gras, sont facultatifs.
	• Tableau : `input:int[]=[1,2,3,4]`

outputs	Permet d'accéder aux zones de nom, de type et de valeur, y compris les attributs, des sorties SOAP. Utilisez des paramètres SOAP simple, complexe ou de tableau. Pour plus d'informations sur la syntaxe, voir les exemples de sorties des paramètres SOAP.

Classification des niveaux des services

Les classifications des niveaux de services définissent les règles de détermination du niveau de service fourni par l'interface SOAP.

Les options de classification des niveaux de services disponibles pour le moniteur SOAP sont :

```
totalTime
message
```

Dans les classifications des niveaux de services :

- Spécifiez d'autres classifications des niveaux de services en entrant manuellement le nom de l'élément de moniteur. Ce nom doit correspondre à celui qui est indiqué pour l'élément dans la section des éléments Moniteurs.
- `message` peut correspondre à n'importe quel message transmis via l'élément **$message** au IBM Application Performance Management utilisé dans un widget. Pour obtenir une liste des valeurs possibles, voir Messages d'état.

Eléments du moniteur

Outre les résultats de test communs à tous les éléments, le moniteur SOAP génère un ensemble de résultats de test contenant les données propres aux tests de service SOAP.

Le tableau suivant répertorie les éléments supplémentaires du moniteur SOAP.

Tableau 143. Eléments de moniteur SOAP	
Elément	**Description**
(Location)	URL du service SOAP surveillé.
(Operation)	Nom du service SOAP surveillé.
$outputMatch	`Success` si la valeur renvoyée correspond à la valeur de sortie, sinon `Failure`.
$responseValueName	Nom de la valeur reçue dans la réponse SOAP.

Tableau 143. Eléments de moniteur SOAP (suite)	
Elément	**Description**
$soapname	Nom du conteneur dans la réponse SOAP. S'applique uniquement aux types de données complexes définis par l'utilisateur.
$soaptype	Type du conteneur dans la réponse SOAP. S'applique uniquement aux types de données complexes définis par l'utilisateur.
(WSDL)	Chemin d'accès d'une copie locale du fichier WSDL.

Messages d'état

Le moniteur SOAP fournit des messages d'état dans l'attribut **ResultMessage** lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Les messages sont soit `Success` si les valeurs renvoyées correspondent aux valeurs de sortie, soit un message d'erreur. Le message d'erreur contient une description de l'erreur.

Exemple

Surveillance de la disponibilité de l'interface SOAP à des intervalles de 5 minutes. Si cette interface est indisponible, répétez le test au moins deux fois, en respectant un délai de 5 secondes entre chaque essai. Envoyez une demande qui ajoute 1 + 2 et vérifiez que la réponse contient la valeur 3.

Créez un élément de profil SOAP et définissez les zones présentées dans le tableau suivant.

Tableau 144. Exemple d'élément de profil SOAP	
Zone de configuration	**Valeur**
wsdl	`c:\%ISMHOME%\etc\SOAP.wsdl`
operation	add
operationnamespace	`http://localhost/SOAP/Calculator`
location	`http://serverA/SOAP/Calculator`
description	Moniteur SOAP du calculateur de base
Rapports actifs	Sélectionné
timeout	30
poll	300
failureretests	2
retestinterval	5
inputs	[in0=1,in1=2]
outputs	[addReturn=3]

Moniteur TCPPort

Le moniteur TCPPort fournit une couverture des services non testés par les autres moniteurs. Il détecte les commandes ou les chaînes d'un port TCP et y répond. Ce moniteur est particulièrement utile pour surveiller les services indiqués.

Le tableau suivant répertorie les fichiers du moniteur TCPPort.

Tableau 145. Fichiers du moniteur TCPPort

Fichiers du moniteur	**Nom ou emplacement**
Exécutable du moniteur	`nco_m_tcpport`
Fichier de propriétés	`$ISHOME/etc/props/tcpport.props`
Fichier de règles	`$ISHOME/etc/rules/tcpport.rules`
Fichier journal	`$ISHOME/log/tcpport.log`

Consignes de configuration du moniteur TCPPort

Le moniteur TCPPort teste les services de type TCP en établissant une connexion au service, en surveillant les messages reçus du service et en lui envoyant des réponses.

Pour configurer un test, définissez une séquence de messages et de réponses attendus qui se compose d'une interaction normale sur ce service.

Par exemple, une interaction standard d'un service telnet implique la séquence suivante :

- Le service telnet envoie un message de connexion, vous invitant à entrer un nom d'utilisateur.
- Le client envoie une réponse contenant un nom d'utilisateur.
- Le service telnet envoie un message, vous invitant à entrer un mot de passe.
- Le client envoie une réponse contenant un mot de passe.
- Si la tentative de connexion aboutit, le service telnet envoie un message de bienvenue.

Les propriétés **`WaitForn`** et **`Sendn`** spécifiées du moniteur définissent les messages attendus et les réponses à ceux-ci. Ces propriétés indiquées dans le fichier de propriétés du moniteur, définissent le mode d'interaction du moniteur avec le service TCP :

- Les propriétés **`WaitForn`** sont des expressions régulières. Le moniteur les utilise pour la correspondance des messages reçus sur le port surveillé.
- Les propriétés **`Sendn`** sont des chaînes littérales que le moniteur écrit sur le port.

Remarque : Si nécessaire, vous pouvez insérer des caractères de contrôle dans ces propriétés à l'aide d'un éditeur de texte qui l'autorise.

Le format permettant de définir les propriétés `WaitForn` et `Sendn` est :

```
WaitFor1: 1er_message_reçu
Send1: 1ère_réponse
WaitFor2: 2ème_message_reçu
Send2: 2ème_réponse
...
WaitFor5: 5ème_message_reçu
Send5: 5ème_réponse
```

Lorsque le moniteur atteint la première propriété **`WaitFor`** non définie, il arrête les opérations d'envoi et de réception. Si la propriété **`MonitorDisconnect`** a la valeur 0, le service surveillé doit fermer la connexion ouverte par le moniteur. Sinon, le moniteur inclut un message indiquant que le délai a expiré lors de l'attente de la lecture (`Timed out waiting to read`) dans son élément **`$message`**. Avec un grand nombre de services, vous pouvez fermer la connexion en envoyant une commande `quit`. Si **`MonitorDisconnect`** a la valeur 1, le moniteur se déconnecte à la fin de la dernière commande `Send` ou `WaitFor` ou une fois que le délai est atteint.

Configuration du test de service du moniteur TCPPort

Utilisez les paramètres de configuration du moniteur TCPPort pour définir les tests de service.

Tableau 146. Configuration de TCPPort

Zone	Description
serveur	Adresse IP du système sur lequel le service cible est en cours d'exécution. Par exemple, `server.mycompany.com`
port	Port sur lequel se connecter au service cible.
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément.
délai d'attente	Délai d'attente, en secondes, avant une réponse du serveur. Valeur par défaut : `30`
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : `300`
failureretests	Nombre de nouvelles tentatives de test avant d'indiquer un échec. Valeur par défaut : `0`
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : `10`

Remarque : Surveillez la disponibilité du service `telnet` qui s'exécute sur l'hôte `server.mycompany.com` sur le port 23. Utilisez les données d'identification `user` ou `guest` pour vous connecter au serveur et fermez la connexion immédiatement après la connexion établie. Exécutez le test toutes les 5 minutes et définissez un délai d'attente de 10 secondes pour les tentatives de connexion.

1. Ajoutez les entrées suivantes dans le fichier de propriétés TCPPort :

```
WaitFor1: ".*[Ll]ogin:"
Send1: "user"
WaitFor2: ".*[Pp]assword:"
Send2: "guest"
WaitFor3: ".*%"
Send3: "exit"
```

2. Démarrez ou redémarrez le moniteur TCPPort.

Correspondances d'expressions régulières

Vous pouvez effectuer une recherche d'expression régulière sur les informations téléchargées en entrant jusqu'à 50 expressions régulières différentes. Le moniteur TCPPort tente de faire correspondre les contenus extraits à chaque expression régulière. Si une correspondance à une expression régulière indiquée est trouvée, les lignes correspondantes (ou le nombre maximal de lignes correspondantes pouvant être stockées dans la mémoire tampon interne du moniteur) sont renvoyées dans l'élément `$regexpMatchn` correspondant. Si l'expression régulière a plusieurs correspondances dans les informations téléchargées, seule la première correspondance est renvoyée. L'état de chaque test d'expression régulière est indiqué par les éléments `$regexpStatusn`. Vous pouvez utiliser les correspondances d'expression régulière et les informations d'état en tant que critères pour les classifications de niveau de service.

Pour plus d'informations, voir Tableau 50, à la page 335.

Eléments du moniteur

Le tableau suivant décrit les éléments supplémentaires du moniteur TCPPort.

Les éléments indiqués par un astérisque (*) sont disponibles en tant qu'attributs. Le nom des attributs est affiché entre parenthèses. L'absence d'astérisque indique qu'il n'existe aucun attribut équivalent. Les attributs entre parenthèses mais sans élément sont disponibles uniquement en tant qu'attributs ; il n'existe aucun élément équivalent.

Outre les résultats de test communs à tous les éléments, le moniteur TCPPort génère un ensemble de résultats de test contenant les données propres aux tests de service TCPPort.

Tableau 147. Eléments du moniteur TCPPort

Elément	Description
`$bytesPerSec`	Nombre moyen d'octets transférés par seconde.
`$bytesTransferred`	Nombre d'octets transférés ou téléchargés.
`$connectTime*(ConnectTime)`	Temps mis pour établir une connexion au serveur cible.
`$downloadTime*(DownloadTime)`	Temps mis pour télécharger des données.
`$lastlineThere's`	Contenus de la dernière ligne reçue du serveur cible.
`$lookupTime*(LookupTime)`	Temps mis pour obtenir l'adresse IP du serveur hôte.
`$networkError`	Contient toutes les erreurs réseau survenues pendant la connexion.
`$port*` `(Port)`	Port du serveur cible auquel le moniteur a tenté de se connecter.
`$waitingFor`	Si la connexion est arrêtée avant que le moniteur n'ait terminé sa séquence d'attentes et d'envois, cet élément renferme les contenus de la dernière propriété `WaitFor`.

Message d'état

Le moniteur TCPPort fournit des messages d'état dans l'attribut `ResultMessage` lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Le tableau suivant décrit les messages d'état TCPPort.

Tableau 148. Messages d'état du moniteur TCPPort

Message	Description
`OK`	Demande effectuée.
`Timed out waiting to read/write`	Une connexion de données a été établie avec le serveur, mais ce dernier ne répond pas.
`Connection closed unexpectedly`	La connexion au serveur a été interrompue.
`Connection failed`	Le moniteur n'a pas pu se connecter au serveur. Pour plus d'informations, consultez le fichier journal.
`Network connect error`	Un incident a été détecté sur le réseau.
`Network error whilst reading`	

Propriétés

Les propriétés spécifiques au moniteur TCPPort sont décrites dans le tableau suivant.

Tableau 149. Propriétés du moniteur TCPPort

Nom de la propriété	Paramètre de la propriété	Description
`Monitor Disconnect`	`0`|`1`	Indique que le moniteur doit se déconnecter après la dernière commande `Send` ou `WaitFor`. Si la dernière commande est `Send`, le moniteur se déconnecte immédiatement après l'envoi de la chaîne. Si la dernière commande est `WaitFor`, le moniteur se déconnecte dès qu'il reçoit une correspondance ou lorsque le délai d'attente de l'interrogation est dépassé. `0` - désactivé (le moniteur ne se connecte pas) `1` - activé
`OutputDirectory`	chaîne	Indique le répertoire de sortie à utiliser si `OutputResult` est sauvegardé. Valeur par défaut : `$ISHOME/var`.
`OutputResult`	`0`|`1`	Indique que le moniteur doit sauvegarder les données reçues du service. `0` - désactivé `1` - activé
`Send`	*n*	Chaîne littérale que le moniteur écrit sur le port. Voir Consignes de configuration du moniteur TCPPort. n est une valeur numérique comprise entre 1 et 30 (inclus).
`singleLineMatch`	`0`|`1`	Indique que le moniteur renvoie une seule correspondance de ligne en cas de correspondance à une expression régulière. `0` - désactivé (plusieurs lignes sont recherchées) `1` - activé (une seule ligne est recherchée)
`WaitFor`	*n*	Expression régulière utilisée pour faire correspondre les commandes ou chaînes sur le port surveillé. Pour plus d'informations, voir Consignes de configuration du moniteur TCPPort. n est une valeur numérique comprise entre 1 et 30 (incluse).

Suites de chiffrement

La propriété `SSLCipherSuite` spécifie la suite de chiffrement utilisée par le moniteur TCPPORT. Pour plus d'informations sur les paramètres SSL, voir «Paramètre SSL dans Internet Service Monitoring», à la page 447.

Moniteur TFTP

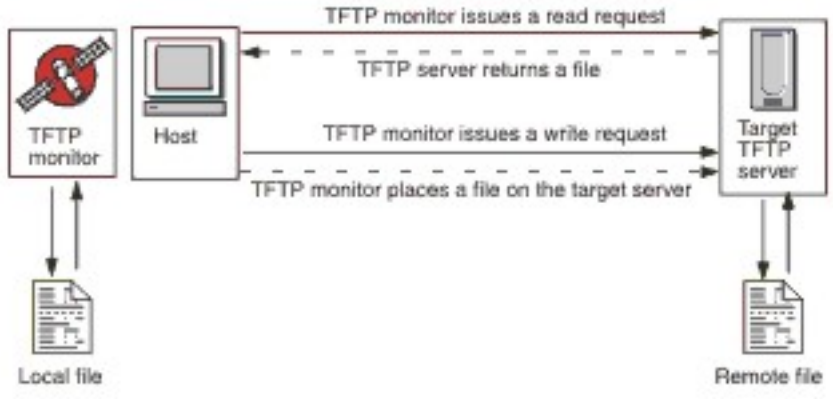
Le moniteur TFTP mesure les performances du service TFTP (Trivial File Transfer Protocol) entre deux systèmes.

Le tableau ci-dessous répertorie les fichiers du moniteur TFTP.

Tableau 150. Récapitulatif du moniteur FTP	
Fichiers du moniteur	**Nom ou emplacement**
Nom de l'exécutable	`nco_m_tftp`
Fichier de propriétés	`$ISHOME/etc/props/tftp.props`
Fichier de règles	`$ISHOME/etc/rules/tftp.rules`
Fichier journal	`$ISHOME/log/tftp.log`

Consignes de configuration du moniteur TFTP

Le moniteur TFTP assure la transmission des fichiers entre le système hôte et le serveur cible à l'aide de demandes TFTP READ ou WRITE, puis enregistre le temps de réponse et la vitesse de transfert des données. Utilisez-le pour vous assurer que votre serveur TFTP est en cours d'exécution et que le transfert des fichiers s'effectue à un taux acceptable.



Pour transférer un fichier, le moniteur envoie la demande TFTP WRITE (WRQ) et pour télécharger un fichier, il envoie la demande TFTP READ (RRQ). Sur les clients TFTP, l'opération de transfert est PUT et l'opération de téléchargement est GET.

Le moniteur TFTP prend en charge les modes de transfert de fichier octet (binaire) et netascii.

Configuration des tests de service du moniteur TFTP

Les paramètres de configuration du moniteur TFTP permettent de définir des tests de service.

Tableau 151. Configuration du moniteur TFTP	
Zone	**Description**
server	Adresse IP du serveur TFTP cible ou du système à partir duquel ou vers lequel vous souhaitez transférer des fichiers.
localfile	Pour les opérations GET, cette zone spécifie le nom et le chemin d'accès vers lequel le fichier est téléchargé. Pour les opérations PUT, cette zone spécifie le nom et le chemin d'accès du fichier transféré sur le serveur.
remotefile	Pour les opérations GET, cette zone spécifie le nom et le chemin d'accès du fichier téléchargé depuis le serveur. Pour les opérations PUT, cette zone spécifie le nom et le chemin d'accès vers lesquels le fichier est transféré sur le serveur.

Tableau 151. Configuration du moniteur TFTP (suite)	
Zone	**Description**
description	Zone de texte permettant d'indiquer des informations descriptives sur le moniteur TFPT.
port	Port utilisé par le serveur TFTP. Par défaut : 69
localip	Adresse IP de l'interface réseau de l'hôte sur lequel le moniteur ouvre la connexion TFTP. Si cette zone est vide, le moniteur utilise l'interface spécifiée par la propriété `IpAddress`.
localport	Port utilisé par le moniteur pour établir la connexion TFTP. Si la valeur de cette zone est `0`, le moniteur sélectionne un port adapté.
command	Commande TFTP à utiliser par le moniteur : • GET - Télécharge un fichier depuis le serveur cible sur l'hôte du moniteur. • PUT - Transfère un fichier depuis l'hôte du moniteur vers le serveur cible. Valeur par défaut : GET
transfermode	Indique le format dans lequel le moniteur transfère le fichier : • OCTET (8 bits) • NETASCII Par défaut : OCTET
timeout	Durée d'attente d'une réponse du serveur TFTP, en secondes. Valeur par défaut : 10
retries	Nombre de nouvelles tentatives du moniteur de transférer un fichier avant d'abandonner. Valeur par défaut : 3
poll	Délai, en secondes, entre chaque interrogation. N'attribuez pas une valeur trop élevée à ce paramètre car des interrogations constantes pourraient saturer le service. Valeur par défaut : 300
failureretests	Nombre de tentatives effectuées par le moniteur pour tester le serveur TFTP après un premier échec avant qu'un échec soit indiqué. Valeur par défaut : 0
retestinterval	Délai, en secondes, avant chaque nouveau test en cas d'incident. Valeur par défaut : 10

Classifications des niveaux de services

Les classifications des niveaux de services définissent les règles de détermination du niveau de service fourni par un serveur TFTP.

Les options de classification des niveaux de services disponibles pour le moniteur TFTP sont :

```
totalTime
lookupTime
responseTime
transferTime
bytesTransferred
bytesPerSec
checksum
message
```

Dans les classifications des niveaux de services :

- Spécifiez d'autres classifications des niveaux de services en entrant manuellement le nom de l'élément de moniteur. Ce nom doit correspondre à celui qui est indiqué pour l'élément dans la section des éléments Moniteurs.
- `message` peut correspondre à n'importe quel message transmis via l'élément `$message` au IBM Application Performance Management utilisé dans un widget. Pour obtenir une liste des valeurs possibles, voir Messages d'état.
- L'opérande est une chaîne ou un nombre positif.
- Normalement, l'élément `checksum` ne fournit pas de résultats significatifs pour les classifications des niveaux de services. Sa valeur est inconnue au moment où il est créé. Les valeurs de total de contrôle sont calculées par le moniteur au cours des tests. Cet élément est destiné à l'enrichissement des alertes à l'aide des fichiers de règles.

Eléments du moniteur

Outre les résultats de test communs à tous les éléments, le moniteur TFTP génère un ensemble de résultats de test contenant les données propres aux tests de service TFTP.

Le tableau suivant décrit les éléments supplémentaires du moniteur TFTP.

Tableau 152. Eléments du moniteur TFTP

Elément	Description
`$bytesPerSec*` (`BytesPerSec`)	Nombre moyen d'octets transférés par seconde.
`$bytesTransferred*` (`BytesTransferred`)	Nombre d'octets transférés ou téléchargés.
`$checksum`	Valeur de la somme de contrôle des données téléchargées. Elle est générée par le moniteur et fournie pour traitement supplémentaire par le biais de fichiers de règles.
`$command*` (`TftpCommand`)	Commande TFTP émise par le moniteur (GET ou PUT).
`$localFile*` (`TftpLocalFile`)	Nom de chemin complet du fichier stocké sur l'hôte local. Cet élément est tiré du fichier de configuration.
`$localIP`	Adresse IP locale que le moniteur doit utiliser. Cet élément peut être vide sur un système n'ayant qu'une seule interface.

Tableau 152. Eléments du moniteur TFTP (suite)	
Elément	**Description**
$lookupTime* (LookupTime)	Temps mis pour obtenir l'adresse IP du serveur hôte.
$remoteFile* (TftpRemoteFile)	Nom de chemin complet du fichier stocké sur l'hôte distant (serveur FTP). Cet élément est tiré du fichier de configuration.
(TransferTime)	Durée nécessaire pour transférer le fichier.
(TftpConnection)	Format auquel le moniteur a transféré le fichier. Il s'agit de OCTET (8 bits) ou NETASCII.

Messages d'état

Le moniteur TFTP fournit des messages d'état dans l'attribut ResultMessage lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Tableau 153. Messages d'état du moniteur TFTP	
Message	**Description**
OK	La requête TFTP a abouti.
FAILED: connect failed	Le moniteur n'a pas pu se connecter au serveur. Vérifiez que le serveur est en cours d'exécution.
FAILED: internal tftp monitor error	Un incident a été détecté sur le moniteur, probablement causé par une mémoire insuffisante.
FAILED: A send/wait timed out	La requête TFTP a échoué. Le problème est peut-être lié au réseau.
FAILED: An unspecific error condition. The transfer should be aborted	
FAILED: Received a short or malformed packet	
FAILED: local file open/read/write failed	
FAILED: unrecognized status from transfer attempt	

Exemple

Testez la disponibilité du serveur TFTP tftp.mycompany.com en transférant le fichier $ISHOME/etc/testfiles/upload.txt vers /ism/test/upload_result.txt. Utilisez le mode netascii pour télécharger les fichiers à des intervalles de 20 minutes

Classifiez le niveau de service selon les critères suivants :

- Si le téléchargement n'aboutit pas, le niveau de service est Failed
- Si la durée totale du transfert est supérieure à 10 secondes, le niveau de service est Marginal

- Sinon, le niveau de service est Good

Créez un élément de profil du moniteur TFTP et définissez la configuration comme indiqué dans le tableau ci-dessous.

Tableau 154. Exemple d'élément de profil TFTP

Zone de configuration	**Valeurs**
server	tftp.mycompany.com
localfile	`$ISHOME/etc/ism/testfiles/upload.txt`
remotefile	`/ism/test/upload_result.txt`
description	Test TFTP
Active	Sélectionné
command	PUT
transfermode	NETASCII
poll	1200

instruction	`If (Message != OK) then status Failed`
	`else if (TotalTime > 10) then status Marginal`
	`else status Good`

Moniteur TRANSX

Le moniteur TRANSX simule les actions d'un utilisateur Internet réel en exécutant une série d'activités à l'aide d'autres moniteurs de service Internet.

Par exemple, vous pouvez configurer TRANSX pour accéder à des pages d'un site Web à l'aide du moniteur HTTP, télécharger certains fichiers, et effectuer des envois ou des réceptions à l'aide des moniteurs POP3 et SMTP.

Le tableau ci-dessous répertorie les fichiers du moniteur TRANSX.

Tableau 155. Fichiers du moniteur TRANSX

Fichiers du moniteur	**Nom ou emplacement**
Exécutable du moniteur	`nco_m_transaction`
Fichier de propriétés	`$ISHOME/etc/props/transx.props`
Fichier de règles	`$ISHOME/etc/rules/transx.rules`
Fichier journal	`$ISHOME/log/transx.log`

Propriétés

Tableau 156. Propriétés du moniteur TRANSX

Nom de la propriété	Paramètre de la propriété	Description
`CompleteTransax`	`0`|`1`	Indique que la transaction continue même en cas d'échec d'une étape. • `0` - désactivé (ne continue pas) • `1` - activé (continue)
`DetailedTimings`	`0`|`1`	Indique que le moniteur TRANSX produit des journaux de données contenant des durées à granularité fine pour chaque étape. Les durées à granularité fine produites dans les journaux de données sont prédéfinies et ne peuvent pas être modifiées. • `0` - désactivé • `1` - activé
`MultipleEvents`	`0`|`1`	Indique si le moniteur génère plusieurs événements pour les résultats de transaction : • `0` - désactivé (le moniteur génère un seul événement contenant les résultats de toutes les étapes et les résultats récapitulatifs) • `1` - activé (le moniteur génère un événement pour chaque étape de transaction, ainsi qu'un événement récapitulatif final)
`StepPause`	entier	Indique la durée de la pause, en secondes, entre l'exécution de chaque étape de la transaction. La durée de la pause n'affecte pas la valeur de l'élément `$totalTime` d'une transaction. `$totalTime` représente la somme des éléments `$stepXTime` d'une transaction. Valeur par défaut : `0`

Le tableau ci-dessous décrit les propriétés propres au moniteur SMTP.

Consignes de configuration du moniteur TRANSX

Le moniteur TRANSX teste des services en simulant un ensemble d'activités qui impliquent une expérience utilisateur standard. L'ensemble d'activités est appelé une `transaction`, et chaque activité de la transaction est appelée une `étape de transaction`.

Les éléments de profil TRANSX définissent les transactions. Chaque étape de transaction configure un moniteur de service Internet, comme un moniteur HTTP, pour exécuter l'opération pour cette étape. Vous configurez les étapes de transaction à l'aide du bouton Editer dans l'onglet Etapes de l'élément de profil TRANSX.

Les étapes sont configurées de la même manière que tout autre élément de profil. Par exemple, les détails de configuration d'une étape qui implique le moniteur HTTP peuvent inclure des paramètres d'en-tête/formulaire, des paramètres de serveur proxy, des expressions régulières et des classifications de niveau de service.

Lorsque le moniteur TRANSX teste une étape dans la transaction, il enregistre la durée et le niveau de service de l'étape.

Remarque : Le moniteur TRANSX requiert des droits d'accès de niveau superutilisateur si des étapes de transaction utilisent un autre moniteur, ICMP par exemple, qui requiert ces droits d'accès.

Gestion du contenu dynamique avec des moniteurs HTTP et HTTPS

Un grand nombre de sites Web utilisent un contenu dynamique pour fournir des fonctions, telles des interactions basées sur des régions ou des sessions. En cas d'utilisation avec le moniteur TRANSX, les moniteurs HTTP et HTTPS peuvent tester les pages Web qui contiennent du contenu dynamique, comme des ID session, des codes de région ou des dates et des heures intégrées dans des liens, dont les valeurs peuvent être différentes à chaque test de la transaction.

Les fonctions de contenu dynamique fournies par les moniteurs HTTP et HTTPS lors de l'exécution en mode transaction permettent d'identifier le contenu dynamique sous la forme de paires nom-valeur, appelées `éléments de page dynamique`, intégrées dans des URL ou définies dans des éléments `form` HTML, que le moniteur extrait ensuite d'une page lors de chaque test, garantissant que la valeur dynamique appropriée est utilisée à chaque test d'une transaction.

Par exemple, prenons en compte une page de connexion d'un site Web, `http://www.mycompany.com/login`, qui contient un lien permettant de se connecter au site Web. L'URL de lien de l'action de connexion `http://www.mycompany.com/doLogin?sessionID=id` inclut un ID session pour la transaction de connexion. Dans cet exemple, la paire nom-valeur est un élément de page dynamique `sessionID=id` ; la valeur `id` change à chaque accès de la page de connexion. Si vous souhaitez tester la page de connexion dans le cadre d'une transaction, configurez la transaction pour obtenir et utiliser la valeur de `sessionID` à chaque test de la transaction et l'insérer dans l'URL d'action de connexion.

Le moniteur TRANSX fait passer des éléments de page dynamique d'une étape de transaction à la suivante. Dans l'exemple de connexion au site Web, la première étape de la transaction accède à la page de connexion pour obtenir l'ID session, puis le transmet à une deuxième étape qui soumet la demande de connexion contenant cet ID. Les opérations effectuées dans ces étapes sont les suivantes :

1. Accès à la page contenant les éléments de page dynamique, par exemple `http://www.mycompany.com/login`
2. Soumission de l'action en utilisant les éléments de page dynamique, par exemple `http://www.mycompany.com/doLogin?sessionID=@@030671`

Lorsque vous identifiez un élément de page dynamique dans une étape de transaction, il est transmis à la prochaine étape de transaction qui insère la paire nom-valeur dans sa demande. L'élément est transmis à chaque transaction HTTP ou HTTPS suivante jusqu'à ce que vous la supprimiez explicitement.

Ajout et suppression des pages dynamiques

Chaque étape de transaction HTTP ou HTTPS est constituée d'une demande, qui renvoie une page HTML. Lors de l'exécution d'une étape de transaction qui contient des éléments de page dynamiques, le moniteur analyse la page HTML pour définir l'emplacement de chaque paire nom-valeur d'élément et le transmet à l'étape de transaction suivante, qui les insère dans la requête HTTP ou HTTPS.

Pour indiquer qu'une étape utilise des éléments de page dynamiques, associez le type de paramètre de l'élément à la valeur DYNAMIC. Indiquez ensuite chaque élément dynamique à extraire et passez aux étapes suivantes. Identifiez chaque élément dynamique en entrant son nom, par exemple `sessionID` et sélectionnez Ajouter à en tant que valeur. L'option Ajouter à indique que l'élément doit être transmis aux étapes suivantes.

Remarque : Pour obtenir le nom d'un élément de page dynamique, affichez le code source HTML de la page sur laquelle il se trouve.

Les éléments de page dynamiques passent d'une transaction à la suivante. S'il n'est plus nécessaire qu'un élément de page soit transmis à une étape suivante, associez l'option Valeur de l'élément à Retirer de. Mettez à jour manuellement les étapes de transaction afin de garantir que les éléments de page corrects sont traités.

Utilisez les instructions suivantes pour ajouter et supprimer des éléments de page dynamiques :

- Si une étape n'utilise pas d'élément de page dynamique, ne sélectionnez pas DYNAMIC en tant que type de paramètre.
- Si une étape requiert un élément de page dynamique, l'étape qui extrait la page sur laquelle l'élément dynamique apparaît doit spécifier le nom de l'élément et la valeur Ajouter à.
- Si une étape ne requiert pas d'élément dynamique provenant d'étapes précédentes, sélectionnez Retirer de pour la valeur de l'étape précédente.

GET et POST

Dans les méthodes GET, tous les éléments de page dynamiques sont insérés automatiquement dans l'URL de demande. Dans les méthodes POST, vous devez indiquer chaque élément dynamique en tant que paramètre FORM dans l'onglet Paramètres.

Le moniteur insère automatiquement les valeurs dynamiques pour chaque formulaire lors de l'exécution de l'étape de transaction.

Création de transaction

Vous définissez des transactions en créant des éléments de profil et des étapes de transaction TRANSX à l'aide de l'interface utilisateur Internet Service Monitoring. Pour plus d'informations, voir «Création de transactions», à la page 446.

Configuration du test des services du moniteur TRANSX

Tableau 157. Configuration du moniteur TRANSX

Zone	Description
transxname	Nom de la transaction.
description	Zone de texte permettant d'indiquer des informations descriptives sur l'élément.
poll	Délai, en secondes, entre chaque interrogation. Valeur par défaut : 300

Remarque : Surveillez la disponibilité d'un site Web à l'aide d'une séquence de navigation Web, de téléchargements de fichier et d'envois d'e-mail.

1. Créez un élément de profil TRANSX.
2. Créez une étape de transaction HTTP pour surveiller la disponibilité d'un site Web.
3. Créez une étape de transaction FTP pour surveiller un téléchargement de fichier.
4. Créez une étape de transaction POP3 ou SMTP pour surveiller les e-mails.

Pour plus d'informations, reportez-vous à la documentation de chaque moniteur.

Eléments du moniteur

Le moniteur TRANSX génère des événements contenant les résultats de chaque transaction. Ces événements contiennent les résultats de l'ensemble de la transaction, ainsi que ceux des différentes étapes de la transaction.

Par défaut, le moniteur place tous les résultats de transaction et d'étape dans un seul événement, mais en utilisant la propriété `MultipleEvents`, vous pouvez configurer le moniteur pour créer des événements spécifiques pour chaque étape de transaction et un événement récapitulatif pour l'ensemble de la transaction. Le tableau 1 répertorie les éléments récapitulatifs TRANSX.

Les éléments indiqués par un astérisque (*) sont disponibles en tant qu'attributs. Le nom des attributs est affiché entre parenthèses. L'absence d'astérisque indique qu'il n'existe aucun attribut équivalent. Les attributs entre parenthèses mais sans élément sont disponibles uniquement en tant qu'attributs ; il n'existe aucun élément équivalent.

Tableau 158. Eléments de moniteur récapitulatifs TRANSX	
Elément	**Description**
$numberOfSteps*(NumberOfSteps)	Nombre d'étapes de la transaction.
$stepDescriptions	Liste des descriptions de chaque étape, séparées par un caractère de barre verticale (|).
$stepTimes*(Step*1 to 10*TotalTime)	Données de durée renvoyées par chaque étape (1 à 10).
$stepUnits	Liste des unités de chaque étape, généralement des secondes, séparées par un caractère de barre verticale (|).
(TransName)	Nom de la transaction, spécifié lors de la configuration de la transaction.
(TransStepDescription)	Description de l'étape de transaction, spécifiée lors de la configuration de l'étape.

Message d'état

Le moniteur TRANSX fournit des messages d'état dans l'attribut ResultMessage lors de l'utilisation d'IBM Application Performance Management. Ces messages indiquent le résultat du test.

Le tableau ci-dessous décrit les messages d'état.

Tableau 159. Messages d'état du moniteur TRANSX	
Message	**Description**
Successfully completed transaction	La transaction a abouti.
Error in transaction	Un incident est survenu dans l'une des étapes de la transaction.
Service Level Failed, ending transactionService Level Failed	Le niveau de service de l'une des étapes a renvoyé une réponse d'échec, qui a provoqué l'arrêt de la transaction.

Création de transactions
Les transactions peuvent être définies en créant des éléments de profil et des étapes de transaction TRANSX à l'aide de l'interface utilisateur Internet Service Monitoring agent.

Procédure

Pour créer une transaction à l'aide de l'interface, procédez comme suit :

1. Cliquez sur l'icône **Configuration système**. Cliquez ensuite sur **Configuration d'agent**.
   La fenêtre de configuration de l'agent apparaît.
2. Cliquez sur l'onglet **ISM** pour configurer l'agent Internet Service Monitoring.
3. Cliquez sur l'icône plus **(+)** pour créer un nouveau profil. Entrez le **Nom de profil** et la **Description**.
4. Cliquez sur **Suivant**.
5. Cliquez sur Moniteur **TRANSX** dans la liste déroulante du moniteur pour sélectionner Moniteur TRANSX.
6. Cliquez sur **Suivant**.
7. Entrez les paramètres obligatoires.
8. Dans l'onglet **Avancé**, indiquez la **Fréquence de sondage**.
9. Cliquez sur l'icône plus **(+)** dans l'onglet Etapes.

10. Cliquez sur le moniteur qui doit être sélectionné dans la liste déroulante du moniteur.
11. Cliquez sur **Sélectionner** pour configurer l'étape de la transaction.
    a) Indiquez les paramètres obligatoires et facultatifs de la même manière que lorsqu'ils ont précédemment été entrés pour configurer les éléments de profil.
    b) Si vous créez des étapes dynamiques pour le moniteur HTTP ou HTTPS, définissez les paires Nom et Valeur dans l'onglet Paramètres, puis sélectionnez DYNAMIC comme type de paramètre.
12. Cliquez sur **Ajouter**.
13. Cliquez sur l'icône Actualiser dans la grille des étapes.
14. Répétez les étapes 1 à 13 pour chaque transaction supplémentaire.
15. Cliquez sur **Ajouter** pour terminer.
16. Cliquez sur **Terminé** pour sauvegarder.

Résultats

Remarque : Pour spécifier une pause entre chaque étape de la transaction, utilisez la propriété `StepPause`.

Paramètre SSL dans Internet Service Monitoring
Internet Service Monitoring utilise OpenSSL pour communiquer en toute sécurité avec des services Internet généralement distants à l'aide de différents moniteurs ; par exemple, le moniteur HTTPS communique avec un service HTTPD sécurisé. Internet Service Monitoring agent utilise également OpenSSL entre les moniteurs et Databridge et entre l'Internet Service Monitoring agent (KIS) et Databridge. Indiquez la suite de chiffrement que votre application utilise dans la propriété `SSLCipherSuite`.

Databridge doit être configuré pour communiquer de manière sécurisée avec les moniteurs et l'Internet Service Monitoring agent afin que chaque moniteur partage un ensemble commun de propriétés liées à Databridge pour gérer la communication sécurisée avec ce dernier. Certains moniteurs partagent également un ensemble comparable mais différent de propriétés connexes pour gérer les communications sécurisées avec leurs services Internet testés respectifs.

Les moniteurs suivants prennent en charge la surveillance de services Internet sécurisés :

- HTTPS
- IMAP4
- POP3
- SMTP

Ces moniteurs utilisent des certificats. Tous les certificats sont stockés au format X509 dans Privacy Enhanced Mail .Pemfiles dans `$ISMHOME/certificates`. Le certificat de Databridge est stocké au même endroit. C'est la raison pour laquelle les propriétés suivantes sont partagées par tous les moniteurs, Databridge et l'Internet Service Monitoring agent :

- SSLTrustStore (par défaut : $ISMHOME/certificates/trust.pem)
- SSLTrustStorePath (par défaut : $ISMHOME/certificates/)

Comme toutes les communications entre les moniteurs et Databridge et entre des moniteurs sélectionnés et leurs services Internet sécurisés s'appuient sur la même version d'OpenSSL, elles partagent un certain nombre de propriétés. Par exemple, le niveau maximal de sécurité qu'Internet Service Monitoring peut fournir est une fonction du plus haut niveau de sécurité fourni par le protocole OpenSSL sous-jacent. De la même manière, le niveau minimal de sécurité fourni est dépendant du protocole OpenSSL sous-jacent.

Si Internet Service Monitoring agent est mis à jour et que l'OpenSSL sous-jacent est concerné, les services Internet surveillés peuvent en être affectés. Par exemple :

1. Le moniteur HTTPS dans Internet Service Monitoring agent V7.x.1 surveille un serveur HTTPD sécurisé.

2. Appliquez une nouvelle version d'Internet Service Monitoring agent qui contient une version mise à jour d'OpenSSL, ce qui signifie que le moniteur HTTPS est maintenant au niveau de version V7.x.2.
3. Vous constatez que le moniteur HTTPS ne parvient plus à surveiller le processus HTTPD sécurisé.

Le niveau de sécurité du serveur HTTPD est inférieur au niveau minimal pris en charge par la nouvelle version d'Internet Service Monitoring agent V7.x.2. Si la configuration du moniteur HTTPS n'a pas changé, son comportement, lui, a changé car il dépend de la couche OpenSSL sous-jacente. La combinaison plus récente d'Internet Service Monitoring agent/moniteur HTTPS /OpenSSL est plus sécurisée que l'ancienne et il est nécessaire à présent d'élever le niveau de sécurité du serveur HTTPD distant.

La surveillance des services Internet sécurisés vous mettent face à un dilemme. Le niveau de sécurité d'Internet Service Monitoring agent doit-il être maintenu à un niveau faible pour permettre la surveillance des services Internet bénéficiant d'une protection réduite ou doit-il être relevé pour atteindre le niveau minimal requis par les paramètres recommandés actuels ? Dans la première hypothèse, Internet Service Monitoring agent est affaibli et la sécurité risque d'être compromise, peut-être même aux deux extrémités.

La même version d'OpenSSL est utilisée par tous les moniteurs. Tous ces moniteurs partagent un ensemble commun de propriétés décrites dans le tableau ci-après pour configurer la couche OpenSSL sous-jacente.

Tableau 160. Propriétés de moniteur liées à OpenSSL

Nom de la propriété	**Paramètre de la propriété**	**Description**
`SSLCipherSuite`	chaîne	Indique les suites de chiffrement à utiliser pour des opérations SSL entre le moniteur et le service Internet surveillé. Les valeurs de cette propriété doivent être indiquées dans un format recommandé par OpenSSL. Valeur par défaut : `AES:3DES:DES:!EXP:!DHE:!EDH`
`SSLDisableSSLv2`	0|1	Détermine le type de connexion sécurisée à créer lors de la surveillance d'un service Internet sécurisé. `0` – SSLv2 est autorisé `1` – SSLv2 n'est PAS autorisé Valeur par défaut : `1` (SSLv2 n'est PAS autorisé).
`SSLDisableSSLv3`	0|1	Détermine le type de connexion sécurisée à créer lors de la surveillance d'un service Internet sécurisé. `0` – SSLv3 est autorisé `1` – SSLv3 n'est PAS autorisé Valeur par défaut : `1` (SSLv3 n'est PAS autorisé).
`SSLDisableTLS`	0|1	Détermine le type de connexion sécurisée à créer lors de la surveillance d'un service Internet sécurisé. `0` – TLSv1.0 est autorisé `1` – TLSv1.0 n'est PAS autorisé Valeur par défaut : `0` (TLSv1.0 est autorisé).

Tableau 160. Propriétés de moniteur liées à OpenSSL (suite)

Nom de la propriété	Paramètre de la propriété	Description
SSLDisableTLS11	0|1	Détermine le type de connexion sécurisée à créer lors de la surveillance d'un service Internet sécurisé. 0 – TLSv1.1 est autorisé 1 – TLSv1.1 n'est PAS autorisé Valeur par défaut : 0 (TLSv1.1 est autorisé).
SSLDisableTLS12	0|1	Détermine le type de connexion sécurisée à créer lors de la surveillance d'un service Internet sécurisé. 0 – TLSv1.2 est autorisé 1 – TLSv1.2 n'est PAS autorisé Valeur par défaut : 0 (TLSv1.2 est autorisé).
SSLCertificateFile	chaîne	Chemin et nom du fichier de certificat numérique public utilisé par le moniteur. Lorsqu'un moniteur tente d'établir une connexion à un service Internet, ce dernier peut exiger de lui qu'il fournisse un certificat côté client, pour lui permettre de vérifier le moniteur ou le client (vérification du certificat côté client). Le certificat doivent être au format PEM (Privacy Enhanced Mail). Pour le moniteur HTTPS, cette valeur peut être définie pour chaque élément HTTPS au moment de la création. Toutefois, si le moniteur HTTPS doit utiliser le même certificat pour tous les éléments, la valeur du fichier HTTPS.props est utilisée. Pour les moniteurs IMAP, LDAP, POP3, SIP, SMTP et SOAP, la valeur est définie au niveau du moniteur. Si le chemin d'accès n'est pas absolu, il est interprété par le moniteur comme étant relatif par rapport au répertoire de travail, $ISMHOME/certificates. Valeur par défaut : “”
SSLKeyFile	chaîne	Chemin et nom du fichier contenant la clé privée utilisée par le moniteur. Le moniteur utilise ce fichier pour chiffrer les messages qu'il l'envoie aux autres. Les récepteurs utilisent le certificat numérique public du moniteur pour déchiffrer le message. Valeur par défaut : monitoryKey.pem
SSLKeyPassword	chaîne	Mot de passe utilisé pour chiffrer la clé privée SSL. Valeur par défaut : “”

Tableau 160. Propriétés de moniteur liées à OpenSSL (suite)		
Nom de la propriété	**Paramètre de la propriété**	**Description**
SSLTrustStoreFile	chaîne	Nom complet du fichier qui stocke tous les certificats publics X509 des services Internet surveillés sous la forme d'une liste concaténée. Les certificats révoqués (CRL) sont également stockés ici sous la forme d'une liste concaténée. Databridge peut également stocker son certificat public ici. Cette propriété apparaît dans le fichier `bridge.props`. Les certificats sont stockés au format PEM (Privacy Enhanced Mail). Convertissez au format PEM les certificats obtenus dans d'autres formats à l'aide des logiciels OpenSSL disponibles sur le site http://www.openssl.org. Valeur par défaut : **“$ISMHOME/certificates/trust.pem”**
SSLTrustStorePath	chaîne	Emplacement des fichiers `.pem` contenant les certificats X509 du service Internet sécurisé surveillé. Les certificats révoqués (CRL) sont également stockés ici. Databridge peut également stocker son certificat public ici. Cette propriété apparaît dans le fichier `bridge.props`. Si de nouveaux certificats sont ajoutés à ce répertoire, exécutez la commande openssl `rehash` pour analyser le répertoire et calculer un hachage pour chaque certificat. Si les propriétés `SSLTrustStoreFile` et `SSLTrustStorePath` sont toutes les deux utilisées, OpenSSL utilise les deux propriétés pour localiser les certificats de confiance. Valeur par défaut : “`$ISMHOME/certificates/`”
`VerifyCertificate Preference`	0|1	Active ou désactive la vérification du certificat fourni par le service Internet surveillé en fonction de la liste de révocation de certificat (CRL). Valeur par défaut : 0 - désactivé

Suites de chiffrement

Les suites de chiffrement dont disposent Internet Service Monitoring sont un sous-ensemble des suites autorisées par OpenSSL. L'ensemble de suites de chiffrement autorisées par OpenSSL change au fil du temps. Au fur et à mesure que de nouvelles vulnérabilités sont détectées et que les meilleures pratiques évoluent, l'accès à des types spécifiques et généraux de suites de chiffrement peut être limité ou supprimé intégralement par OpenSSL. Ces versions ultérieures d'OpenSSL étant incluses dans les versions ultérieures d'ISM, les effets produits peuvent avoir une incidence sur la configuration et le fonctionnement des moniteurs.

Utilisez la propriété SSLCipherSuite au niveau du moniteur pour indiquer les suites de chiffrement autorisés par un moniteur à partir de toutes les suites de chiffrement disponibles à l'aide de mots clés. Pour indiquer plusieurs suites, utilisez une liste de mots clés séparés par le signe deux points. Par exemple, la propriété SSLCipherSuite par défaut est AES:3DES:DES:!EXP:!DHE:!EDH. Cette sélection signifie que les suites de chiffrement incluant AES, 3DES et DES sont autorisées mais les suites de chiffrement qui utilisent les échanges de clés EXP (Export short key lengths)), DHE (Diffie Hellman Exchange) ou EDH (Ephemeral Diffie Hellman) sont exclus. Lorsque la connexion sécurisée est établie entre le moniteur et le service Internet, AES est utilisé en premier, suivi de 3DES, puis de DES, si nécessaire. La syntaxe de la suite de chiffrement pour Internet Service Monitoring agent est la même que pour OpenSSL.

Pour sélectionner l'ensemble de suites de chiffrement approprié pour un moniteur, examinez les algorithmes pris en charge par la couche OpenSSL sous-jacente, la plage de suites de chiffrement prises en charge par le service Internet surveillé et les normes de sécurité de votre organisation. Vous ne pourrez peut-être pas surveiller un site externe sécurisé dont le niveau de sécurité est inférieur à celui que Internet Service Monitoring ou OpenSSL tolère. Dans certains cas, un moniteur qui pouvait auparavant surveiller un service Internet risque d'échouer après avoir mis à niveau Internet Service Monitoring car les niveaux de sécurité sont incompatibles.

Le tableau ci-dessous répertorie un sous-ensemble de suites de chiffrement équivalent à la propriété SSLCiperSuite par défaut incluant AES:3DES:DES:!EXP:!DHE:!EDH avec leurs propriétés. Les termes suivants apparaîtront dans le tableau :

- Nom de la suite de chiffrement : décrit la suite de chiffrement à l'aide d'un nom construit à partir de mots clés.
- Protocole : décrit la version du protocole pris en charge.
- Echange de clés : décrit le système d'échange de clés utilisé pour le chiffrement et le déchiffrement.
- Chiffrement et longueur de la clé : décrit le type d'algorithme de chiffrement utilisé et la longueur de la clé (en bits) utilisée.
- MAC : décrit le code d'authentification de message (Message Authentication Code) utilisé pour s'assurer que les données n'ont pas été faussées.

Tableau 161. Nom de la suite de chiffrement et valeurs de propriété AES:3DES:DES:!EXP:!DHE:!EDH

Nom de la suite de chiffrement	Protocole	Echange de clés	Authentification	Chiffrement et longueur de clé	Code d'authentification de message
ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	ECDH	RSA	AESGCM(256)	AEAD
ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	ECDH	ECDSA	AESGCM(256)	AEAD
ECDHE-RSA-AES256-SHA384	TLSv1.2	ECDH	RSA	AES(256)	SHA384
ECDHE-ECDSA-AES256-SHA384	TLSv1.2	ECDH	ECDSA	AES(256)	SHA384
ECDHE-RSA-AES256-SHA	SSLv3	ECDH	RSA	AES(256)	SHA1
ECDHE-ECDSA-AES256-SHA	SSLv3	ECDH	ECDSA	AES(256)	SHA1
SRP-DSS-AES-256-CBC-SHA	SSLv3	SRP	DSS	AES(256)	SHA1
SRP-RSA-AES-256-CBC-SHA	SSLv3	SRP	RSA	AES(256)	SHA1

Tableau 161. Nom de la suite de chiffrement et valeurs de propriété AES:3DES:DES:!EXP:!DHE:!EDH (suite)					
Nom de la suite de chiffrement	**Protocole**	**Echange de clés**	**Authentification**	**Chiffrement et longueur de clé**	**Code d'authentification de message**
SRP-AES-256-CBC-SHA	SSLv3	SRP	SRP	AES(256)	SHA1
DH-DSS-AES256-GCM-SHA384	TLSv1.2	DH/DSS	DH	AESGCM(256)	AEAD
...suivi de 61 lignes supplémentaires					

Le tableau ci-dessous répertorie un sous-ensemble de suites de chiffrement équivalent à la valeur de la propriété `SSLCiperSuite` incluant `AES:3DES:DES:!EXP:!DHE:!EDH:!SSLv2:!SSLv3` avec leur propriétés. Certains protocoles sont maintenant éliminés et l'ensemble global des suites de chiffrement est réduit de 71 à 31.

*Tableau 162. Nom de la suite de chiffrement et valeurs de propriétés **AES:3DES:DES:!EXP:!DHE:!EDH:!SSLv2:!SSLv3***					
Nom de la suite de chiffrement	**Protocole**	**Echange de clés**	**Authentification**	**Chiffrement et longueur de clé**	**Code d'authentification de message**
ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	ECDH	ECDSA	AESGCM(256)	AEAD
ECDHE-RSA-AES256-SHA384	TLSv1.2	ECDH	RSA	AES(256)	SHA384
ECDHE-ECDSA-AES256-SHA384	TLSv1.2	ECDH	ECDSA	AES(256)	SHA384
DH-DSS-AES256-GCM-SHA384	TLSv1.2	DH/DSS	DH	AESGCM(256)	AEAD
DH-RSA-AES256-GCM-SHA384	TLSv1.2	DH/RSA	DH	AESGCM(256)	AEAD
DH-RSA-AES256-SHA256	TLSv1.2	DH/RSA	DH	AES(256)	SHA256
DH-DSS-AES256-SHA256	TLSv1.2	DH/DSS	DH	AES(256)	SHA256
ADH-AES256-GCM-SHA384	TLSv1.2	DH	Aucun	AESGCM(256)	AEAD
ADH-AES256-SHA256	TLSv1.2	DH	Aucun	AES(256)	SHA256
ECDH-RSA-AES256-GCM-SHA384	TLSv1.2	ECDH/RSA	ECDH	AESGCM(256)	AEAD
...suivi de 21 lignes supplémentaires					

Réduction des vulnérabilités

Les chiffrements DHE et EDH seront désactivés par défaut dans les éditions ultérieures en raison de vulnérabilités. Pour les versions antérieures d'Internet Service Monitoring agent, il peut s'avérer nécessaire de désactiver les chiffrements DHE et EDH dans tous les moniteurs. Pour désactiver les chiffrements DHE et EDH, mettez à jour les propriétés `SSLCipherSuite` et `BridgeSSLCipherSet` des moniteurs.

Par exemple, pour désactiver des chiffrements DHE et EDH dans le moniteur HTTPS, mettez à jour le fichier `https.props` pour inclure les propriétés suivantes :

```
SSLCipherSuite: AES:3DES:DES:!DES-CBC-SHA:!EXP:!DHE:!EDH
BridgeSSLCipherSet: AES:3DES:DES:!DES-CBC-SHA:!EXP:!DHE:!ED
```

Assurez-vous que cette modification de configuration n'entraîne pas de problèmes de compatibilité. Si vous modifiez le paramètre par défaut après l'application de ce correctif, vous risquez de vous exposer à une vulnérabilité en matière de sécurité. Vous devez examiner l'ensemble de votre environnement pour identifier les autres emplacements où vous avez activé le protocole d'échange de clés Diffie-Hellman utilisé dans TLS et exécutez les actions d'atténuation et de correction appropriées.

Sélection de protocoles

Vous pouvez faire votre choix parmi une série de protocoles de communication sécurisée anciens ou plus récents. Vous pouvez les sélectionner individuellement à l'aide d'un ensemble de propriétés de moniteur de type booléen :

- SSLDisableSSLv2
- SSLDisableSSLv3
- SSLDisableTLS
- SSLDisableTLS11
- SSLDisableTLS12
- BridgeSSLDisableSSLv2
- BridgeSSLDisableSSLv3

Vous devez désactiver SSLv2 et SSLv3. La sécurité de ces protocoles est compromise et présente plusieurs vulnérabilités connues. Ils sont désactivés par défaut et sont fournis uniquement pour des raisons .

Internet Service Monitoring active TLS par défaut. Si vous savez que les services Internet que vous surveillez n'utilisent pas TLS 1.0 et sont déjà passés à TLS 1.1 ou TLS 1.2, désactivez les protocoles inutilisés dans Internet Service Monitoring.

Le composant Databridge communique avec l'agent Internet Service Monitoring et chacun des moniteurs. Par défaut, cette communication est chiffrée et TLS est le protocole préféré.

Magasins de clés de confiance et certificats

Internet Service Monitoring stocke ses certificats dans un fichier et dans un emplacement définis par l'utilisateur. Tous les certificats doivent être stockés au format PEM (Privacy Enhanced Mail). Vérifiez que les certificats publics obtenus auprès d'autres organisations sont convertis au format PEM. Des logiciels de conversion sont disponibles à l'adresse http://www.openssl.org.

Les certificats de confiance indiqués à l'aide de la propriété `SSLTrustStoreFile` sont stockés dans le fichier sous la forme d'une liste concaténée.

Il est recommandé de stocker les listes de révocation de certificats (CRL) dans le magasin de clés de confiance dans lequel les certificats peuvent être validés. Les autorités de certification ont mis en place des systèmes qui génèrent des listes de certificats révoqués, ainsi que des systèmes de distribution qui les rendent disponibles publiquement. Ainsi, tout certificat compromis est révoqué.

Paramètres de sécurité de Databridge

Tous les moniteurs communiquent avec Databridge ; ils possèdent donc tous un ensemble commun de propriétés qui doivent être définies pour gérer les communications entre les moniteurs et Databridge. Par défaut, la communication est chiffrée. Le protocole de chiffrement par défaut est TLS. Contrairement aux propriétés des moniteurs, il n'y a pas de mécanisme pour contrôler si une version spécifique de TLS est activée ou désactivée. Tous les moniteurs doivent posséder les mêmes valeurs pour les propriétés Databridge. Sinon, des problèmes de communication apparaissent. De la même manière, les propriétés définies dans le fichier .props de Databridge doivent être cohérentes avec

celles des moniteurs. Databridge communique également avec l'agent Internet Service Monitoring qui possède son propre fichier .props. Certaines des valeurs du fichier .props sont liées à Databridge et comme pour les moniteurs, elles doivent posséder des valeurs cohérentes avec celles définies dans le fichier `.props` de Databridge.

Tableau 163. Propriétés de Databridge liées à OpenSSL

Nom de la propriété	Paramètre de la propriété	Description
BridgeSSLEncryption	0|1	Détermine si les communications avec Databridge sont chiffrées ou non. Cette propriété couvre toutes les communications de Databridge vers les moniteurs et l'agent Internet Service Monitoring. `0` – non chiffré `1` – chiffré **Restriction :** Définissez la même valeur dans l'agent Internet Service Monitoring, tous les moniteurs et Databridge.
BridgeSSLCipherSet	chaîne	Indique les suites de chiffrement à utiliser pour des opérations SSL en provenance et à destination de Databridge. Les valeurs de cette propriété doivent être indiquées dans le format recommandé par OpenSSL. **Restriction :** Définissez la même valeur dans l'agent Internet Service Monitoring, tous les moniteurs et Databridge. Valeur par défaut : `AES:3DES:DES:!EXP:!DHE:!EDH`
BridgeSSLDisableSSLv2	0|1	Détermine le type de connexion sécurisée à créer en provenance et à destination de Databridge. `0` – SSLv2 et SSLv3 sont autorisés `1` – SSLv2 n'est PAS autorisé **Restriction :** Définissez la même valeur dans l'agent Internet Service Monitoring, tous les moniteurs et Databridge. Valeur par défaut : `1` (SSLv2 n'est PAS autorisé).
BridgeSSLDisableSSLv3	0|1	Détermine le type de connexion sécurisée à créer en provenance et à destination de Databridge. `0` – SSLv3 est autorisé `1` – SSLv3 n'est PAS autorisé **Restriction :** Définissez la même valeur dans l'agent Internet Service Monitoring, tous les moniteurs et Databridge. Valeur par défaut : `1` (SSLv3 n'est PAS autorisé).
BridgeSSLCertificateFile	chaîne	Chemin et nom de fichier du certificat SSL Databridge numérique. Valeur par défaut : `$ISMHOME/certificates/bridgeCert.pem`

Tableau 163. Propriétés de Databridge liées à OpenSSL (suite)

Nom de la propriété	Paramètre de la propriété	Description
BridgeSSLKeyFile	chaîne	Chemin et nom du fichier de clé privée SSL Databridge. Valeur par défaut : `$ISMHOME/certificates/bridgeKey.pem`
BridgeSSLKeyPassword	chaîne	Mot de passe utilisé pour chiffrer la clé privée SSL Databridge. Valeur par défaut : **Tivoli**
BridgeSSLTrustStore	chaîne	Chemin et nom du fichier de certificat sécurisé pour l'authentification. Cette propriété est nécessaire uniquement lorsque vous utilisez la propriété **BridgeSSLAuthenticatePeer**. Valeur par défaut : `$ISMHOME/certificates/trust.pem` Si vous souhaitez configurer l'authentification SSL entre un moniteur et Databridge, ou entre Databridge et l'agent, associez `BridgeSSLAuthenticatePeer` à la valeur 1 et redémarrez Databridge. Cette action permet d'authentifier les certificats du serveur. Vous pouvez stocker des certificats à la fois dans `SSLTrustStoreFile` et `SSLTrustStorePath`. Valeurs par défaut : • `SSLTrustStoreFile`, `$ISMHOME/certificates/trust.pem` • `SSLTrustStorePath`, `$ISMHOME/certificates/` Pour ajouter de nouveaux certificats, effectuez l'une des étapes suivantes : • Ajoutez un certificat à la fin de la liste dans le fichier texte `SSLTrustStoreFile` • Ajoutez un nouveau certificat au répertoire `SSLTrustStorePath`, et exécutez la commande OpenSSL **c_rehash certificate_dir** pour hacher les certificats
SSLTrustStoreFile	chaîne	Cette propriété est utilisée par des moniteurs sécurisés et Databridge. Pour plus d'informations, voir Tableau 160, à la page 448.
SSLTrustStorePath	chaîne	Cette propriété est utilisée par des moniteurs sécurisés et Databridge. Pour plus d'informations, voir Tableau 160, à la page 448.

Tableau 163. Propriétés de Databridge liées à OpenSSL (suite)		
Nom de la propriété	**Paramètre de la propriété**	**Description**
BridgeSSLAuthenticatePeer	0|1	Indique si Databridge doit effectuer une authentification croisée avec d'autres composants Internet Service Monitoring. 0 – désactivé 1 – activé Si un moniteur entre en contact avec Databridge, il doit s'authentifier auprès de Databridge et Databridge doit s'authentifier auprès du moniteur. Si l'agent Internet Service Monitoring contacte Databridge, il doit s'authentifier auprès de Databridge et Databridge doit s'authentifier auprès de l'agent. Les certificats de Databridge sont stockés dans BridgeSSLTrustStore. Valeur par défaut : 0 - désactivé

Propriétés de l'agent Internet Service Monitoring

L'Internet Service Monitoring agent possède son propre fichier de propriétés qui contient un ensemble de propriétés et de paramètres de sécurité. Le fichier de propriétés de l'agent ne communique pas avec les moniteurs, mais il communique avec Databridge, de sorte que les paramètres de sécurité définis dans le fichier `.props` de l'agent gèrent la communication entre l'agent et Databridge.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent sur les systèmes Windows à l'aide de la fenêtre **IBM Performance Management**.

Procédure

Configurez l'agent Internet Service Monitoring agent sur le système utilisateur de la manière suivante.

Pour configurer manuellement l'agent Internet Service Monitoring sur les systèmes utilisateur :

1. Dans le tableau de bord **IBM Performance Management**, cliquez sur **Configuration système** > **Configuration d'agent** sous **Configuration système**.
2. Cliquez sur l'onglet **ISM** pour ouvrir le tableau de bord de l'agent Internet Service Monitoring.

Configuration de Databridge

La configuration de Databridge comprend la définition de propriétés qui en contrôlent le fonctionnement, comme la connexion des modules du composant et des moniteurs de service Internet.

Fonctionnement et configuration
Databridge et ses modules de composant sont configurés à l'aide de fichiers de propriétés.

Les propriétés déterminent le fonctionnement de Databridge et de ses modules de composant qui envoient les résultats de test à IBM Cloud Application Performance Management en vue de la génération de rapport dans le tableau de bord de l'agent Internet Service Monitoring.

Configuration de Databridge
Databridge doit être configuré de sorte à recevoir des données provenant des moniteurs de service Internet et les transmettre à ses modules pour un traitement plus poussé.

Le tableau suivant répertorie les fichiers associés à Databridge. Le **`fichier de propriétés`**, le **`fichier SAF (Store And Forward)`** et le **`fichier journal`** sont décrits en détail dans leurs sections respectives.

Tableau 164. Fichiers Databridge et leur emplacement

Fichier Databridge	Emplacement ou nom
Fichier exécutable	`$ISHOME/platform/arch/bin/nco_m_bridge`
Fichier de propriétés	`$ISHOME/etc/props/bridge.props`
Fichier SAF (Store and Forward) and Forward) and Forward	Le nom et l'emplacement sont définis par les propriétés dans le fichier `bridge.props`. Le nom et l'emplacement par défaut sont `$ISHOME/var/sm_bridge.saf`
Fichier journal	`$ISHOME/log/bridge.log`
Fichier journal des erreurs	`$ISHOME/log/bridge.err`

Fichier SAF (Store And Forward)
Si Databridge ne peut pas transmettre des données à Netcool/OMNIbus, il stocke toutes les données qu'il doit normalement envoyer dans un fichier SAF (Store And Forward). Lorsque Netcool/OMNIbus est à nouveau disponible, il traite tous les événements stockés dans le fichier SAF.

Les propriétés QFile et QSize du fichier de propriétés Databridge déterminent le nom, l'emplacement et le fonctionnement du traitement SAF (Store and Forward).

Fichier journal
Databridge envoie des messages quotidiens concernant ses opérations à un fichier journal des messages. Par défaut, le nom de ce fichier est `$ISHOME/log/bridge.log`. Il est mis à jour à minuit (12:00 am). Les propriétés MsgDailyLog et MsgTimeLog de Databridge contrôlent l'opération de journalisation des messages.

Démarrage de Databridge
Démarrage de Databridge à l'aide de la console Windows Services.

Procédure

Remarque : Si le module ObjectServer est connecté à Databridge, vérifiez que son système cible est en cours d'exécution avant de démarrer Databridge. Si les modules Databridge ne parviennent pas à s'initialiser correctement, Databridge ne démarre pas.

1. A partir du bureau Windows, cliquez sur **Démarrer** > **Outils d'administration** > **Services**.
2. Dans la liste des services, sélectionnez le service NCO BRIDGE Internet Service Monitor et cliquez sur **Démarrer** dans le menu.

Connexion des modules
Le fichier de propriétés Databridge définit les modules à connecter à Databridge.

Pourquoi et quand exécuter cette tâche
Chaque paire de propriétés Module n `SharedLib` et Module n `PropFile` définit la connexion d'un module. Les modules sont chargés dans l'ordre de définition en commençant par Module0.

Procédure

1. Pour connecter des modules spécifiques à Databridge, procédez comme suit :

a) Dans le fichier de propriétés de Databridge, identifiez la paire de propriétés Module n SharedLib et Module n PropFile disponible suivante.

b) Affectez à Module n SharedLib le nom de la bibliothèque partagée du module (son implémentation binaire).

c) Affectez à Module n PropFile le chemin d'accès complet au fichier de propriétés du module.

Dans cet exemple, les lignes 1 et 2 connectent le module ObjectServer, les lignes 3 et 4 connectent le module Datalog et les lignes 5 et 6 connectent le module IBM Application Performance Management (pipe). Le module Datalog n'a pas de fichier de propriétés. L'entrée du fichier de propriétés a donc pour valeur "".

2. Pour désactiver un module, procédez comme suit :

a) Affectez la valeur "NONE" à la propriété Module n SharedLib correspondante, et la valeur "" à la propriété Module n PropFile. Tous les autres modules d'une valeur supérieure à n sont également ignorés.

Connexion des moniteurs
Les moniteurs de service Internet se connectent à Databridge via TCP. Chaque moniteur comporte un ensemble de propriétés qui configure la connexion à Databridge.

Pourquoi et quand exécuter cette tâche
Pour connecter un moniteur à Databridge, affectez la valeur de la propriété SocketPort définie dans le fichier de propriétés de Databridge à la propriété BridgePort définie dans le fichier de propriétés du moniteur. La valeur par défaut de chaque propriété BridgePort du moniteur et de la propriété SocketPort de Databridge est 9510.

DataBridge prend en charge le chiffrement SSL des résultats de test envoyés par les moniteurs. Pour chiffrer les résultats de test du moniteur, affectez les valeurs des propriétés BridgeSSL définies dans le fichier de propriétés de Databridge aux propriétés BridgeSSL définies dans le fichier de propriétés Databridge. Pour chiffrer tous les résultats de test des moniteurs, tous les moniteurs doivent avoir les mêmes propriétés BridgeSSL.

Configuration du module Databridge
Databridge transmet les résultats du test à l'agent Internet Service Monitoring. L'agent de surveillance convertit ces données dans le format approprié et les transmet au serveur IBM Application Performance Management. Configurez le module Databridge et l'agent Internet Service Monitoring via leurs fichiers de propriétés respectifs.

Configurez le fonctionnement de Databridge en modifiant les valeurs de propriétés définies dans le fichier de propriétés du module.

Le fichier de propriétés du module s'appelle pipe_module.props. Ce fichier se trouve dans le répertoire $ISHOME/etc/props/.

Le tableau ci-après répertorie les propriétés disponibles pour le module. Si vous apportez des modifications aux propriétés, vous devez redémarrer Databridge pour que ces modifications s'appliquent.

Tableau 165. Propriétés du module Databridge

Nom de la propriété	Type	Description
TEMAHOST	chaîne	Nom du système hôte qui exécute l'agent de surveillance. Valeur par défaut : localhost
TEMAPORT	entier	Numéro de port utilisé par l'hôte. Valeur par défaut : 9520

Vous pouvez configurer le fonctionnement de l'agent Internet Service Monitoring en modifiant les valeurs de propriétés définies dans le fichier de propriétés de l'agent.

Le fichier de propriétés de l'agent de surveillance s'appelle `kisagent.props`. Il se trouve dans le répertoire `$ISMHOME/etc/props/`.

Le tableau suivant répertorie les propriétés disponibles pour l'agent de surveillance.

Tableau 166. Propriétés de l'agent de surveillance

Nom de la propriété	Type	Description
TEMAPORT	entier	Numéro de port utilisé par l'hôte. Il doit correspondre au numéro de port de la propriété TEMAPORT indiquée dans le fichier de propriétés du module. Valeur par défaut : 9520
ObsoleteDuration	entier	Délai, en secondes, à l'issue duquel les données qui n'ont pas été mises à jour sont supprimées de la mémoire de l'agent de surveillance. Les données ne peuvent pas être mises à jour si, par exemple, un élément de profil a été arrêté ou qu'une défaillance du réseau s'est produite. **Remarque :** N'affectez pas à la propriété ObsoleteDuration une valeur inférieure à l'intervalle d'interrogation car cela risque d'entraîner des pertes de données entre les intervalles d'interrogation. Valeur par défaut : 900
AggDuration	entier	Période, en secondes, à l'issue de laquelle l'agent de surveillance arrête l'agrégation et l'affichage des données dans le tableau de bord de l'agent. Toutes les données antérieures à l'heure indiquée sont supprimées de la mémoire de l'agent de surveillance. Les données antérieures sont calculées en comparant l'intervalle entre l'heure de début et l'heure actuelle à l'heure de la durée d'agrégation. Si l'intervalle est supérieur à la durée d'agrégation, 10 % des anciennes données sont supprimées et l'heure de début est augmentée d'un dixième de l'intervalle. L'agent de surveillance exécute ce calcul toutes les 5 minutes. Valeur par défaut : 3600
ManageServices	0|1	Démarre et arrête tous les moniteurs et Databridge lorsque l'agent Internet Service Monitoring est démarré ou arrêté. 1 correspond à Activé et 0 correspond à Désactivé. Valeur par défaut : 1

La connexion entre l'agent Internet Service Monitoring et le module Databridge est créée lorsque vous installez Internet Service Monitoring.

Activation de Netcool/OMNIbus

Suivez cette procédure pour permettre à Tivoli Netcool/OMNIbus d'envoyer les événements de l'Internet Service Monitoring agent à Netcool/OMNIbus.

Avant de commencer

Assurez-vous que vous avez installé IBM Tivoli Netcool/OMNIbus.

Procédure

Pour activer Netcool/OMNIbus, procédez comme suit :

1. Arrêtez l'Internet Service Monitoring agent à l'aide de la commande suivante :

   ```
   $CANDLEHOME/bin/ism-agent.sh stop
   ```

2. Ouvrez le fichier `bridge.props` qui est placé dans `$ISMHOME/etc/props` et mettez-le à jour avec le fragment de code suivant :

   ```
   Module0SharedLib : "libSMModulePipe"
   Module0PropFile : "$ISMHOME/etc/props/pipe_module.props"
   Module1SharedLib : "libSMModuleObjectServer"
   Module1PropFile : "$ISMHOME/etc/props/objectserver.props"
   ```

3. Modifiez les droits du répertoire `8.1.0` placé dans le chemin `$ISMHOME/objectserver` de la manière suivante :

   ```
   cd  $ISMHOME/objectserver/
   chmod -R 777 8.1.0
   ```

   Remarque : Modifiez les droits de tous les fichiers dans le répertoire `8.1.0` à l'aide de la commande `chmod -R 777 <nom-fichier>`. Où `<nom-fichier>` est le nom du fichier placé dans le répertoire `8.1.0`.

4. Modifiez le fichier `omni.dat` placé dans le chemin `$ISMHOME/objectserver/8.1.0/etc` pour configurer l'adresse du serveur Netcool/OMNIbus.
5. Exécutez `nco_igen` à partir de l'emplacement suivant :

   ```
   cd $ISMHOME/objectserver/8.1.0/bin
   ./nco_igen
   ```

6. Démarrez l'Internet Service Monitoring agent à l'aide de la commande suivante :

   ```
   $CANDLEHOME/bin/ism-agent.sh start
   ```

7. Vérifiez que l'Internet Service Monitoring agent, Databridge et tous les moniteurs sont à l'état actif.

   Pour vérifier le statut de Databridge et des moniteurs, exécutez la commande suivante :

   ```
   ps -aef|grep -i nco_*
   ```

   Pour vérifier le statut de l'Internet Service Monitoring agent, exécutez la commande suivante :

   ```
   ps -aef|grep -i kis
   ```

8. Utilisez l'interface utilisateur IBM Tivoli Netcool/OMNIbus pour vérifier que Databridge envoie les données au serveur Netcool/OMNIbus.

   Les données doivent s'afficher pour l'Internet Service Monitoring agent dans l'interface utilisateur d'IBM Application Performance Management.

Configuration de la surveillance de J2SE

Pour collecter les données de surveillance et de diagnostic des ressources des applications Java sur site surveillées, vous devez configurer le collecteur de données J2SE.

Avant de commencer

Installez l'un des environnements d'exécution Java pris en charge :

- Oracle Java Platform Standard Edition 7 (kit de développement Java SE 7)

  A faire : Cet environnement Java Runtime ne prend pas en charge l'image du collecteur de données J2SE qui est configurée avec le protocole HTTPS.
- Oracle Java Platform Standard Edition 7 (Java SE Runtime Environment 7)

  A faire : Cet environnement Java Runtime ne prend pas en charge l'image du collecteur de données J2SE qui est configurée avec le protocole HTTPS.
- Oracle Java Platform Standard Edition 8 (kit de développement Java SE 8)
- Oracle Java Platform Standard Edition 8 (Java SE Runtime Environment 8)
- IBM SDK, Java Technology Edition, Version 7
- IBM SDK, Java Technology Edition, Version 8

Important : Pour le serveur Windows 2016, installez le JDK 8, mise à jour 131 (kit de développement Java SE 8u131) ou le kit de développement Java SE 7, mise à jour 80 (JDK 7u80).

Pour plus d'informations sur la configuration système requise, voir Software Product Compatibility Reports for J2SE data collector.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer le collecteur de données J2SE sur les systèmes Windows, Linux et AIX.

Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions de collecteur de données et d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Procédure

1. Copiez les fichiers suivants du programme d'installation d'APM dans un répertoire :

   Important : Le chemin de répertoire ne doit pas contenir d'espace.

   - Windows Copiez le fichier `gdc.zip` du programme d'installation d'APM dans un répertoire et extrayez-le.
   - Linux AIX Copiez le fichier `gdc-apd.tar.gz` du programme d'installation d'APM dans un répertoire et extrayez-le.
   - Linux AIX Accordez à l'utilisateur des droits en lecture/écriture et exécution sur le dossier `j2se_dc`. Les droits en exécution sont fournis pour l'exécution des scripts et des fichiers JAR dans le dossier. Les droits en lecture/écriture sont fournis car les fichiers de diagnostic approfondi sont générés dans ce dossier.
2. Sur la ligne de commande, accédez à *DCHOME*`\.gdc\<version_kit_outils>\bin`

   Où *version_kit_outils* correspond à :

   - Pour la version 8.1.4.0 et antérieure, *version_kit_outils* est 7.3.0.5.0.
   - Pour la version 8.1.4.0.1 et ultérieure, *version_kit_outils* est 7.3.0.14.0.
3. Exécutez la commande suivante :

   Windows `config.bat`

Linux AIX `config.sh`

4. Lorsque vous y êtes invité, indiquez le chemin d'accès au répertoire de base Java et appuyez sur la touche **Entrée**.
   Par exemple,

   Windows `C:\Program Files\jre7`

   Linux AIX `/opt/ibm/java`

5. Selon la version d'agent utilisée, suivez l'une des procédures ci-dessous :

   - Pour la version 8.1.4.0.2 et antérieure, procédez comme suit :

     a. Lorsque vous y êtes invité, entrez le nom complet (nom qualifié) de la classe principale de l'application et appuyez sur la touche **Entrée**. La classe principale est le point d'entrée de l'application qui doit être surveillée. Exemple : `testapp.TemperatureConveter`

     b. Lorsque vous y êtes invité, entrez un nom d'alias d'application distinct et appuyez sur la touche **Entrée**. Le nom indiqué est utilisé pour créer le nom d'instance sur le tableau de bord APM.

     Windows Le fichier `dcstartup.bat` est généré à l'emplacement suivant : *DCHOME*`\.gdc\`*version_kit_outils*`\runtime\j2se`*alias_application*`.`*nom_hôte*`.`*alias_application*. Ce fichier est le script permettant d'exécuter votre application avec le collecteur de données.

     Linux AIX Le fichier `dcstartup.sh` est généré à l'emplacement suivant : *DCHOME*`/.gdc/`*version_kit_outils*`/runtime/j2se`*alias_application*`.`*nom_hôte*`.`*alias_application*. Ce fichier est le script permettant d'exécuter votre application avec le collecteur de données.

   - Pour la version 8.1.4.0.3 à la version 8.1.4.0.5, procédez comme suit :

     a. A l'invite, entrez le répertoire de base de l'application Java. Par exemple, `/root/J2seApp/`

     b. Sélectionnez une application Java dans la liste présentée et cliquez ensuite sur Quitter.

     - `com.ibm.SampleApplication`
     - `com.ibm.DBApplication`
     - `com.ibm.SpringBootApplication`

     Sélectionnez une application répertoriée dans la liste ou saisissez 0 pour en sélectionner une qui n'y figure pas.

     1) Si vous saisissez 0, entrez le `nom complet` de la classe Main d'une autre application. Par exemple, `com.ibm.testApp.Main`

     2) Si vous sélectionnez une option dans la liste fournie, le nom d'alias est créé à partir du nom de la classe. Si le nom d'alias dépasse le nombre limite de caractères, réduisez ce nombre.

        Important : Le nombre limite de caractères pour le nom d'alias est calculé de sorte que `nom_alias + nom_hôte` ne dépasse pas 24 caractères.

     c. Sélectionnez l'option pour activer ou désactiver le suivi des transactions. La valeur par défaut est *Oui*.

     d. Sélectionnez l'option pour activer ou désactiver la collecte des données de diagnostic. La valeur par défaut est *Oui*.

     1) Si vous sélectionnez *Oui*, sélectionnez l'option permettant d'activer le mode de trace de méthode. La valeur par défaut est *Non*.

     e. Si vous sélectionnez une option dans la liste fournie à l'étape b, copiez le script de démarrage `<DCHOME>/j2se_dc/.gdc/`*version_kit_outils*`/runtime/j2se<alias_application>.<nom_hôte>.<alias_application>` à l'emplacement de votre choix.

   - Pour la version 8.1.4.0.6 et ultérieures, procédez comme suit :

a. A l'invite, entrez le répertoire de base de l'application Java. Par exemple, `/root/J2seApp/`

b. Sélectionnez le type d'application que vous voulez surveiller.

- Application Java
- Serveur Jetty

c. Si vous sélectionnez le type d'application *Application Java*, procédez comme indiqué à la section Version 8.1.4.0.3 à version 8.1.4.0.5 de l'étape 5.

d. Si vous sélectionnez le type d'application *Serveur Jetty*, procédez comme suit :

1) Entrez le répertoire de base de Jetty. Par exemple, `/home/jetty/jetty-distribution-9.4.12.v20180830`

2) Entrez le nom d'alias. Si le nom d'alias dépasse le nombre limite de caractères, réduisez ce nombre.

Important : Si vous sélectionnez le type d'application *Application Java* et une option de la liste à l'étape b de la section Version 8.1.4.0.3 à version 8.1.4.0.5, copiez le script de démarrage `<DCHOME>/j2se_dc/.gdc/version_kit_d'outils/runtime/j2se<alias_application>.<nom_hôte>.<alias_application>` à l'emplacement de votre choix.

e. Si le type sélectionné est *Serveur Jetty*, `dcstartup.bat/dcstartup.sh` est copié dans le répertoire de base de Jetty indiqué.

- Pour la version 8.1.4.0.7, procédez comme suit :
  - Si vous configurez le collecteur de données J2SE à l'aide d'Open JDK version 9 ou ultérieure et que vous entrez le chemin d'accès au répertoire de base Java, un avertissement dont le contenu est le suivant s'affiche :

Avertissement :

```
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by jnr.posix.JavaLibCHelper
(file:/root/testopen/preconf-13march/j2se_dc/.gdc/7.3.0.14.0/
bin/lib/jython.jar)to method sun.nio.ch.SelChImpl.getFD()
WARNING: Please consider reporting this to the maintainers of
jnr.posix.JavaLibCHelper
WARNING: Use --illegal-access=warn to enable warnings of next
illegal reflective access operations
WARNING: All illegal access operations will be denied in next
release Mar 15, 2019 11:35:06 AM
org.python.netty.util.internal.PlatformDependent <clinit>
INFO: Your platform does not provide complete lowlevel API for
accessing direct buffers reliably.
Unless explicitly requested, heap buffer is always preferred
to avoid potential system unstability.
```

Le collecteur de données J2SE fonctionne correctement et vous pouvez ignorer cet avertissement.

Pour la version 8.1.4.0.2 et antérieures, suivez l'étape 6 pour modifier le fichier Windows `dcstartup.bat` ou Linux AIX `dcstartup.sh`.

6. Pour modifier le fichier Windows `dcstartup.bat` ou Linux AIX `dcstartup.sh`, procédez comme suit :

- Si les classes et les fichiers JAR de l'application sont fournis dans un seul fichier JAR, procédez comme suit :

a. Ouvrez le fichier suivant :

- Windows `dcstartup.bat`
- Linux AIX `dcstartup.sh`

b. Remplacez `-cp .:$classpath:$Classpath $ITCAM_JVM_OPTS` *`nom complet de la classe principale`* par `$ITCAM_JVM_OPTS -jar` *`fichier jar de l'application`* et sauvegardez le fichier.

- Si l'application utilise plusieurs fichiers JAR, procédez comme suit :

  a. Ouvrez le fichier suivant :

  – Windows `dcstartup.bat`

  – Linux AIX `dcstartup.sh`

  b. Définissez la variable *CLASSPATH* sur les fichiers JAR.

  c. Remplacez `-cp .:$classpath:$Classpath $ITCAM_JVM_OPTS` *`nom complet de la classe principale`* par `-cp .:$classpath:$Classpath $ITCAM_JVM_OPTS -jar` *`fichier jar de l'application`* et sauvegardez le fichier.

  Le fichier JAR de l'application doit contenir la classe Main de cette dernière.

Remarque : Pour modifier le fichier Windows `dcstartup.bat` ou Linux AIX `dcstartup.sh` pour la version 8.1.4.0.3 à la version 8.1.4.0.5 et la version 8.1.4.0.6 et ultérieures (si le type d'application sélectionné est *Application Java*), suivez l'étape 7.

7. Suivez la procédure ci-dessous lorsque votre application utilise plusieurs fichiers JAR.

   a) Ouvrez le fichier suivant :

   - Windows `dcstartup.bat`
   - Linux AIX `dcstartup.sh`

   b) Définissez la variable *CLASSPATH* sur les fichiers JAR.

   c) Pour la version 8.1.4.0.7, si vous configurez le collecteur de données J2SE avec Java 9 ou 10 et si vous utilisez la connexion SSL pour la connectivité APM, les données Suivi des transactions ne s'affichent pas. Pour résoudre le problème, vous pouvez ajouter l'indicateur **--add-modules java.xml.bind** à la dernière ligne du fichier `dcstartup.bat` ou `dcstartup.sh`.

   Par exemple,

   - Si l'application est un fichier jar, mettez à jour la dernière ligne de la manière suivante :

   ```
   PathToJava --add-modules java.xml.bind --add-opens=

   jdk.management/com.sun.management.internal=

   ALL-UNNAMED -jar $Classpath $ITCAM_JVM_OPTS AppJarName.jar
   ```

   - Si l'application n'est pas intégrée dans un fichier jar, mettez à jour la dernière ligne de la manière suivante :

   ```
   PathToJava --add-modules java.xml.bind --add-opens=

   jdk.management/com.sun.management.internal=ALL-UNNAMED -cp
   .:$classpath:$Classpath $ITCAM_JVM_OPTS FullyQualifiedClassName
   ```

8. Pour activer le diagnostic approfondi, modifiez le fichier `custom_request.xml` avec les classes et les méthodes J2SE spécifiques que vous souhaitez surveiller. L'opération peut s'effectuer de deux manières : manuellement ou automatiquement.

   Pour remplir automatiquement la propriété `custom_request.xml` avec les classes et méthodes J2SE spécifiques de l'application :

   a) Accédez au répertoire `<DCHOME>/j2se_dc/.gdc/7.3.0.14.0/runtime/j2se<alias_application>.<nom_hôte>.<alias_application>/` et ouvrez le fichier `dc.properties`.

   b) Activez la propriété `is.auto.update.custom_requests.xml` en lui attribuant la valeur *true* et sauvegardez le fichier.

   c) Exécutez les commandes à partir de l'étape 9.

d) Arrêtez le collecteur de données après 10 à 15 minutes.

e) Vérifiez si la propriété DCHOME>/j2se_dc/.gdc/7.3.0.14.0/runtime/j2se<alias_application>.<nom_hôte>.<alias_application>/custom/custom_requests.xml est remplie avec les méthodes et classes personnalisées.

f) Supprimez les entrées indésirables et ouvrez à nouveau le fichier dc.properties.

g) Désactivez la propriété is.auto.update.custom_requests.xml en lui attribuant la valeur *false* et sauvegardez le fichier.

h) Exécutez les commandes à partir de l'étape 9.

Remarque : Si des méthodes personnalisées de l'application ne sont pas reconnues automatiquement, vous devez les ajouter manuellement.

Pour remplir manuellement la propriété custom_request.xml :

a) Accédez au répertoire <DCHOME>/j2se_dc/.gdc/7.3.0.14.0/runtime/j2se<alias_application>.<nom_hôte>.<alias_application>/custom/custom_requests.xml et modifiez custom_request.xml.

Par exemple,

```
<edgeRequest>
<requestName>truncateDb</requestName>
<Matches>testApp.JDBC.DBManager</Matches>
<type>application</type>
<methodName>truncateDb</methodName>
</edgeRequest>
```

b) Ajoutez les classes et les méthodes spécifiques de l'application.

9. Exécutez la commande suivante :

Windows `dcstartup.bat`

Linux AIX `dcstartup.sh`

Remarque : Si le type d'application sélectionné est *Serveur Jetty*, exécutez le script dcstartup.bat/dcstartup.sh qui se trouve dans le répertoire de base de Jetty.

L'application J2SE est démarrée avec le collecteur de données configuré.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par le collecteur de données dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console, voir «Démarrage de la console Cloud APM», à la page 1003.

Pour obtenir de l'aide sur le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Vérification du statut du suivi des transactions et de la collecte des données de diagnostic

Pour la version 8.1.0.3 et ultérieure, sur la page de configuration de l'agent, vous pouvez vérifier le statut du suivi des transactions et des données de diagnostic.

Pourquoi et quand exécuter cette tâche

Vous pouvez vérifier le statut du suivi des transactions et de la collecte des données de diagnostic à l'aide de deux commandes. Reportez-vous à la procédure pour en savoir plus sur les commandes associées.

Procédure

1. Utilisez la commande **config status**.

a) Ouvrez le répertoire bin. Exécutez la commande suivante :

Linux AIX **cd <DCHOME>/j2se_dc/.gdc/version_kit_outils/bin/**

Windows **cd <DCHOME>\j2se_dc\.gdc\version_kit_outils\bin**

Où *version_kit_outils* correspond à :

- Pour la version 8.1.4.0 et antérieure, *version_kit_outils* est 7.3.0.5.0.
- Pour la version 8.1.4.0.1 et ultérieure, *version_kit_outils* est 7.3.0.14.0.

b) Entrez la commande suivante pour vérifier le statut :

Linux AIX **config.sh status**

Windows **config.bat status**

c) Sélectionnez dans la liste les applications Java portant un nom d'alias qui sont identifiées pour vérifier leur statut, ou quittez.

1) ddperf
2) Main
3) Exit

2. Utilisez la commande **config status <nom_alias_application>**.

a) Entrez la commande suivante pour ouvrir un répertoire :

Linux AIX **cd <DCHOME>/j2se_dc/.gdc/7.3.0.14.0/bin/**

Windows **cd <DCHOME>\j2se_dc\.gdc\7.3.0.14.0\bin**

b) Entrez la commande suivante pour vérifier le statut :

Linux AIX **config.sh status <nom_alias_application>**

Windows **config.bat status <nom_alias_application>**

Changement du statut du suivi des transactions et de la collecte des données de diagnostic

Pour la version 8.1.0.3 et ultérieure, sur la page de configuration de l'agent, vous pouvez changer le statut du suivi des transactions et des données de diagnostic.

Pourquoi et quand exécuter cette tâche

Vous pouvez changer le statut du suivi des transactions et de la collecte des données de diagnostic à l'aide de l'invite de commande. Reportez-vous à la procédure suivante pour en savoir plus sur les commandes associées.

Procédure

1. Ouvrez le répertoire bin et exécutez la commande suivante :

Linux AIX **cd <DCHOME>/j2se_dc/.gdc/version_kit_outils/bin/**

Windows **cd <DCHOME>\j2se_dc\.gdc\version_kit_outils\bin**

Où *version_kit_outils* correspond à :

- Pour la version 8.1.4.0 et antérieure, *version_kit_outils* est 7.3.0.5.0.
- Pour la version 8.1.4.0.1 et ultérieure, *version_kit_outils* est 7.3.0.14.0.

2. Pour vérifier l'état, entrez la commande suivante :

Linux AIX **config.sh <nom_alias_application>**

Windows **config.bat <nom_alias_application>**

3. A l'invite, sélectionnez l'option permettant d'activer ou de désactiver le suivi des transactions. La valeur par défaut est Yes.
4. A l'invite, sélectionnez l'option permettant d'activer ou de désactiver la collecte des données de diagnostic. La valeur par défaut est Yes.
   a) Si vous définissez la valeur Yes, sélectionnez l'option permettant d'activer ou de désactiver la trace de méthode. La valeur par défaut est NO.

Configuration de la surveillance de JBoss

Monitoring Agent for JBoss surveille les ressources des serveurs d'applications JBoss et de la plateforme JBoss Enterprise Application. Utilisez les tableaux de bord fournis avec l'agent JBoss pour identifier les applications et les demandes les plus lentes, les goulots d'étranglement dans le pool d'unités d'exécution, les problèmes de segment de mémoire JVM et de récupération de place, les sessions les plus actives et les autres goulots d'étranglement sur le serveur d'applications JBoss.

Avant de commencer

- Les instructions figurant dans cette rubrique concernent l'édition la plus récente de l'agent, sauf indication contraire.
- Assurez-vous que votre environnement possède la configuration système requise pour l'agent JBoss. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent JBoss.
- Avant de configurer l'agent JBoss, le serveur JBoss doit d'abord être configuré en procédant comme suit :
  1. «Activer les connexions au serveur JMX MBean», à la page 469.
  2. «Ajouter un utilisateur de gestion de serveur JBoss», à la page 470.
  3. «Activation de la collecte des statistiques Web/HTTP», à la page 471. Cette procédure est applicable à JBoss EAP version 7.x et WildFly versions 8.x, 9.x et 10.x.

Pourquoi et quand exécuter cette tâche

Le nom de système géré inclut le nom d'instance que vous spécifiez, *nom_instance*:*nom_hôte*:*cp* par exemple, où *cp* est le code produit à deux caractères. Il est limité à 32 caractères.

Le nom d'instance que vous entrez est limité à 28 caractères, moins la longueur de votre nom d'hôte. Par exemple, si vous spécifiez JBoss comme nom d'instance, votre nom de système géré est JBoss:hostname:JE.

Remarque : Si vous indiquez un nom d'instance long, le nom du système géré est tronqué et le code d'agent ne s'affiche pas correctement.

L'agent JBoss est un agent multi-instance. Vous devez créer une instance d'agent pour chaque serveur JBoss que vous surveillez et démarrer chaque instance d'agent manuellement.

La fonction de suivi des transactions est disponible pour l'agent JBoss dans l'offre Cloud APM, Advanced.

- Pour activer le suivi des transactions pour une nouvelle instance d'agent, suivez l'étape 1 ou l'étape 2 de cette procédure, puis suivez la procédure de «Configuration du collecteur de données de suivi des transactions de l'agent agent JBoss», à la page 478.
- Pour activer le suivi des transactions pour une instance d'agent déjà configurée pour la surveillance de base, suivez la procédure de «Configuration du collecteur de données de suivi des transactions de l'agent agent JBoss», à la page 478.
- Pour désactiver le suivi des transactions pour une instance d'agent, suivez la procédure de «Désactivation du collecteur de données du suivi des transactions de l'agent JBoss», à la page 480.
- Pour désinstaller le suivi des transactions pour toutes les instances d'agent et supprimer le kit d'outils de suivi des transactions, suivez la procédure de «Désinstaller le suivi des transactions de l'agent JBoss», à la page 481.

Procédure

1. Configurez l'agent sur des systèmes Windows à l'aide de la fenêtre **IBM Performance Management** ou du fichier de réponses silencieux.
   - «Configuration de l'agent sur des systèmes Windows», à la page 472.
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 475.
2. Configurez l'agent sur des systèmes Linux en exécutant le script de ligne de commande et en répondant aux invites, ou à l'aide du fichier de réponses silencieux.
   - «Configuration de l'agent en répondant à des invites», à la page 474.
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 475.
3. Facultatif : Configurez le suivi des transactions en configurant des instances d'agent individuelles pour fournir les données de suivi des transactions et en configurant votre Tableau de bord d'Application Performance pour afficher les données de suivi des transactions.
   a) Suivez la procédure de «Configuration du collecteur de données de suivi des transactions de l'agent agent JBoss», à la page 478.
   b) Activez les données de suivi des transactions dans le Tableau de bord d'Application Performance pour l'agent JBoss.
      1) A partir de la barre de navigation, cliquez sur **Configuration système** > **Configuration d'agent**. La page **Configuration d'agent** s'affiche.
      2) Sélectionnez l'onglet **JBoss**.
      3) Sélectionnez les cases à cocher pour les instances de l'agent du serveur JBoss que vous souhaitez surveiller et effectuez l'une des actions suivantes figurant dans la liste **Actions** :
         - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Enabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour sur *Enabled*.
         - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Disabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour sur *Disabled*.
   c) Consultez les tableaux de bord des données de suivi des transaction de l'agent JBoss en ajoutant l'instance d'agent JBoss à une application dans votre Tableau de bord d'Application Performance.
      Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.
   d) Assurez-vous que des comptes utilisateur sont affectés à un rôle qui inclut les droits d'accès au Tableau de bord de diagnostic pour autoriser l'accès aux boutons suivants du Tableau de bord des applications pour le suivi des transactions de l'agent JBoss.
      Sinon, ces boutons sont désactivés pour ces utilisateurs dans le Tableau de bord des applications.
      1) Le bouton d'analyse détaillée **Diagnostiquer** sur le widget **Slowest 5 Response Time** (Temps de réponse - les 5 les plus lents).
      2) Le bouton **Inflight Requests** sur le widget **Applications**.

   Remarque : La fonction de suivi des transactions est disponible pour l'agent JBoss dans l'offre Cloud APM, Advanced. Pour l'agent JBoss avec la fonction de base de surveillance des ressources, présente dans l'offre Cloud APM, Base, ignorez cette étape.

Que faire ensuite

Dans la console Cloud APM, accédez à votre Tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux `/opt/ibm/apm/agent/logs`

- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Pour identifier et résoudre les incidents, reportez-vous au forum Cloud Application Performance Management.

Activer les connexions au serveur JMX MBean

Avant que l'agent JBoss puisse recueillir des données à partir du serveur JBoss, il faut que les connexions au serveur MBean Java Management Extensions (JMX) soient activées.

Procédure

Suivez les étapes correspondant à votre édition et version du serveur JBoss.

- Configurez EAP 5.2.

  Effectuez une copie de sauvegarde du fichier `run.conf`, puis ajoutez-y les lignes suivantes :

  ```
  JAVA_OPTS="$JAVA_OPTS -Djboss.platform.mbeanserver"
  JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote"
  JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.ssl=false"
  JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.authenticate=false"
  JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.port=1090"
  JAVA_OPTS="$JAVA_OPTS -Djavax.management.builder.initial=
                        org.jboss.system.server.jmx.MBeanServerBuilderImpl"
  ```

- Configurez AS 6.x.

  Indiquez l'adresse d'association comme paramètre lorsque vous démarrez le serveur JBoss.

  – Linux *rép_principal_serveur_jboss*`/bin/run.sh` **-b** `adresse_IP`

  – Windows *rép_principal_serveur_jboss*`\bin\run.bat` **-b** `<adresse_IP>`

  où *rép_principal_serveur_jboss* représente le répertoire d'installation du serveur JBoss.

  Par exemple, si l'adresse d'association est 10.77.9.250 :

  `/apps/wildfly-9.0.2.Final/bin/run.sh` **-b** `10.77.9.250`

- Configurez toutes les autres versions prises en charge.

  Les serveurs JBoss et WildFly sont installés avec leurs ports JMX désactivés pour la gestion à distance par défaut. Vous devez modifier la configuration du serveur JBoss pour autoriser la gestion à distance. Vous devez éditer le fichier *rép_principal_serveur_jboss*`/standalone/configuration/standalone.xml` pour autoriser la gestion à distance.

  a) Effectuez une copie de sauvegarde du fichier *rép_principal_serveur_jboss*`/standalone/configuration/standalone.xml`.

  Où *rép_principal_serveur_jboss* représente le répertoire d'installation du serveur JBoss.

  b) Autorisez la configuration à distance.

  Recherchez `urn:jboss:domain:jmx` et dans la section subsystem, vérifiez que l'entrée `remoting-connector` contient `use-management-endpoint="true"`.

  Exemple de résultat.

  ```
  <subsystem xmlns="urn:jboss:domain:jmx:1.3">
              <expose-resolved-model/>
              <expose-expression-model/>
              <remoting-connector use-management-endpoint="true"/>
  </subsystem>
  ```

  c) Autorisez les connexions à distance.

  Trouvez où les interfaces sont définies et remplacez 127.0.0.1 (bouclage) par l'IP externe sur le serveur avec lequel la connexion doit s'effectuer. Ne pas définir de connexion à 0.0.0.0.

  Exemple avant remplacement.

```
<interfaces>
      <interface name="management">
          <inet-address value="${jboss.bind.address.management:127.0.0.1}"/>
      </interface>
      <interface name="public">
          <inet-address value="${jboss.bind.address:127.0.0.1}"/>
      </interface>
...
```

Exemple après remplacement si l'adresse IP externe est 192.168.101.1.

```
<interfaces>
      <interface name="management">
          <inet-address value="${jboss.bind.address.management:192.168.101.1}"/>
      </interface>
      <interface name="public">
          <inet-address value="${jboss.bind.address:192.168.101.1}"/>
      </interface>
...
```

Ajouter un utilisateur de gestion de serveur JBoss

Avant que l'agent JBoss puisse recueillir des données à partir du serveur JBoss, un utilisateur de gestion doit être ajouté s'il n'en existe pas déjà un.

Procédure

Utilisez le script JBoss **add-user** pour ajouter un utilisateur de gestion.

1. Accédez au répertoire binaire ou `bin` sous le répertoire d'installation du serveur JBoss.
2. Exécutez le script **add-user**.
   - Linux **./add-user.sh**
   - Windows **add-user.bat**
3. Suivez les invites pour générer un utilisateur de gestion.

Exemple

```
root@jboss-wf10-rh7:/apps/wildfly-10.0.0.Final/bin
] ./add-user.sh

Quel type d'utilisateur souhaitez-vous ajouter ?
 a) Utilisateur de gestion (mgmt-users.properties)
 b) Utilisateur d'application (application-users.properties)
(a) : a

Entrez les détails du nouvel utilisateur à ajouter.
Utilisez le domaine 'ManagementRealm' tel qu'il a été découvert à partir des fichiers de
propriétés existants.
Nom d'utilisateur : MyAdmin
Les recommandations relatives au mot de passe sont indiquées ci-dessous. Pour modifier ces
restrictions, modifiez le fichier de configuration add-user.properties
.
 - Le mot de passe doit être différent du nom d'utilisateur.
 - Le mot de passe ne doit pas être l'une des valeurs restreintes suivantes {root, admin,
administrateur}
 - Le mot de passe doit contenir au moins 8 caractères, 1 caractère alphabétique, 1 caractère
numérique,
1 symbole non alphanumérique
Mot de passe :
Entrer à nouveau le mot de passe :
A quel groupe souhaitez-vous que cet utilisateur appartienne ? (Veuillez entrer une liste
séparée par des virgules, ou laissez en blanc
pour n'en indiquer aucun)[  ] :
En ce qui concerne l'ajout de l'utilisateur 'MyAdmin' pour le domaine 'ManagementRealm'
Est-ce correct, oui/non ? oui
Utilisateur 'MyAdmin' ajouté au fichier '/apps/wildfly-10.0.0.Final/standalone/configuration/
mgmt-users.properties'
Utilisateur 'MyAdmin' ajouté au fichier '/apps/wildfly-10.0.0.Final/domain/configuration/mgmt-
users.properties'
Utilisateur 'MyAdmin' ajouté avec des groupes au fichier
           '/apps/wildfly-10.0.0.Final/standalone/configuration/mgmt-groups.properties'
```

```
Utilisateur 'MyAdmin' ajouté avec des groupes au fichier
           '/apps/wildfly-10.0.0.Final/domain/configuration/mgmt-groups.properties'
Ce nouvel utilisateur va-t-il être utilisé pour qu'un processus AS se connecte à un autre
processus AS ?
Par exemple, pour qu'un contrôleur d'hôte esclave se connecte au maître ou pour l'exécution
d'une connexion à distance pour les appels EJB de serveur
à serveur.
oui/non ? non
```

Activation de la collecte des statistiques Web/HTTP

Avant que l'agent JBoss ne puisse recueillir les mesures Web du serveur JBoss et les mesures des autres sous-systèmes, la collecte des statistiques doit être activée pour chaque sous-système. Cette procédure est applicable à JBoss EAP version 7.x et WildFly versions 8.x, 9.x et 10.x.

Procédure

L'attribut **statistics-enabled** des divers sous-systèmes JBoss contrôle la collecte des statistiques. Il peut être affiché et mis à jour à l'aide de l'interface de ligne de commande JBoss.

Remarque : Cette procédure est applicable à JBoss EAP version 7.x et WildFly versions 8.x, 9.x et 10.x.

1. Accédez au répertoire binaire ou `bin` sous le répertoire d'installation du serveur JBoss.
2. Démarrez l'interface de ligne de commande JBoss.
   - Linux **./jboss-cli.sh --connect** [**--controller**=*IP*:*port*]
   - Windows **jboss-cli.bat --connect** [**--controller**=*IP*:*port*]

   où *IP* représente l'adresse IP du serveur JBoss et *port*, le port du serveur JBoss. Par exemple, `192.168.10.20:9990`.

   Conseil : si la tentative de connexion se solde par un échec, "`Echec de la connexion au contrôleur : Le contrôleur n'est pas disponible à localhost:9990. La connexion a échoué : WFLYPRT0053 : Echec de la connexion à http-remoting://localhost:9990. Echec de la connexion : Connexion refusée`", utilisez le paramètre **--controller**.

   Cette erreur indique que le serveur de gestion n'est pas en mode écoute sur l'adresse IP du système hôte local (127.0.0.1) et qu'il est configuré pour être en mode écoute sur l'adresse IP de l'ordinateur.
3. Exécutez les commandes suivantes pour afficher l'état actuel de l'attribut statistics-enabled de chaque sous-système :

   Remarque : Si JBoss est exécuté en mode de domaine, les commandes doivent avoir pour préfixe le profil associé et elles doivent être exécutées pour chaque profil surveillé. Par exemple : `/profile=full/subsystem=ejb3:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`ejb3`**`:read-attribute(name=enable-statistics)`

   `/subsystem=`**`transactions`**`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`undertow`**`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`webservices`**`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`datasources/data-source`**`=`*`nom_source_données`*`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`datasources/data-source`**`=`*`nom_source_données`*`/`**`statistics=pool`**`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`datasources/data-source`**`=`*`nom_source_données`*`/`**`statistics=jdbc`**`:read-attribute(name=statistics-enabled)`

   où *nom_source_données* représente le nom d'une source de données configurée pour être utilisée avec JBoss.

Remarque : les sources de données peuvent être répertoriées à l'aide de la commande `/subsystem=datasources:read-resource`.

Exemple de résultat lorsque les statistiques ne sont pas activées :

```
{
    "outcome" => "success",
    "result" => false
}
```

4. Exécutez la commande suivante pour remplacer la valeur de l'attribut statistics-enabled de chaque sous-système par *true* :

   `/subsystem=`**`ejb3`**`:write-attribute(name=enable-statistics, value=true)`

   `/subsystem=`**`transactions`**`:write-attribute(name=statistics-enabled,value=true)`

   `/subsystem=`**`undertow`**`:write-attribute(name=statistics-enabled,value=true)`

   `/subsystem=`**`webservices`**`:write-attribute(name=statistics-enabled,value=true)`

   `/subsystem=`**`datasources/data-source`**`=`*`nom_source_données`*`:write-attribute(name=statistics-enabled,value=true)`

   `/subsystem=`**`datasources/data-source`**`=`*`nom_source_données`*`/`**`statistics=pool`**`:write-attribute(name=statistics-enabled,value=true)`

   `/subsystem=`**`datasources/data-source`**`=`*`nom_source_données`*`/`**`statistics=jdbc`**`:write-attribute(name=statistics-enabled,value=true)`

   Exemple de résultat lorsque vous activez les statistiques d'un sous-système :

```
{
    "outcome" => "success",
    "response-headers" => {
        "operation-requires-reload" => true,
        "process-state" => "reload-required"
    }
}
```

5. Quittez l'interface de ligne de commande JBoss.
6. Redémarrez le serveur JBoss.

   Remarque : Les agents JBoss en cours d'exécution avec le suivi des transactions activé doivent être redémarrés.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent JBoss sur les systèmes d'exploitation Windows dans la fenêtre IBM Cloud Application Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **Agents IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur le modèle **Monitoring Agent for JBoss**, puis cliquez sur **Configure agent**.

   A faire : Après avoir configuré une instance d'agent pour la première fois, l'option **Configure agent** est désactivée. Pour reconfigurer l'instance d'agent, cliquez dessus avec le bouton droit de la souris et sélectionnez **Reconfigure**.
3. Entrez un nom d'instance unique, puis cliquez sur **OK**. N'utilisez que des lettres, des chiffres arabes, le caractère de soulignement et le caractère moins dans le nom de l'instance.
   Par exemple, `jboss01`.

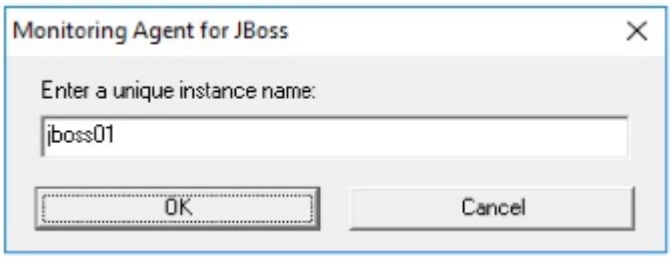


Figure 17. Fenêtre de saisie d'un nom d'instance unique.

4. Entrez les paramètres du serveur JBoss, puis cliquez sur **Suivant**.
   Pour obtenir une description de chaque paramètre de configuration, voir Tableau 167, à la page 477.

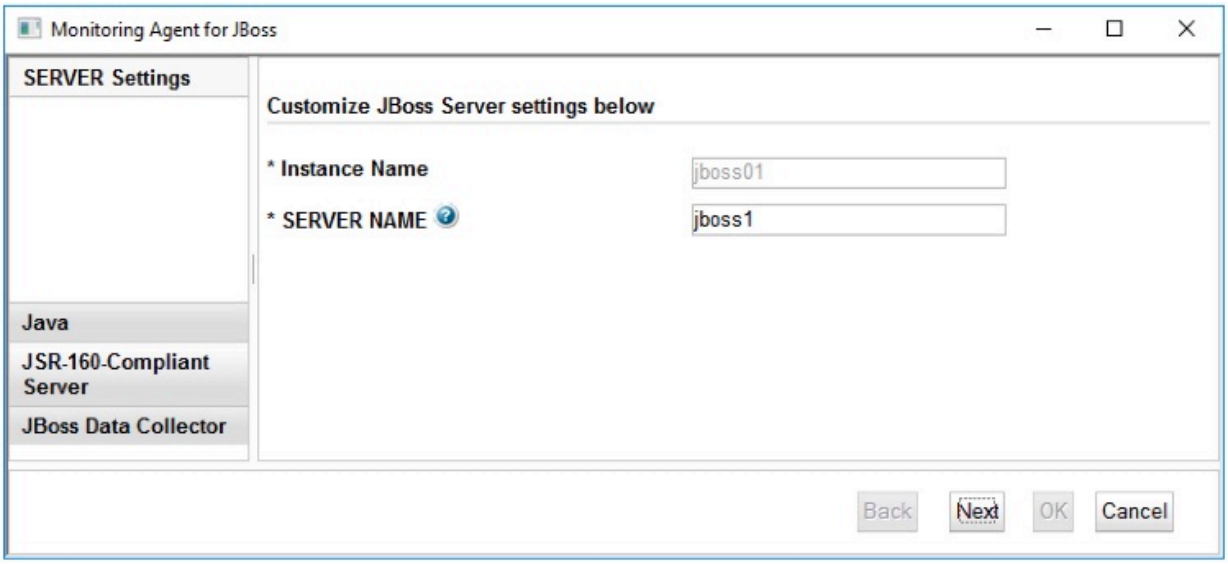


Figure 18. Fenêtre des paramètres de configuration pour le serveur JBoss

5. Entrez les paramètres Java, puis cliquez sur **Suivant**.
   Pour obtenir une description de chaque paramètre de configuration, voir Tableau 167, à la page 477.

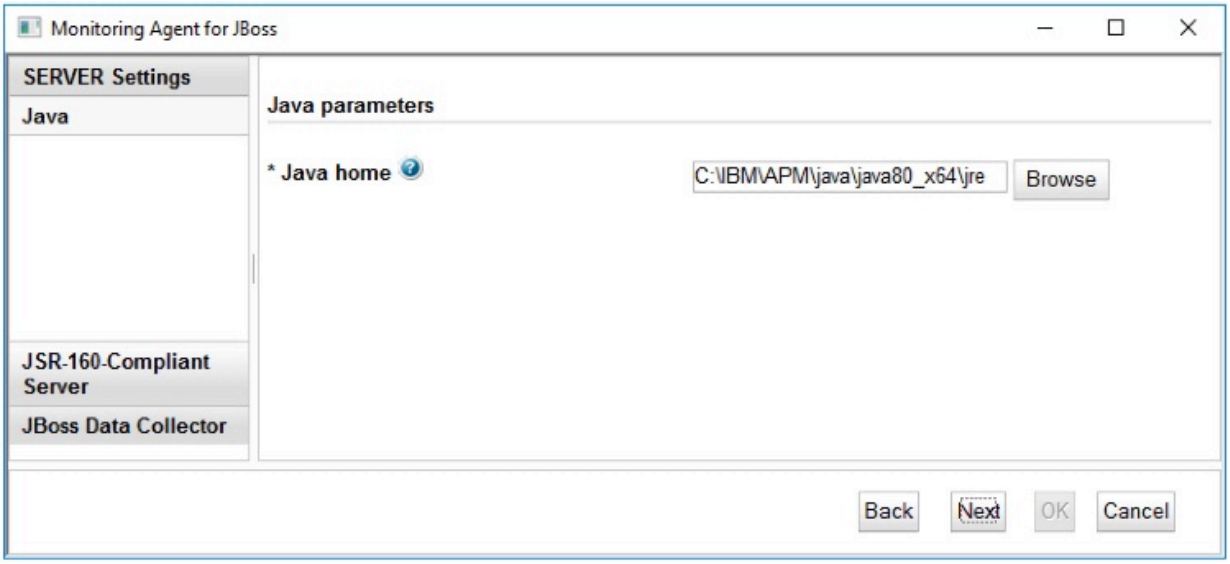


Figure 19. Fenêtre de spécification des paramètres Java.

6. Entrez les paramètres JMX, puis cliquez sur **Suivant**.
   Pour obtenir une description de chaque paramètre de configuration, voir Tableau 167, à la page 477.

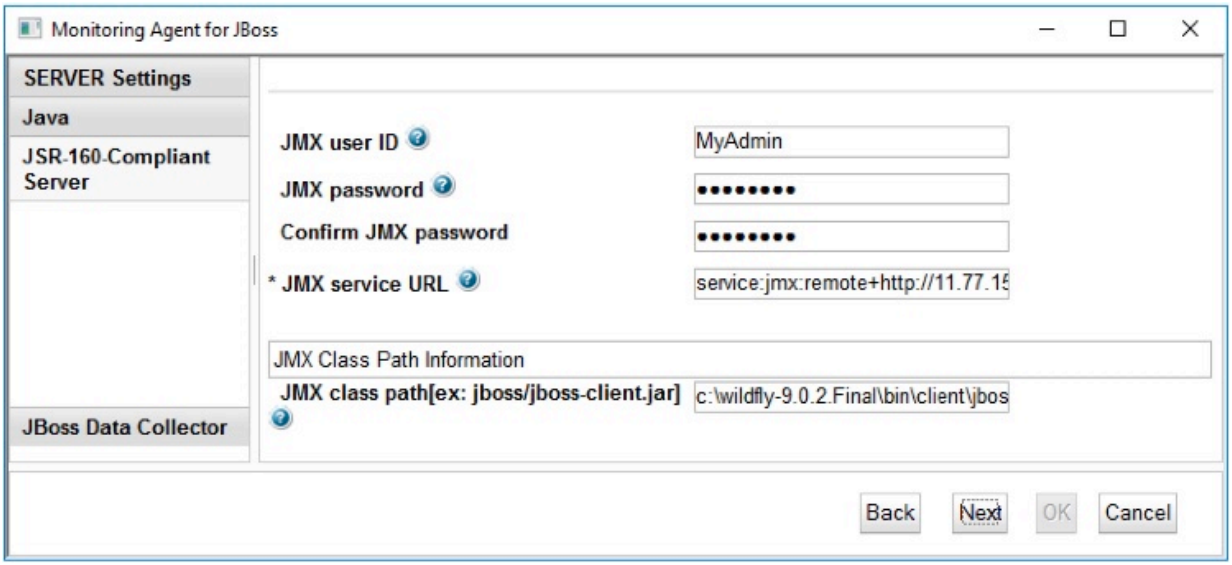


Figure 20. Fenêtre de spécification des paramètres JMX.

7. Affichez les paramètres du collecteur de données d'agent de l'agent JBoss.

   Laissez le paramètre **`DC Runtime Directory`** vide lors de la configuration initiale de l'agent. Pour obtenir une description de chaque paramètre de configuration, voir Tableau 167, à la page 477.

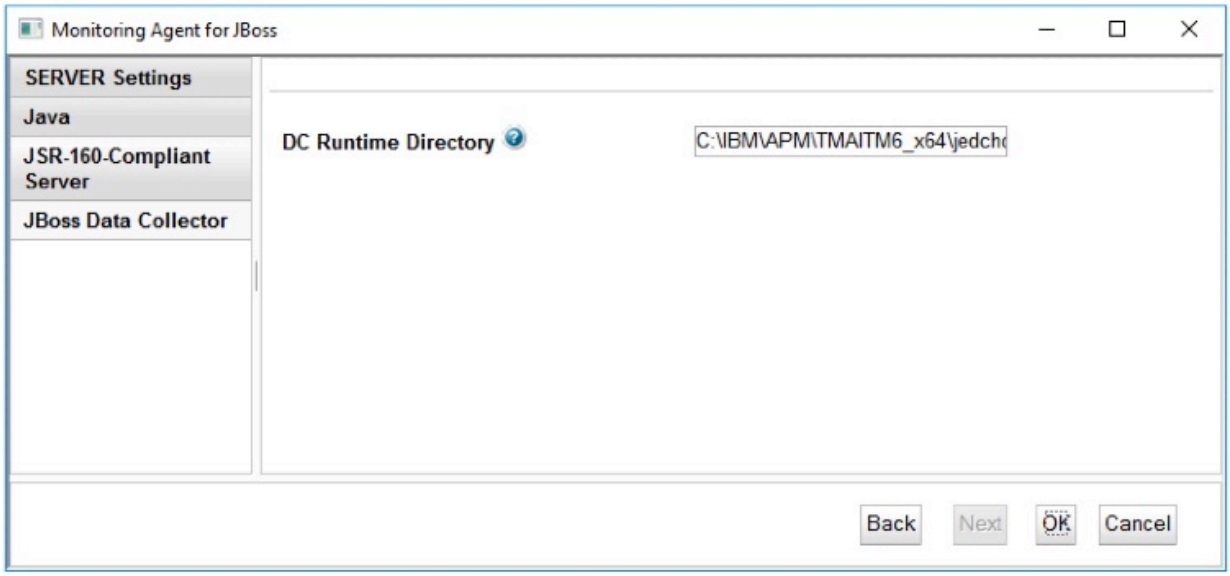


Figure 21. Fenêtre de spécification des paramètres du collecteur de données de l'agent JBoss

8. Cliquez sur **OK** pour terminer la configuration de l'agent.
9. Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur l'instance que vous avez configurée, puis cliquez sur **Démarrer**.

Configuration de l'agent en répondant à des invites

Après avoir installé l'agent JBoss, vous devez le configurer pour pouvoir le démarrer. Si l'agent JBoss est installé sur un ordinateur Linux ou UNIX local, vous pouvez suivre ces instructions pour le configurer de manière interactive en suivant des invites de ligne de commande.

Pourquoi et quand exécuter cette tâche

A faire : Si vous reconfigurez une instance d'agent configurée, la valeur définie dans la dernière configuration s'affiche pour chaque paramètre. Pour effacer une valeur existante, appuyez sur la touche Espace lorsque le paramètre s'affiche.

Procédure

1. A partir d'une ligne de commande, exécutez la commande suivante :

   ```
   rép_install/bin/jboss-agent.sh config
   nom_instance
   ```

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent.

   Exemple

   ```
   /opt/ibm/apm/agent/bin/jboss-agent.sh config example-inst01
   ```

2. Répondez aux invites pour définir les valeurs de configuration de l'agent.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'agent JBoss», à la page 477.

3. Exécutez la commande suivante pour démarrer l'agent :

   ```
   rép_install/bin/jboss-agent.sh start
   nom_instance
   ```

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

   Exemple

   ```
   /opt/ibm/apm/agent/bin/jboss-agent.sh start example-inst01
   ```

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

- Pour configurer l'agent JBoss en mode silencieux, procédez comme suit :
  a) Dans un éditeur de texte, ouvrez le fichier `jboss_silent_config.txt` disponible à l'emplacement suivant :
  – Linux AIX *rép_install*`/samples/jboss_silent_config.txt`

    Par exemple, `/opt/ibm/apm/agent/samples/jboss_silent_config.txt`
  – Windows *rép_install*`\samples\jboss_silent_config.txt`

    où *rép_install* représente le chemin d'installation de l'agent.

    Les chemins d'accès *rép_install* par défaut sont répertoriés ici :
  – Linux `/opt/ibm/apm/agent`
  – Windows `C:\IBM\APM\TMAITM6_x64`

Exemple

Linux AIX
```
/opt/ibm/apm/agent/samples/jboss_silent_config.txt
```

Windows
```
C:\IBM\APM\samples\jboss_silent_config.txt
```

b) Dans le fichier `jboss_silent_config.txt`, indiquez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.

Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'agent JBoss», à la page 477.

c) Sauvegardez et fermez le fichier `jboss_silent_config.txt`, puis exécutez la commande suivante :

– Linux AIX *rép_install*`/bin/jboss-agent.sh config` **nom_instance** *rép_install*`/samples/jboss_silent_config.txt`

– Windows *rép_install*`\bin\jboss-agent.bat config` **nom_instance** *rép_install*`\samples\jboss_silent_config.txt`

où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

Les chemins d'accès *rép_install* par défaut sont répertoriés ici :

– Linux `/opt/ibm/apm/agent`

– Windows `C:\IBM\APM\TMAITM6_x64`

Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.

Exemple

Linux AIX
```
/opt/ibm/apm/agent/bin/jboss-agent.sh config example-inst01
/opt/ibm/apm/agent/samples/jboss_silent_config.txt
```

Windows
```
C:\IBM\APM\bin\jboss-agent.bat config example-inst01 C:\IBM\APM\samples
\jboss_silent_config.txt
```

d) Exécutez la commande suivante pour démarrer l'agent :

– Linux AIX *rép_install*`/bin/jboss-agent.sh start` **nom_instance**

– Windows *rép_install*`\bin\jboss-agent.bat start` **nom_instance**

où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

Les chemins d'accès *rép_install* par défaut sont répertoriés ici :

– Linux `/opt/ibm/apm/agent`

– Windows `C:\IBM\APM\TMAITM6_x64`

Exemple

Linux AIX
```
/opt/ibm/apm/agent/bin/jboss-agent.sh start example-inst01
```

Windows
```
C:\IBM\APM\bin\jboss-agent.bat start example-inst01
```

Paramètres de configuration de l'agent JBoss

Les paramètres de configuration de l'agent JBoss sont regroupés dans un tableau.

1. Paramètres de l'agent JBoss - Paramètres de l'environnement de l'agent JBoss.
2. Tableau 168, à la page 477 - Exemples d'adresses URL de service de JMX.

Tableau 167. Paramètres de l'agent JBoss

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
nom de serveur	Indiquez un nom pour identifier le serveur JBoss/WildFly.	**KJE_SERVER**
Accueil Java	Chemin d'accès où Java est installé.	**JAVA_HOME**
ID utilisateur JMX	ID utilisateur pour la connexion au serveur MBean.	**KQZ_JMX_JSR160_JSR160_USER_ID**
Mot de passe JMX	Mot de passe	**KQZ_JMX_JSR160_JSR160_PASSWORD**
Adresse URL de service JMX	Adresse URL de service pour la connexion au serveur MBean. Voir Tableau 168, à la page 477 pour obtenir des exemples.	**KQZ_JMX_JSR160_JSR160_SERVICE_URL**
Chemin d'accès aux classes JMX	Fichiers JAR dans lesquels sont recherchées les localisations d'une classe ou d'une ressource. Localisez et entrez le chemin d'accès au fichier `jboss-client.jar` pour votre serveur JBoss. Exemple pour un serveur JBoss EAP 6 : `/opt/EAP-6.3.0/jboss-eap-6.3/bin/client/jboss-client.jar`.	**KQZ_JMX_JSR160_JSR160_JAR_FILES**
Répertoire d'exécution DC	**Remarque :** Ce paramètre concerne uniquement l'agent JBoss avec la fonction de suivi des transactions, qui fait partie de l'offre de Cloud APM, Advanced. Pour l'agent JBoss avec la fonction de base de surveillance des ressources, présente dans l'offre Cloud APM, Base, ignorez ce paramètre. Le chemin d'accès complet au répertoire d'exécution du collecteur de données JBoss est défini par le script **`simpleConfig`**. Laissez ce paramètre vide lors de la configuration initiale de l'agent.	**KQZ_DC_RUNTIME_DIR**

Tableau 168. Adresse URL de service JMX

Version du serveur JBoss	Adresse URL de service JMX avec un port par défaut[1]
WildFly 8, 9 et 10 JBoss EAP 7	`service:jmx:remote+http://ip:9990` `service:jmx:remote+https://ip:9994`

Tableau 168. Adresse URL de service JMX (suite)	
Version du serveur JBoss	**Adresse URL de service JMX avec un port par défaut[1]**
JBoss EAP 6 JBoss AS 7	`service:jmx:remoting-jmx://ip:9999`
JBoss EAP 5.2 JBoss AS 6.1	`service:jmx:rmi:///jndi/rmi://ip:1090/jmxrmi`

[1] Le port est défini en fonction du port contenu dans l'entrée suivante du fichier de configuration de JBoss : `<socket-binding name="management-native" interface="management" port="${jboss.management.native.port:`*NNNN*`}"/>`. Si la valeur par défaut du port a été modifiée, redéfinissez-la sur le numéro de port contenu dans votre fichier de configuration.

Configuration du collecteur de données de suivi des transactions de l'agent agent JBoss

La fonction de suivi des transactions de l'agent JBoss requiert des modifications dans le fichier des paramètres d'environnement de l'instance d'agent, le fichier de démarrage du serveur JBoss et le paramètre de configuration de l'agent DC Runtime Directory. Un script est fourni pour vous aider à apporter ces modifications.

Avant de commencer

Linux Vérifiez que la limite de ressource pour les fichiers ouverts est supérieure à 5 000 pour que le kit d'outils de suivi des transactions fonctionne correctement.

- Affichez le paramètre de limite de fichiers ouverts en cours. **`ulimit -n`**
- Exemple de paramètre définissant la limite de fichiers ouverts à 5 056. **`ulimit -n 5056`**

Effectuez l'étape Configuration de l'agent JBoss «1», à la page 468 ou «2», à la page 468 avant de suivre cette procédure.

L'agent JBoss doit être installé en local sur le serveur JBoss surveillé avec la fonction de suivi des transactions.

Le compte utilisateur qui exécute ce script doit disposer de droits en écriture aux répertoires et fichiers suivants :

1. Répertoire *JBOSS_HOME*.
2. Répertoire *JBOSS_HOME*`/bin` et ses fichiers.
3. Fichier *JBOSS_HOME*`/modules/system/layers/base/org/jboss/as/server/main/module.xml`.
4. Répertoire *rép_install*`/config`.
5. Fichier *rép_install*`/config/`*nom_hôte*`_je_`*nom_instance*`.cfg`.

où

JBOSS_HOME
Répertoire d'installation du serveur JBoss.

rép_install
Chemin d'installation de l'agent. Le chemin d'accès par défaut est :

- Linux `/opt/ibm/apm/agent`
- Windows `C:\IBM\APM\TMAITM6_x64`

nom_hôte
Nom de l'ordinateur hôte sur lequel l'agent est installé.

nom_instance
Nom de l'instance d'agent affectée dans la rubrique sur la méthode de configuration de l'agent :

- Configuration de l'agent sur des systèmes Windows, étape «3», à la page 472
- Configuration de l'agent en répondant à des invites, étape «1», à la page 475
- Configuration de l'agent à l'aide du fichier de réponses silencieux, étape «3», à la page 476

Procédure

Exécutez le script **simpleConfig**.

1. Connectez-vous au serveur JBoss sur lequel l'agent JBoss est installé.
2. Accédez au répertoire du répertoire d'installation de l'agent.
   - Linux *rép_install*
   - Windows *rép_install*\TMAITM6_x64

   où *rép_install* représente le chemin d'installation de l'agent.

   Les chemins d'accès *rép_install* par défaut sont répertoriés ici :
   - Linux /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64
3. Accédez au répertoire jedchome/7.3.0.13.0/bin.
4. Exécutez le script d'installation.
   - Linux ./simpleConfig.sh
   - Windows simpleConfig.bat
5. Suivez les invites pour entrer des paramètres pour votre environnement :
   a) Entrez le *nom_instance* de l'instance d'agent JBoss choisie.
   b) Entrez le répertoire d'installation du serveur JBoss.
      Si la variable d'environnement *JBOSS_HOME* est définie, sa valeur sera proposée comme valeur par défaut.

   où

   JBOSS_HOME
   Répertoire d'installation du serveur JBoss.

   nom_instance
   Nom de l'instance d'agent affectée dans la rubrique sur la méthode de configuration de l'agent :
   - Configuration de l'agent sur des systèmes Windows, étape «3», à la page 472
   - Configuration de l'agent en répondant à des invites, étape «1», à la page 475
   - Configuration de l'agent à l'aide du fichier de réponses silencieux, étape «3», à la page 476

   rép_install
   Chemin où l'agent est installé. Le chemin d'accès par défaut est :
   - Linux /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64
6. Redémarrez l'agent et le serveur JBoss s'ils sont en cours d'exécution.

Résultats

Fichiers du serveur JBoss modifiés lors de la configuration du suivi des transactions :

- *JBOSS_HOME*/bin/standalone.conf

  Ce fichier est mis à jour avec les paramètres de configuration requis pour la fonction de suivi des transactions. Des repères de configuration sont insérés dans le fichier pour pouvoir être utilisés lorsque vous désactivez la fonction de suivi des transactions. Un fichier de sauvegarde est sauvegardé dans le

répertoire *JBOSS_HOME*/bak avant l'ajout ou la suppression de modifications de la fonction de suivi des transactions.

- *JBOSS_HOME*/modules/system/layers/base/org/jboss/as/server/main/module.xml

  Ce fichier est mis à jour avec une dépendance de module d'API JAVA EE. Des repères de configuration sont insérés dans le fichier pour pouvoir être utilisés lorsque vous désactivez la fonction de suivi des transactions. Un fichier de sauvegarde est sauvegardé dans le répertoire *JBOSS_HOME*/bak avant l'ajout ou la suppression de modifications de la fonction de suivi des transactions.

Fichiers de l'agent modifiés lors de la configuration du suivi des transactions :

- Fichier de configuration de l'instance d'agent
  - Linux *rép_install*/config/*nom_hôte*_je_*nom_instance*.cfg
  - Windows *rép_install*\TMAITM6_x64*nom_hôte*_JE_*nom_instance*.cfg
- Fichier des paramètres d'environnement de l'agent
  - Linux *rép_install*/config/je_*nom_instance*.environment
  - Windows *rép_install*\TMAITM6_x64\KJEENV_*nom_instance*

où

JBOSS_HOME
Répertoire d'installation du serveur JBoss.

rép_install
Chemin d'installation de l'agent. Le chemin d'accès par défaut est :

- Linux /opt/ibm/apm/agent
- Windows C:\IBM\APM\TMAITM6_x64

nom_hôte
Nom de l'ordinateur hôte sur lequel l'agent est installé.

nom_instance
Nom de l'instance d'agent affectée dans la rubrique sur la méthode de configuration de l'agent :

- Configuration de l'agent sur des systèmes Windows, étape «3», à la page 472
- Configuration de l'agent en répondant à des invites, étape «1», à la page 475
- Configuration de l'agent à l'aide du fichier de réponses silencieux, étape «3», à la page 476

Désactivation du collecteur de données du suivi des transactions de l'agent JBoss
La fonction de suivi des transactions de l'agent JBoss requiert des modifications dans le fichier des paramètres d'environnement de l'instance d'agent, le fichier de démarrage du serveur JBoss et le paramètre de configuration de l'agent DC Runtime Directory. Un script est fourni pour supprimer ces modifications pour une instance d'agent dont le suivi des transactions est activé.

Avant de commencer

Assurez-vous que le serveur JBoss et l'agent JBoss sont arrêtés.

Le compte utilisateur qui exécute ce script doit disposer de droits en écriture aux répertoires et fichiers suivants :

1. Répertoire *JBOSS_HOME*
2. Répertoire et fichiers *JBOSS_HOME*/bin
3. Fichier *JBOSS_HOME*/modules/system/layers/base/org/jboss/as/server/main/module.xml
4. Répertoire *rép_install*/config
5. Fichier *rép_install*/config/*nom_hôte*_je_*nom_instance*.cfg

Procédure

Exécutez le script **simpleConfig** avec l'option **remove**.

1. Connectez-vous au serveur JBoss sur lequel l'agent JBoss est installé.
2. Accédez au répertoire du répertoire d'installation de l'agent.
   - Linux *rép_install*
   - Windows *rép_install*\TMAITM6_x64
3. Accédez au répertoire jedchome/7.3.0.13.0/bin.
4. Exécutez le script **simpleConfig** avec l'option **remove**.
   - Linux ./simpleConfig.sh **remove** *nom_instance*
   - Windows simpleConfig.bat **remove** *nom_instance*
5. Démarrez l'agent et le serveur JBoss.

   Où :

   JBOSS_HOME
   Répertoire d'installation du serveur JBoss

   nom_hôte
   Nom de l'ordinateur hôte sur lequel l'agent est installé

   nom_instance
   Nom de l'instance d'agent affectée dans la rubrique sur la méthode de configuration de l'agent :
   - Configuration de l'agent sur des systèmes Windows, étape «3», à la page 472
   - Configuration de l'agent en répondant à des invites, étape «1», à la page 475
   - Configuration de l'agent à l'aide du fichier de réponses silencieux, étape «3», à la page 476

   rép_install
   Chemin où l'agent est installé. Le chemin d'accès par défaut est :
   - Linux /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64

   architecture
   Identificateur de l'architecture système d'IBM Application Performance Management ou de Cloud APM. Par exemple, lx8266 représente Linux Intel version 2.6 (64 bits). Pour obtenir la liste complète des codes d'architecture, voir le fichier *rép_install*/registry/archdsc.tbl.

Désinstaller le suivi des transactions de l'agent JBoss

La fonction de suivi des transactions de l'agent JBoss peut être désinstallée. Un script est fourni pour supprimer toutes les instances d'agent dont le suivi des transactions est activé et le kit d'outils du suivi des transactions.

Avant de commencer

Assurez-vous que le serveur JBoss et toutes les instances d'agent JBoss sont arrêtés.

Le compte utilisateur qui exécute ce script doit disposer de droits d'accès en écriture aux répertoires et fichiers suivants :

1. Répertoire *JBOSS_HOME*.
2. Répertoire *JBOSS_HOME*/bin et ses fichiers.
3. Fichier *JBOSS_HOME*/modules/system/layers/base/org/jboss/as/server/main/module.xml.
4. Répertoire *rép_install*/config.
5. Fichier *rép_install*/config/*nom_hôte*_je_*nom_instance*.cfg.

Procédure

Exécutez le script **simpleConfig** avec l'option **uninstall**.

1. Connectez-vous au serveur JBoss sur lequel l'agent JBoss est installé.
2. Accédez au répertoire du répertoire d'installation de l'agent.
   - Linux *rép_install*/*architecture*/je/bin. Par exemple : /opt/ibm/apm/agent/lx8266/je/bin ou /opt/ibm/apm/agent/lx8266/je/bin
   - Windows *rép_install*\TMAITM6_x64
3. Accédez au répertoire jedchome/7.3.0.13.0/bin.
4. Exécutez le script **simpleConfig** avec l'option **uninstall**.
   - Linux ./simpleConfig.sh **uninstall**
   - Windows simpleConfig.bat **uninstall**
5. Démarrez le serveur JBoss et toutes les instances d'agent.

Où :

JBOSS_HOME
Répertoire d'installation du serveur JBoss.

nom_hôte
Nom de l'ordinateur hôte sur lequel l'agent est installé.

nom_instance
Nom de l'instance d'agent affectée dans la rubrique sur la méthode de configuration de l'agent :

- Configuration de l'agent sur des systèmes Windows, étape «3», à la page 472
- Configuration de l'agent en répondant à des invites, étape «1», à la page 475
- Configuration de l'agent à l'aide du fichier de réponses silencieux, étape «3», à la page 476

rép_install
Chemin où l'agent est installé. Le chemin d'accès par défaut est :

- Linux /opt/ibm/apm/agent
- Windows C:\IBM\APM\TMAITM6_x64

architecture
Identificateur de l'architecture système d'IBM Application Performance Management ou de Cloud APM. Par exemple, lx8266 représente Linux Intel version 2.6 (64 bits). Pour obtenir la liste complète des codes d'architecture, voir le fichier *rép_install*/registry/archdsc.tbl.

Configuration de la surveillance de Linux KVM

Vous devez configurer Monitoring Agent for Linux KVM pour collecter les données des serveurs Red Hat Enterprise Virtualization Hypervisor (RHEVH) et Red Hat Enterprise Virtualization Manager (RHEVM). Une fois que vous avez installé l'agent sur un serveur ou une machine virtuelle, vous devez créer la première instance et démarrer l'agent manuellement.

Avant de commencer
Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Linux KVM.

Pourquoi et quand exécuter cette tâche
L'agent Linux KVM est un agent multi-instance et à connexions multiples. Multi-instance signifie que vous pouvez créer plusieurs instances et que chaque instance peut établir plusieurs connexions à un ou plusieurs serveurs RHEVM ou RHEVH.

A faire : Utilisez des instances différentes pour surveiller les serveurs RHEVM ou RHEVH.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Vous pouvez utiliser le même script de configuration afin de configurer des instances pour les serveurs RHEVH et RHEVM :

- Pour configurer une connexion au serveur de RHEVM, effectuez les étapes décrites dans la section "Configuration d'une connexion au serveur RHEVM".
- Pour configurer une connexion au serveur de RHEVH, effectuez les étapes décrites dans la section "Configuration d'une connexion au serveur RHEVH".

Création d'un utilisateur et attribution des droits nécessaires

Avant de configurer l'agent Linux KVM, vous devez créer un utilisateur et lui accorder les droits appropriés lui permettant de surveiller les serveurs RHEVM et RHEVH.

Procédure

1. Ouvrez le portail **Red Hat Enterprise Virtualization Manager Web Administration**.
2. Cliquez sur **Configure**.
3. Dans la fenêtre **Configuration**, sélectionnez **Roles**.
   a) Pour créer un rôle, cliquez sur **New**.
   b) Dans la fenêtre **New role**, ajoutez le nom du rôle et sélectionnez **Admin** comme type de compte.
   c) Assurez-vous que les cases à cocher du panneau **Check boxes to Allow Action** ne sont pas sélectionnées, et cliquez sur **OK**.
4. Dans la fenêtre **Configuration**, sélectionnez **System Permission**.
   a) Pour accorder un droit utilisateur, cliquez sur **Add**.
   b) Dans la fenêtre **Add System Permission to User**, sélectionnez l'utilisateur auquel vous souhaitez accorder le droit.
   c) Dans la liste **Assign role to user**, sélectionnez le rôle que vous avez créé et cliquez sur **OK**.

Que faire ensuite

Effectuez la configuration de l'agent :

- «Configuration d'une connexion au serveur RHEVH», à la page 489
- «Configuration d'une connexion au serveur RHEVM», à la page 488

Configuration des protocoles

L'agent utilise différents protocoles pour la connexion au serveur RHEVH. Vous pouvez configurer l'un de ces protocoles : SSH, TLS ou TCP.

Pourquoi et quand exécuter cette tâche

L'agent Linux KVM se connecte à distance à chaque hyperviseur à l'aide de l'outil **`virsh`** qui gère vos machines virtuelles QEMU-KVM, et il collecte les mesures. L'API `libvirt` de l'environnement d'agent utilise plusieurs protocoles de transport à distance différents. Pour obtenir la liste des protocoles pris en charge, voir la Remote support page (page de support à distance).

Configuration du protocole SSH
Vous pouvez configurer le protocole SSH pour surveiller un hôte à distance.

Pourquoi et quand exécuter cette tâche
Supposition : L'agent Linux KVM est installé sur l'hôte A. Vous souhaitez surveiller à distance l'hyperviseur sur l'hôte B.

Procédure

1. Connectez-vous à l'hôte A en utilisant le même ID utilisateur que celui avec lequel le processus de l'agent Linux KVM est exécuté, par exemple, l'ID du superutilisateur.

   Conseil : Assurez-vous de connaître l'ID sur l'hôte B qui accepte la connexion SSH, ainsi que l'ID du superutilisateur sur l'hôte A.
2. Générez les clés **id_rsa** et **id_rsa.pub** sur l'hôte A à l'aide de l'utilitaire *ssh-keygen*.

   Les clés sont enregistrées à l'emplacement : `~/.ssh: $ ssh-keygen -t rsa`.
3. Copiez les clés autorisées à partir de l'hôte B :

   $ scp Id on host B@name or IP address of host B:~/.ssh/authorized_keys ~/.ssh/authorized_keys_from_B
4. Ajoutez la clé publique pour l'hôte A à la fin des clés autorisées pour l'hôte B :

   cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys_from_B
5. Copiez les clés autorisées vers l'hôte B :

   $ scp ~/.ssh/authorized_keys_from_B Id on host B@name or IP address of host B:~/.ssh/authorizede_keys

   A faire : Si vous surveillez plusieurs hôtes, répétez les étapes «3», à la page 484, «4», à la page 484 et «5», à la page 484 pour chaque hôte.
6. Supprimez les clés autorisées que vous avez copiées sur l'hôte B :

   ~/.ssh/authorized_keys_from_B
7. Ajoutez la commande suivante au profil **~/.bash_** de l'ID en cours sur l'hôte A :

   $ eval `ssh-agent`

   A faire : Veillez à utiliser l'apostrophe inversée (`) qui se trouve sur la touche de la lettre è (pour l'obtenir : AltGR + touche è) du clavier français, et non le guillemet simple (').
8. Ajoutez l'identité à l'hôte A et entrez le mot de passe que vous avez utilisé pour créer l'ID :

   $ ssh-add ~/.ssh/id_rsa
9. Exécutez la commande suivante si vous recevez le message `Could not open a connection to your authentication agent` :

   exec ssh-agent bash

   Conseil : Vous pouvez remplacer l'interpréteur de commandes bash par l'interpréteur de commandes que vous utilisez, puis exécuter à nouveau la commande suivante :

   $ ssh-add ~/.ssh/id_rsa
10. Testez le protocole SSH pour vérifier qu'il parvient à se connecter de l'hôte A à l'hôte B sans qu'il soit nécessaire d'entrer le mot de passe SSH :

    Conseil : Si vous surveillez plusieurs hôtes, utilisez la commande suivante pour tester la connexion pour chacun d'eux :

    $ ssh Id on host B@name or IP address of host B
11. Pour vérifier la connexion, exécutez la commande suivante :

    virsh -c qemu+ssh://Id on host B@name or IP address of host B:port/system

    Si vous n'avez pas modifié le port SSH par défaut, omettez la section **:port** dans la commande.

Important : Si la commande **virsh** aboutit, l'agent Linux KVM se connecte à l'hyperviseur.

12. Vous devez redémarrer l'hôte A avant de redémarrer l'agent Linux KVM sur l'hôte A. Pour cela, exécutez à nouveau la commande **ssh-add** et indiquez le mot de passe à chaque fois.

    Conseil : Vous pouvez utiliser des chaînes de clés SSH pour éviter d'avoir à ressaisir le mot de passe.

Configuration du protocole TLS

Vous pouvez configurer le protocole TLS pour surveiller un hôte à distance.

Pourquoi et quand exécuter cette tâche

Supposition : L'agent Linux KVM est installé sur l'hôte A. Vous souhaitez surveiller à distance l'hyperviseur sur l'hôte B.

Procédure

1. Pour créer une clé de l'autorité de certification (CA) et un certificat dans votre hyperviseur, effectuez les étapes suivantes :
   a) Connectez-vous à l'hôte B.
   b) Créez un répertoire temporaire et modifiez le chemin d'accès en fonction de ce répertoire temporaire :

      ```
      mkdir fichiers_cert
      ```

      ```
      cd fichiers_cert
      ```

   c) Créez une clé RSA de 2048 bits :

      ```
      openssl genrsa -out cakey.pem 2048
      ```

   d) Créez un certificat autosigné pour votre autorité de certification locale :

      ```
      openssl req -new -x509 -days 1095 -key cakey.pem -out \
      cacert.pem -sha256 -subj "/C=US/L=Austin/O=IBM/CN=my CA"
      ```

   e) Vérifiez votre certificat de l'autorité de certification :

      ```
      openssl x509 -noout -text -in cacert.pem
      ```

2. Pour créer les clés et certificats du client et du serveur dans votre hyperviseur, effectuez les étapes suivantes :
   a) Créez les clés :

      ```
      openssl genrsa -out serverkey.pem 2048
      ```

      ```
      openssl genrsa -out clientkey.pem 2048
      ```

   b) Créez une demande de signature de certificat pour le serveur :

      A faire : Remplacez l'adresse kvmhost.company.org, qui est utilisée dans la demande de certificat de serveur, par le nom de domaine complet de votre hôte d'hyperviseur.

      ```
      openssl req -new -key serverkey.pem -out serverkey.csr \
      -subj "/C=US/O=IBM/CN=kvmhost.company.org"
      ```

   c) Créez une demande de signature de certificat pour le client :

      ```
      openssl req -new -key clientkey.pem -out clientkey.csr \
      -subj "/C=US/O=IBM/OU=virtualization/CN=root"
      ```

   d) Créez les certificats client et serveur :

      ```
      openssl x509 -req -days 365 -in clientkey.csr -CA cacert.pem \
      -CAkey cakey.pem -set_serial 1 -out clientcert.pem
      ```

      ```
      openssl x509 -req -days 365 -in serverkey.csr -CA cacert.pem \
      -CAkey cakey.pem -set_serial 94345 -out servercert.pem
      ```

   e) Vérifiez les clés :

openssl rsa -noout -text -in clientkey.pem

openssl rsa -noout -text -in serverkey.pem

f) Vérifiez les certificats :

openssl x509 -noout -text -in clientcert.pem

openssl x509 -noout -text -in servercert.pem

3. Pour distribuer les clés et les certificats au serveur hôte, effectuez les étapes suivantes :

a) Copiez le fichier `cacert.pem` du certificat de l'autorité de certification dans ce répertoire : `/etc/pki/CA`

cp cacert.pem /etc/pki/CA/cacert.pem

b) Créez le répertoire `/etc/pki/libvirt` et copiez le fichier de certificat de serveur `servercert.pem` dans le répertoire `/etc/pki/libvirt`. Assurez-vous que seul le superutilisateur peut accéder à la clé privée.

mkdir /etc/pki/libvirt

cp servercert.pem /etc/pki/libvirt/.

chmod -R o-rwx /etc/pki/libvirt

A faire : Si les clés ou les certificats sont nommés de façon incorrecte ou copiés dans les mauvais répertoires, l'autorisation échoue.

c) Créez le répertoire `/etc/pki/libvirt/private` et copiez le fichier de clés serveur `serverkey.pem` dans le répertoire `/etc/pki/libvirt/private`. Assurez-vous que seul le superutilisateur peut accéder à la clé privée.

mkdir /etc/pki/libvirt/private

cp serverkey.pem /etc/pki/libvirt/private/.

chmod -R o-rwx /etc/pki/libvirt/private

A faire : Si les clés ou les certificats sont nommés de façon incorrecte ou copiés dans les mauvais répertoires, l'autorisation échoue.

d) Vérifiez que les fichiers sont placés correctement :

find /etc/pki/CA/*|xargs ls -l

ls -lR /etc/pki/libvirt

ls -lR /etc/pki/libvirt/private

A faire : Si les clés ou les certificats sont nommés de façon incorrecte ou copiés dans les mauvais répertoires, l'autorisation échoue.

4. Pour distribuer les clés et les certificats aux clients ou aux stations de gestion, effectuez les étapes suivantes :

a) Connectez-vous à l'hôte A.

b) Copiez le certificat de l'autorité de certification `cacert.pem` de l'hôte dans le répertoire `/etc/pki/CA` sur l'hôte A sans changer le nom de fichier.

scp kvmhost.company.org:/tmp/cacert.pem /etc/pki/CA/

c) Copiez le fichier `clientcert.pem` de certificat client dans le répertoire `/etc/pki/libvirt` de l'hôte B. Utilisez les noms de fichier par défaut et assurez-vous que seul le superutilisateur peut accéder à la clé privée.

mkdir /etc/pki/libvirt/

scp kvmhost.company.org:/tmp/clientcert.pem /etc/pki/libvirt/.

chmod -R o-rwx /etc/pki/libvirt

A faire : Si les clés ou les certificats sont nommés de façon incorrecte ou copiés dans les mauvais répertoires, l'autorisation échoue.

d) Copiez la clé du client `clientkey.pem` dans le répertoire `/etc/pki/libvirt/private` de l'hôte. Utilisez les noms de fichier par défaut et assurez-vous que seul le superutilisateur peut accéder à la clé privée.

mkdir /etc/pki/libvirt/private

scp kvmhost.company.org:/tmp/clientkey.pem /etc/pki/libvirt/private/.

chmod -R o-rwx /etc/pki/libvirt/private

A faire : Si les clés ou les certificats sont nommés de façon incorrecte ou copiés dans les mauvais répertoires, l'autorisation échoue.

e) Vérifiez que les fichiers sont placés correctement :

ls -lR /etc/pki/libvirt

ls -lR /etc/pki/libvirt/private

5. Pour modifier la configuration du démon `libvirtd`, effectuez les étapes suivantes :
   a) Connectez-vous à l'hôte B.
   b) Effectuez une copie du fichier `/etc/sysconfig/libvirtd` et du fichier `/etc/libvirt/libvirtd.conf`.
   c) Editez le fichier `/etc/sysconfig/libvirtd` et assurez-vous que le paramètre **--listen** est transmis au démon `libvirtd`. Cette étape permet de s'assurer que le démon `libvirtd` est en mode écoute sur les connexions réseau.
   d) Editez le fichier `/etc/libvirt/libvirtd.conf` et configurez un ensemble de sujets autorisés avec l'instruction **tls_allowed_dn_list** dans le fichier `libvirtd.conf`.

   Important : Les zones figurant dans le sujet doivent suivre le même ordre que celui que vous avez utilisé pour créer le certificat.

   e) Redémarrez le service démon `libvirtd` pour que les modifications soient prises en compte :

   /etc/init.d/libvirtd restart
6. Pour modifier la configuration du pare-feu, accédez à la configuration du niveau de sécurité et ajoutez le port TCP 16514 comme port sécurisé.
7. Pour vérifier que la gestion à distance fonctionne, exécutez la commande suivante sur l'hôte A :

   virsh -c qemu+tls://kvmhost.company.org/system list --all

Configuration du protocole TCP
Utilisez le protocole TCP uniquement à des fins de test.

Pourquoi et quand exécuter cette tâche
Supposition : L'agent Linux KVM est installé sur l'hôte A. Vous souhaitez surveiller à distance l'hyperviseur sur l'hôte B.

Procédure

1. Connectez-vous à l'hôte B.
2. Editez le fichier `/etc/libvirt/libvirtd.conf` et assurez-vous que le paramètre **listen_tcp** est activé, et que le paramètre **tcp_port** est défini sur la valeur par défaut 16509.
3. Editez le fichier `/etc/libvirt/libvirtd.conf` pour définir le paramètre **auth_tcp** sur "none". Cette étape invite TCP à ne pas authentifier la connexion.
4. Redémarrez le démon **libvirt** sur l'hôte B en mode écoute en l'exécutant avec l'indicateur **--listen** ou en éditant le fichier `/etc/sysconfig/libvirtd` et en supprimant la mise en commentaire de la ligne `LIBVIRTD_ARGS="--listen"`.
5. Pour vérifier la connexion, exécutez la commande suivante :

virsh -c qemu+tcp://kvmhost.company.org:port/system

Si vous n'avez pas modifié le port TCP par défaut, omettez la section **:port** dans la commande.

Important : Si la commande **virsh** aboutit, l'agent Linux KVM se connecte à l'hyperviseur.

Que faire ensuite
Configurez l'agent en effectuant les étapes décrites dans «Configuration d'une connexion au serveur RHEVH», à la page 489.

Configuration d'une connexion au serveur RHEVM

Pour configurer une connexion au serveur RHEVM, vous devez exécuter le script et répondre aux invites.

Avant de commencer

1. Téléchargez le certificat de sécurité qui est disponible à l'emplacement suivant :

   ```
   https://HOTE-RHEVM:PORT-RHEVM/ca.crt
   ```

   Où

   HOTE-RHEVM
   Nom de l'hôte.

   PORT-RHEVM
   Port que vous utilisez dans votre environnement RHEVM.
2. Utilisez l'utilitaire *keytool* pour importer le fichier du certificat de sécurité afin de générer un fichier de clés local :

   keytool -import -alias ALIAS -file CERTIFICATE_FILE -keystore KEYSTORE_FILE

   Exemple : **keytool -import -alias RHEVM36vmwt9 -file hjs495-vmw-t-9.cer -keystore RHEVM36KeyStore**

   Où

   ALIAS
   Référence unique pour chaque certificat ajouté au fichier de clés certifiées de l'agent ; par exemple, *datasource* est un alias approprié pour le certificat provenant de *datasource.example.com*.

   FICHIER_CERTIFICAT
   Nom et chemin d'accès complet au fichier de certificat de source de données en cours d'ajout au magasin de clés de confiance.

   FICHIER_CLES
   Nom du fichier de clés que vous voulez spécifier.

   Conseil : L'utilitaire *keytool* est disponible avec Java Runtime Environment (JRE). Le fichier de clés est stocké au même emplacement que celui où vous exécutez la commande.
3. Vérifiez que l'utilisateur, qui se connecte à RHEVM, est un administrateur doté du rôle SuperUser (superutilisateur). Vous pouvez utiliser un ID utilisateur existant ayant ce rôle, ou en créer un nouveau en procédant comme décrit à la section «Création d'un utilisateur et attribution des droits nécessaires», à la page 483.

Procédure

1. A partir d'une ligne de commande, exécutez la commande suivante :

   rép_install/bin/linux_kvm-agent.sh config nom_instance

   Exemple : **/opt/ibm/apm/agent/bin/linux_kvm-agent.sh config nom_instance**

   Où

nom_instance
Est le nom que vous voulez attribuer à l'instance.

rép_install
Chemin où l'agent est installé.

2. Répondez aux invites et indiquez les valeurs des paramètres de configuration.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration pour la connexion au serveur RHEVM», à la page 490.

3. Exécutez la commande suivante pour démarrer l'agent :

   rép_install/bin/linux_kvm-agent.sh start nom_instance

   Exemple : **/opt/ibm/apm/agent/bin/linux_kvm-agent.sh start nom_instance**

Que faire ensuite
Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration d'une connexion au serveur RHEVH

Pour configurer une connexion au serveur RHEVH, vous devez exécuter le script et répondre aux invites.

Avant de commencer

- Vérifiez que l'utilisateur qui se connecte à RHEVM est un superutilisateur. Vous pouvez utiliser un ID utilisateur existant ou en créer un nouveau en procédant comme décrit à la section «Création d'un utilisateur et attribution des droits nécessaires», à la page 483.
- Configurez le protocole que vous voulez utiliser pour vous connecter au serveur RHEVH en procédant comme décrit à la section «Configuration des protocoles», à la page 483.

Procédure

1. A partir d'une ligne de commande, exécutez la commande suivante :

   rép_install/bin/linux_kvm-agent.sh config nom_instance

   Exemple : **/opt/ibm/apm/agent/bin/linux_kvm-agent.sh config nom_instance**

   Où

   nom_instance
   Est le nom que vous voulez attribuer à l'instance.

   rép_install
   Chemin où l'agent est installé.

2. Répondez aux invites et indiquez les valeurs des paramètres de configuration.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration pour la connexion au serveur RHEVH», à la page 492.

3. Exécutez la commande suivante pour démarrer l'agent :

   rép_install/bin/linux_kvm-agent.sh start nom_instance

   Exemple : **/opt/ibm/apm/agent/bin/linux_kvm-agent.sh start nom_instance**

Que faire ensuite
Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Paramètres de configuration pour la connexion au serveur RHEVM

Vous pouvez modifier les valeurs par défaut des paramètres de configuration qui sont utilisés pour connecter l'agent avec le serveur RHEVM.

Le tableau ci-après contient une description détaillée des paramètres de configuration.

Tableau 169. Noms et descriptions des paramètres de configuration pour la connexion au serveur RHEVM

Nom du paramètre	Description	Zone obligatoire
Edit Monitoring Agent for Linux KVM settings	Indique que vous pouvez commencer à éditer les valeurs par défaut des paramètres de configuration. Entrez `1 (Yes)` (valeur par défaut) pour continuer.	Oui
Maximum number of Data Provider Log Files	Nombre maximal de fichiers journaux créés par le fournisseur de données avant qu'il remplace les anciens fichiers journaux. La valeur par défaut est 10.	Oui
Maximum Size in KB of Each Data Provider Log	Taille maximale en ko qu'un fichier journal de fournisseur de données doit atteindre avant que le fournisseur de données ne crée un autre fichier journal. La valeur par défaut est 5190 ko.	Oui

Tableau 169. Noms et descriptions des paramètres de configuration pour la connexion au serveur RHEVM (suite)

Nom du paramètre	Description	Zone obligatoire
Level of Detail in Data Provider Log	Niveau de détail qui peut être inclus dans le fichier journal que le fournisseur de données crée. La valeur par défaut est 4 (Info). Les valeurs suivantes sont valides : • 1 = Off : aucun message n'est consigné. • 2 = Severe : seules les erreurs sont consignées. • 3 = Warning : toutes les erreurs et tous les messages consignés au niveau Severe et les erreurs potentielles qui peuvent entraîner un comportement non souhaité. • 4 = Info : toutes les erreurs et tous les messages consignés au niveau Warning et les messages d'information de niveau supérieur qui décrivent l'état du fournisseur de données pendant son traitement. • 5 = Fine : toutes les erreurs et tous les messages consignés au niveau Info et les messages d'information de niveau inférieur qui décrivent l'état du fournisseur de données pendant son traitement. • 6 = Finer : toutes les erreurs et tous les messages consignés au niveau Fine plus les messages d'information très détaillés, tels que les informations sur le profil de performance et les données de débogage. Si vous sélectionnez cette option, cela peut affecter les performances de l'agent de surveillance. Ce paramètre n'est destiné qu'à être utilisé comme un outil pour l'identification des problèmes, en collaboration avec l'équipe de support IBM. • 7 = Finest : toutes les erreurs et tous les messages consignés au niveau Fine et les messages d'information les plus détaillés qui incluent les messages et les données de programmation de niveau inférieur. Cette option risque d'affecter les performances de l'agent de surveillance de manière négative. Ce paramètre n'est destiné qu'à être utilisé comme un outil pour l'identification des problèmes, en collaboration avec l'équipe de support IBM. • 8 = All : toutes les erreurs et tous les messages sont consignés.	Oui
Edit Hypervisor settings	Indique si vous voulez éditer les paramètres pour une connexion au serveur RHEVH. Entrez `5 (Next)` pour indiquer que vous configurez une connexion au serveur RHEVM. La valeur par défaut est `5 (Next)`.	Oui
Edit RHEVM Connection Details settings	Indique si vous voulez éditer les paramètres pour une connexion au serveur RHEVM. Entrez `1 (Add)` pour continuer. La valeur par défaut est `5 (Next)`. **Important :** Après avoir spécifié des valeurs pour tous les paramètres de configuration, vous êtes de nouveau invité à indiquer si vous voulez continuer à éditer les paramètres. Entrez `5 (Exit)`.	Oui
RHEVM ID	Le nom d'utilisateur unique que vous indiquez pour le RHEVM auquel vous vous connectez.	Oui

Tableau 169. Noms et descriptions des paramètres de configuration pour la connexion au serveur RHEVM (suite)		
Nom du paramètre	**Description**	**Zone obligatoire**
Host	Nom d'hôte ou adresse IP de la source de données qui est utilisée pour la connexion au serveur RHEVM.	Oui
User	Nom d'utilisateur de la source de données disposant des privilèges appropriés pour se connecter au serveur RHEVM.	Oui
Password	Mot de passe associé au nom d'utilisateur permettant de se connecter au serveur RHEVM.	Oui
Re-type password	Mot de passe que vous avez indiqué dans la zone **Password**.	Oui
Port	Numéro de port utilisé pour la connexion au serveur RHEVM.	Oui
Domaine	Domaine auquel appartient l'utilisateur.	Oui
KeyStorePath	Nom et chemin d'accès au fichier de clés local que vous avez créé à l'aide de la commande **keytool**.	Oui

Paramètres de configuration pour la connexion au serveur RHEVH

Vous pouvez modifier les valeurs par défaut des paramètres de configuration qui sont utilisés pour connecter l'agent avec le serveur RHEVH.

Le tableau ci-après contient une description détaillée des paramètres de configuration.

Tableau 170. Noms et descriptions des paramètres de configuration pour la connexion à l'hyperviseur		
Nom du paramètre	**Description**	**Zone obligatoire**
Edit Monitoring Agent for Linux KVM settings	Indique que vous pouvez commencer à éditer les valeurs par défaut des paramètres de configuration. Entrez `1 (Yes)` (valeur par défaut) pour continuer.	Oui
Maximum number of Data Provider Log Files	Nombre maximal de fichiers journaux créés par le fournisseur de données avant qu'il remplace les anciens fichiers journaux. La valeur par défaut est 10.	Oui
Maximum Size in KB of Each Data Provider Log	Taille maximale en ko qu'un fichier journal de fournisseur de données doit atteindre avant que le fournisseur de données ne crée un autre fichier journal. La valeur par défaut est 5190 ko.	Oui

Tableau 170. Noms et descriptions des paramètres de configuration pour la connexion à l'hyperviseur (suite)

Nom du paramètre	Description	Zone obligatoire
Level of Detail in Data Provider Log	Niveau de détail qui peut être inclus dans le fichier journal que le fournisseur de données crée. La valeur par défaut est 4 (Info). Les valeurs suivantes sont valides : • 1 = Off : aucun message n'est consigné. • 2 = Severe : seules les erreurs sont consignées. • 3 = Warning : toutes les erreurs et tous les messages consignés au niveau Severe et les erreurs potentielles qui peuvent entraîner un comportement non souhaité. • 4 = Info : toutes les erreurs et tous les messages consignés au niveau Warning et les messages d'information de niveau supérieur qui décrivent l'état du fournisseur de données pendant son traitement. • 5 = Fine : toutes les erreurs et tous les messages consignés au niveau Info et les messages d'information de niveau inférieur qui décrivent l'état du fournisseur de données pendant son traitement. • 6 = Finer : toutes les erreurs et tous les messages consignés au niveau Fine plus les messages d'information très détaillés, tels que les informations sur le profil de performance et les données de débogage. Si vous sélectionnez cette option, cela peut affecter les performances de l'agent de surveillance. Ce paramètre n'est destiné qu'à être utilisé comme un outil pour l'identification des problèmes, en collaboration avec l'équipe de support IBM. • 7 = Finest : toutes les erreurs et tous les messages consignés au niveau Fine et les messages d'information les plus détaillés qui incluent les messages et les données de programmation de niveau inférieur. Si vous sélectionnez cette option, cela risque d'affecter les performances de l'agent de surveillance. Ce paramètre n'est destiné qu'à être utilisé comme un outil pour l'identification des problèmes, en collaboration avec l'équipe de support IBM. • 8 = All : toutes les erreurs et tous les messages sont consignés.	Oui
Edit Hypervisor settings	Indique si vous voulez éditer les paramètres pour une connexion à l'hyperviseur. Entrez `1 (Add)`. La valeur par défaut est 5 `(Next)`.	Oui
Hypervisor ID	Le nom d'utilisateur unique que vous indiquez pour le RHEVH auquel vous vous connectez.	Oui
Host	Nom d'hôte ou adresse IP de la source de données qui est utilisée pour la connexion au serveur RHEVH.	Oui
User	Nom d'utilisateur de la source de données disposant des privilèges appropriés pour se connecter au serveur RHEVM.	Oui

Tableau 170. Noms et descriptions des paramètres de configuration pour la connexion à l'hyperviseur (suite)		
Nom du paramètre	**Description**	**Zone obligatoire**
Remote Transport	Protocole utilisé par l'API `libvirt` locale pour se connecter aux API `libvirt` distantes. La valeur par défaut est 1. Les valeurs suivantes sont admises : • 1 = SSH • 2 = TLS • 3 = TCP (non chiffré - non recommandé dans un environnement de production)	Oui
Port	Port utilisé par le protocole de transport pour se connecter à l'API `libvirt`. La valeur par défaut est 22. **Important :** Ce port n'est nécessaire que si les ports standard ont été modifiés (22 pour SSH, 16514 pour TLS, 16509 pour TCP).	Oui
Domaine	Domaine auquel appartient l'utilisateur.	Oui
Connection Instance Type	Indique si l'API `libvirt` locale se connecte au pilote du système doté de droits ou au pilote de session utilisateur sans droit. La valeur par défaut est 1. Les valeurs suivantes sont admises : • 1 = système • 2 = session	Oui
Edit RHEVM Connection Details settings	Indique si vous voulez éditer les paramètres pour une connexion au serveur RHEVM. Entrez `1 (Add)` pour continuer. La valeur par défaut est `5 (Next)`. **Important :** Après avoir spécifié des valeurs pour tous les paramètres de configuration, vous êtes de nouveau invité à indiquer si vous voulez continuer à éditer les paramètres. Entrez `5 (Next)`.	Oui

Configuration de la surveillance de MariaDB

Vous devez configurer l'Agent MariaDB pour qu'il puisse collecter des données afin de surveiller la disponibilité et les performances des ressources du serveur MariaDB. Prenez connaissance des prérequis suivants pour configurer l'agent MariaDB en vue de la surveillance locale et de la surveillance à distance.

Avant de commencer

Assurez-vous que votre environnement possède la configuration système requise pour l'Agent MariaDB. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent MariaDB.

Pourquoi et quand exécuter cette tâche

L'agent MariaDB est un agent à instance unique. Une fois installé, vous devez le configurer manuellement. Vous pouvez le configurer sur les systèmes d'exploitation Windows et Linux. Pour effectuer la configuration, l'agent requiert un nom d'instance et les données d'identification utilisateur du serveur MariaDB. Le nom de système géré inclut le nom d'instance que vous spécifiez, *nom_instance*:*nom_hôte*:*cp* par exemple, où *cp* est le code produit à deux caractères. Le nom de système géré admet jusqu'à 32 caractères. Le nom d'instance que vous entrez admet jusqu'à 28

caractères, moins la longueur de votre nom d'hôte. Par exemple, si vous spécifiez `MariaDB` comme nom d'instance, le nom de système géré est `MariaDB:hostname:MJ`.

Important : Si vous indiquez un nom d'instance long, le nom de système géré est tronqué et le code d'agent ne s'affiche pas.

Configuration de l'agent sur les systèmes Windows

Vous pouvez configurer l'agent sur des systèmes d'exploitation Windows dans la fenêtre IBM Cloud Application Performance Management. Une fois que vous avez mis à jour les valeurs de configuration, démarrez l'agent pour appliquer les valeurs mises à jour.

Procédure

Pour configurer l'agent sur des systèmes d'exploitation Windows, procédez comme suit :

1. Cliquez sur **Démarrer>Tous les programmes>IBM Monitoring agents>IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, procédez comme suit :
   a) Cliquez deux fois sur le modèle **Monitoring Agent for MariaDB**.
   b) Dans la fenêtre **Monitoring Agent for MariaDB**, indiquez un nom d'instance et cliquez sur **OK**.
3. Dans la fenêtre **Monitoring Agent for MariaDB**, procédez comme suit :
   a) Dans la zone **Adresse IP**, entrez l'adresse IP d'un serveur MariaDB à surveiller à distance. Si l'agent est installé sur un serveur à surveiller, conservez la valeur par défaut.
   b) Dans la zone **Nom d'utilisateur JDBC**, entrez le nom d'un utilisateur du serveur MariaDB. La valeur par défaut est root.
   c) Dans la zone **Mot de passe JDBC**, entrez le mot de passe d'un utilisateur JDBC.
   d) Dans la zone **Confirmer le mot de passe JDBC**, entrez de nouveau le mot de passe.
   e) Dans la zone **Fichier JDBC Jar**, cliquez sur **Parcourir**, puis localisez le répertoire qui contient le fichier Java de connecteur MariaDB et sélectionnez-le.
   f) Cliquez sur **Suivant**.
   g) Dans la zone **Numéro de port JDBC**, indiquez le numéro de port du serveur JDBC.
   Le numéro de port par défaut est 3306.
   h) Dans la liste **Niveau de trace Java**, sélectionnez un niveau de trace pour Java.
   La valeur par défaut est `Error`.
   i) Cliquez sur **OK**.
   L'instance est affichée dans la fenêtre **IBM Performance Management**.
4. Cliquez avec le bouton droit de la souris sur l'instance **Monitoring Agent for MariaDB**, puis cliquez sur **Démarrer**.

   A faire : Pour configurer de nouveau l'agent, effectuez ces étapes dans la fenêtre **IBM Performance Management** :

   a. Arrêtez l'instance d'agent que vous voulez configurer.
   b. Cliquez avec le bouton droit de la souris sur l'instance **Monitoring Agent for MariaDB** et cliquez sur **Reconfigurer**.
   c. Répétez les étapes 3 et 4.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de l'agent sur des systèmes Linux

Vous pouvez exécuter le script de configuration et répondre aux invites pour configurer l'agent sur des systèmes d'exploitation Linux.

Procédure

Pour configurer l'agent sur un système d'exploitation Linux, procédez comme suit :

1. Sur la ligne de commande, exécutez la commande suivante :

   ```
   rép_install/bin/mariadb-agent.sh config nom_instance
   ```

   Où *nom_instance* est le nom à attribuer à l'instance, et *rép_install* est le répertoire d'installation de l'Agent MariaDB.
2. A l'invite d'entrée d'une valeur pour les paramètres suivants, appuyez sur **Entrée** pour accepter la valeur par défaut ou indiquez une autre valeur et appuyez sur **Entrée**.
   - Adresse IP
   - Nom d'utilisateur JDBC
   - Mot de passe JDBC
   - Ressaisir le mot de passe JDBC
   - Fichier JAR JDBC
   - Numéro du port JDBC (le numéro du port par défaut est 3306.)
   - Niveau de trace Java (la valeur par défaut est `Erreur`.)

   Pour plus d'informations sur les paramètres de configuration, voir «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 593.
3. Exécutez la commande suivante pour démarrer l'agent :

   ```
   rép_install/bin/mariadb-agent.sh start nom_instance
   ```

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration de l'agent. Ce mode de configuration est appelé mode silencieux.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'Agent MariaDB sous Linux et Windows. Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

Pour configurer l'agent à l'aide du fichier de réponses silencieux, procédez comme suit :

A faire : Pour cette procédure, le chemin d'accès par défaut est celui où l'agent est installé :
Windows `C:\IBM\APM`
Linux `opt/ibm/apm/agent`

Si vous avez installé l'agent dans un autre chemin, remplacez le chemin dans les instructions. En outre, éditez le paramètre **AGENT_HOME** dans le fichier de réponses silencieux en spécifiant le chemin d'installation de l'agent.

1. Dans un éditeur de texte, ouvrez le fichier de réponses disponible à l'emplacement suivant :

   Linux *rép_install*/samples/mariadb_silent_config.txt

   Windows *rép_install*\samples\mariadb_silent_config.txt

   Où *rép_install* correspond au répertoire d'installation de l'Agent MariaDB
2. Dans le fichier de réponses, indiquez une valeur pour les paramètres suivants :
   - Pour le paramètre **Nom de serveur**, spécifiez l'adresse IP d'un serveur MariaDB à surveiller à distance. Sinon, conservez la valeur par défaut `localhost`.
   - Pour le paramètre **Nom d'utilisateur JDBC**, conservez la valeur de nom d'utilisateur par défaut `root` ou indiquez le nom d'un utilisateur qui dispose des droits permettant d'afficher les tables INFORMATION_SCHEMA.
   - Pour le paramètre **Mot de passe JDBC**, entrez le mot de passe de l'utilisateur JDBC.
   - Pour le paramètre **Fichier JAR JDBC**, conservez le chemin par défaut si ce chemin d'accès au connecteur MariaDB pour le fichier JAR Java est correct. Sinon, indiquez le chemin approprié. Le connecteur est disponible à l'emplacement par défaut suivant :

     Linux `/usr/share/java/mariadb-connector-java.jar`

     Windows `C:\Program Files (x86)\MariaDB\mariadb-connector-java.jar`
   - Pour le paramètre **Numéro de port JDBC**, conservez le numéro de port par défaut 3306 ou indiquez un autre numéro de port.
   - Pour le paramètre **Niveau de trace Java**, conservez la valeur par défaut `Erreur` ou indiquez un autre niveau de trace selon les instructions du support IBM.
3. Sauvegardez et fermez le fichier de réponses, puis entrez la commande suivante pour mettre à jour les paramètres de configuration de l'agent :

   Linux *rép_install*/bin/mariadb-agent.sh config *nom_instance rép_install*/samples/mariadb_silent_config.txt

   Windows *rép_install*\BIN\mariadb-agent.bat config *nom_instance rép_install* \samples\mariadb_silent_config.txt

   Où *nom_instance* est le nom à attribuer à l'instance, et *rép_install* est le répertoire d'installation de l'Agent MariaDB.

   Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les tableaux de bord n'affichent pas les données de l'agent.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de la surveillance de Microsoft Active Directory

Monitoring Agent for Microsoft Active Directory est automatiquement configuré et démarré après l'installation.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel en consultant Génération d'un rapport sur la compatibilité du produit logiciel pour l'agent Microsoft Active Directory

Pour afficher les données de tous les attributs dans le tableau de bord, procédez comme suit :

- «Exécution de l'agent Microsoft Active Directory en tant qu'administrateur», à la page 498
- «Configuration des variables d'environnement local», à la page 498

Pourquoi et quand exécuter cette tâche

Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Exécution de l'agent Microsoft Active Directory en tant qu'administrateur

Vous devez avoir des droits d'administrateur pour exécuter l'agent Microsoft Active Directory.

Pourquoi et quand exécuter cette tâche

Tous les ensembles de données sont disponibles pour les utilisateurs membres du groupe Administrateur. Dans cette tâche, vous créez un utilisateur, affectez des droits d'administrateur à l'utilisateur et remplacez le compte utilisateur de l'agent par cet utilisateur.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **Outils d'administration** > **Utilisateurs et ordinateurs Active Directory**.
2. Pour développer le domaine où vous souhaitez créer l'utilisateur, cliquez sur le signe (+) en regard du nom d'un domaine.
3. Cliquez avec le bouton droit sur **Utilisateurs**, puis cliquez sur **Nouveau** > **Utilisateur**.
4. Pour créer un utilisateur, ouvrez l'assistant **Nouvel objet - Utilisateur**.

   Par défaut, un nouvel utilisateur est membre du groupe Utilisateurs du domaine.
5. Cliquez avec le bouton droit sur le nouvel utilisateur que vous venez de créer dans le groupe Utilisateurs du domaine, puis cliquez **Propriétés**. La fenêtre des **propriétés du nom d'utilisateur** s'affiche. Le nom d'utilisateur est le nom du nouvel utilisateur.
6. Dans la fenêtre des **propriétés du nom d'utilisateur**, procédez comme suit :
   a) Cliquez sur l'onglet **Membre de**. Dans la zone **Membre de**, ajoutez le groupe Administrateurs.
   b) Cliquez sur **Appliquer**, puis sur **OK**.
7. Cliquez sur **Démarrer** > **Exécuter**, puis tapez `services.msc`.
8. Dans la fenêtre **Services**, procédez comme suit :
   a) Cliquez avec le bouton droit de la souris sur **Monitoring Agent for le service Active Directory** et cliquez sur **Propriétés**.
   b) Dans la fenêtre **Monitoring Agent for les propriétés Active Directory**, dans l'onglet **Connexion**, cliquez sur **Ce compte**. Entrez les données d'identification de l'utilisateur.
   c) Cliquez sur **Appliquer**, puis sur **OK**.
9. Redémarrez le service d'agent.

Configuration des variables d'environnement local

Vous devez indiquer des valeurs pour les variables d'environnement pour afficher les données de réplication Sysvol dans le tableau de bord. Vous pouvez aussi éventuellement mettre à jour la valeur d'intervalle de cache afin d'activer ou de désactiver la mise en cache.

Procédure

1. Dans la fenêtre **IBM Performance Management**, dans le menu **Actions**, cliquez sur **Advanced** > **Edit ENV File**.

2. Dans le fichier K3ZENV, changez les valeurs des variables d'environnement suivantes.

   ADO_CACHE_INTERVAL
   Détermine si la mise en cache doit être démarrée ou arrêtée et définit une valeur d'intervalle de mise en cache. L'intervalle de mise en cache est la durée en secondes entre deux collectes consécutives de données. Entrez un entier positif pour l'intervalle de mise en cache afin de démarrer la mise en cache. Entrez la valeur zéro pour l'intervalle de mise en cache afin d'arrêter la mise en cache. Par défaut, la mise en cache est démarrée et l'intervalle de mise en cache défini sur 1200.

   ADO_SYSVOL_FORCE_REPLICATION_FLAG
   Détermine si la réplication forcée qui est initiée par l'agent est activée ou désactivée. La valeur par défaut de cette variable est TRUE. Pour désactiver la réplication forcée, affectez à cette variable la valeur FALSE.

   ADO_SYSVOL_REPLICATION_TEST_INTERVAL
   Détermine l'intervalle de temps en minutes entre deux tests de réplication Sysvol. La valeur par défaut de cette variable est 0 minutes. Pour effectuer le test de réplication Sysvol, assurez-vous que la valeur de cette variable est supérieure à zéro.

   ADO_SYSVOL_REPLICATION_TEST_VERIFICATION_INTERVAL
   Détermine le délai d'attente en minutes de l'agent avant de vérifier les résultats de la réplication Sysvol après avoir effectué le test de réplication Sysvol.

   La valeur de la variable **ADO_SYSVOL_REPLICATION_TEST_INTERVAL** doit être supérieure à celle de la variable **ADO_SYSVOL_REPLICATION_TEST_VERIFICATION_INTERVAL**. Vous pouvez utiliser les valeurs suivantes pour ces variables :

   ADO_SYSVOL_REPLICATION_TEST_INTERVAL : 1440
   ADO_SYSVOL_REPLICATION_TEST_VERIFICATION_INTERVAL : 30

   Une fois que des valeurs valides ont été affectées aux deux variables d'environnement, l'agent Active Directory crée un fichier dans le dossier partagé Sysvol du système géré et lance la réplication Sysvol forcée. Cette réplication forcée est démarrée du système géré vers les dossiers partagés Sysvol des partenaires de réplication Sysvol. Après vérification des résultats du test de réplication, l'agent supprime les fichiers créés et répliqués du système géré et des partenaires de réplication Sysvol.
3. Facultatif : Dans le fichier K3ZENV, ajoutez la variable d'environnement **APM_ATTRIBUTES_ENABLE_COLLECTION** et définissez sa valeur sur Yes pour visualiser des données pour les ensembles de données suivants dans l'onglet **Détails d'attribut**.

   - Services
   - Réplication
   - File Replication Service (FRS)
   - Unité d'org déplacée ou supprimée
   - LDAP
   - Gestionnaire de comptes de la sécurité
   - DFS
   - Carnet d'adresses
   - Journal des événements
   - Objets de configuration de mot de passe

   A faire : Si vous voulez désactiver la collecte de données pour ces ensembles de données, définissez la valeur pour la variable d'environnement **APM_ATTRIBUTES_ENABLE_COLLECTION** sur No.
4. Redémarrez l'agent Microsoft Active Directory.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Exécution de l'agent Microsoft Active Directory en tant qu'utilisateur non-administrateur

Vous pouvez exécuter Log File Agent en tant qu'utilisateur non-administrateur.

Pourquoi et quand exécuter cette tâche

Vous pouvez exécuter Monitoring Agent for Active Directory en tant qu'utilisateur non-administrateur ; cependant, les attributs Topologie d'accréditation et Réplication Sysvol peuvent être indisponibles. Ces attributs ne sont disponibles que pour les utilisateurs de domaine.

Pour afficher les attributs Topologie d'accréditation, un utilisateur non-administrateur doit disposer des autorisations suivantes sur le Registre :

- Droits d'accès complets au répertoire `HKEY_LOCAL_MACHINE\SOFTWARE\Candle`.
- Droits d'accès en lecture au répertoire `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Perflib`.

Pour afficher les attributs Réplication Sysvol, un utilisateur non-administrateur doit disposer de droits d'accès complets au dossier `Sysvol` sur tous les contrôleurs de domaine d'un domaine.

Important : Lorsque vous exécutez l'agent Microsoft Active Directory en tant qu'utilisateur non-administrateur, certains services du groupe d'attributs Services indiquent que les valeurs des attributs Etat actuel et Type de démarrage sont inconnues dans l'interface utilisateur d'APM.

Le tableau suivant contient les groupes d'attributs pour l'agent Active Directory, qui affichent les données des utilisateurs de domaine et des utilisateurs de surveillance des performances.

Tableau 171. Groupes d'attributs des utilisateurs de domaine et des utilisateurs de surveillance des performances

Droits d'utilisateur	**Groupe d'attributs**
Utilisateurs de domaine	• Informations sur le pool RID • Services • Journaux des événements • DNS • Détails de l'intégration à AD DNS • Intégration à AD DNS • DHCP • Accréditation • Objets de stratégie de groupe • Objets perdus et trouvés • Service d'annuaire Exchange • Objets de conflit de réplication • Attribut LDAP • Serveur de répertoire principal • Conteneurs • Partenaire de réplication • Disponibilité du contrôleur de domaine • Temps d'attente de partenaire de réplication • Topologie de forêt

Tableau 171. Groupes d'attributs des utilisateurs de domaine et des utilisateurs de surveillance des performances (suite)

Droits d'utilisateur	Groupe d'attributs
Utilisateurs de domaine et utilisateurs de surveillance des performances	Tous les attributs répertoriés pour les utilisateurs de domaine auxquels s'ajoutent les groupes d'attributs supplémentaires suivants : • Carnet d'adresses • Réplication • Services d'annuaire • Vérificateur de cohérence des données • Centre de distribution de clés kerberos • Protocole LDAP (Lightweight Directory Access Protocol) • Autorité de sécurité locale (LSA) • Fournisseur de service d'annuaire • Gestionnaire de comptes de la sécurité • File Replication Service (FRS) • Réplication de système de fichiers réparti • Connexions de réplication DFS • Dossiers répliqués DFS • Volume de service DFS • Performances du contrôleur de domaine • Serveur d'accès distant • Serveur d'accès direct • Attributs Netlogon

Remarque : De plus, les groupes d'attributs suivants affichent les données des utilisateurs membres du groupe *Administrateurs* :

- Informations sur les bases de données Active Directory
- Unité organisationnelle déplacée ou supprimée
- Objets de configuration de mot de passe

Pour plus d'informations, voir «Configuration de la surveillance de Microsoft Active Directory», à la page 497.

Procédure

1. Cliquez sur **Démarrer>Programmes>Outils d'administration>Utilisateurs et ordinateurs Active Directory**.
2. Développez le domaine dans lequel vous voulez créer l'utilisateur en cliquant sur le signe plus (+) qui se trouve en regard de son nom.
3. Cliquez avec le bouton droit sur **Utilisateurs**, puis cliquez sur **Nouveau>Utilisateur**.
4. Créez un nouvel utilisateur à l'aide de l'assistant **Nouvel objet - Utilisateur**. Par défaut, tout nouvel utilisateur fait partie du groupe **Utilisateurs du domaine**.
5. Cliquez avec le bouton droit de la souris sur le nouvel utilisateur que vous venez de créer dans le groupe *Utilisateurs du domaine*, puis cliquez sur **Propriétés**. La fenêtre **Propriétés de Nom d'utilisateur** s'ouvre, où *nom_utilisateur* est le nom du nouvel utilisateur. Exécutez les étapes suivantes dans la fenêtre **Propriétés de Nom d'utilisateur** :

a) Cliquez sur l'onglet **Membre de**. Dans la zone **Membre de**, ajoutez le groupe **Utilisateurs de l'Analyseur de performances**.

b) Cliquez sur **Appliquer**, puis sur **OK**.

6. Accédez au répertoire `rép_principal_candle`. Le chemin par défaut est `C:\IBM\APM`.
7. Cliquez avec le bouton droit de la souris sur le dossier APM, puis cliquez sur **Propriétés**. La fenêtre **Propriétés d'APM** s'affiche. Exécutez les étapes suivantes dans la fenêtre **Propriétés d'APM** :

   a) Sur l'onglet **Sécurité**, cliquez sur **Editer**.

   b) Cliquez sur **Ajouter** pour ajouter le nouvel utilisateur et lui accorder des droits d'accès complets.

   c) Cliquez sur **Appliquer**, puis sur **OK**.
8. Cliquez sur **Démarrer > Exécuter**, puis tapez `services.msc`. La fenêtre **Services** s'ouvre. Exécutez les étapes suivantes dans la fenêtre **Services** :

   a) Cliquez avec le bouton droit de la souris sur **Agent de surveillance** pour le service Active Directory, puis cliquez sur **Propriétés**.

   b) Dans la fenêtre **Propriétés d'Active Directory**, sous l'onglet **Connexion**, cliquez sur **Ce compte**. Entrez les données d'identification de l'utilisateur.

   c) Cliquez sur **Appliquer**, puis sur **OK**.
9. Redémarrez le service d'agent.

Configuration des services de domaine pour le groupe d'attributs AD_Services_Status

Vous pouvez configurer les services de domaine MS Active Directory dans le fichier `Services.properties` à utiliser ou à exclure
lors de la détermination du `Statut du serveur`. Le groupe d'attributs `AD_Services_Status` et sa situation sont applicables pour
Windows Server 2012 et ultérieur.

Pourquoi et quand exécuter cette tâche

Le fichier `Services.properties` contient les services de domaine MS Active Directory et la configuration associée.
True indique que le service sera pris en compte lors de la détermination de la valeur de statut du serveur, et False qu'il ne le sera pas.

Tableau 172. Services de domaine MS Active Directory et leurs paramètres de configuration.

Services de domaine MS Active Directory	Paramètre par défaut
Réplication DFS	true
Appel de procédure distante (RPC)	false
Client DNS	true
Serveur DNS	true
Client de stratégie de groupe	false
Messagerie inter-site	true
Centre de distribution de clés kerberos	true
NetLogon	true
Heure Windows	true
Client DHCP	false
Active Directory Web Services	false
Active Directory Federation Services	false

Remarque : Il est nécessaire de redémarrer l'agent pour autoriser la collecte des données pour le groupe d'attributs `AD_Services_Status` sous Windows Server 2012 et ultérieur.

Procédure

1. Arrêtez l'agent.
2. Recherchez le fichier `Services.properties` afin de le modifier, le cas échéant.
   Pour l'agent 32 bits, ce fichier se trouve dans le répertoire *rép_base_CANDLE*\TMAITM6\.
   Pour l'agent 64 bits, il se trouve dans le répertoire *rép_base_CANDLE*\TMAITM6_x64\.
   rép_base_CANDLE est le répertoire d'installation de l'agent.
3. Pour que les services de domaine soient pris en compte lors de la détermination du statut du serveur, attribuez-leur la valeur true.
   Pour qu'ils soient exclus, attribuez-leur la valeur false.
   Sauvegardez et fermez le fichier.
4. Démarrez l'agent.

Mise à niveau de l'agent Microsoft Active Directory

Vous pouvez mettre à niveau l'agent MS Active Directory à la dernière version.

Avant de commencer

Vérifiez que le fichier `installAPMAgents.bat` fourni dans le programme d'installation de la dernière version est disponible sur la machine où l'agent est installé.

Pourquoi et quand exécuter cette tâche

Pour mettre à niveau l'agent à la dernière version, procédez comme suit :

Procédure

1. Connectez-vous à la machine sur laquelle l'agent est installé.
2. Lancez une invite de commande et exécutez le fichier `installAPMAgents.bat` provenant du programme d'installation de la dernière version.
3. Saisissez le répertoire d'installation de l'agent et appuyez sur la touche Entrée.
4. Les versions de l'agent de base et de l'agent cible à mettre à niveau s'affichent à l'invite de commande. Appuyez sur la touche Entrée pour continuer.
5. Une fois la mise à niveau terminée, la version mise à niveau de l'agent s'affiche dans la fenêtre **IBM Performance Management**.
6. Dans cette fenêtre, cliquez avec le bouton droit de la souris sur l'agent et sélectionnez **Reconfigure** dans le menu déroulant.
7. Pour refléter la version mise à niveau de l'agent dans le **Tableau de bord d'Application Performance**, connectez-vous au serveur APM et redémarrez ses composants à l'aide des commandes suivantes.
   a. **`apm stop_all`**
   b. **`apm start_all`**
8. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur l'agent et sélectionnez **Recycle** dans le menu déroulant.

Résultats

L'agent mis à niveau apparaît alors dans le **tableau de bord d'Application Performance**.

Remarque : Cela peut prendre plus ou moins 30 minutes.

Configuration de la surveillance de Microsoft Cluster Server

Vous devez configurer Monitoring Agent for Microsoft Cluster Server pour qu'il puisse collecter les données du serveur en cluster. Utilisez le fichier de réponses silencieux pour configurer l'agent.

Avant de commencer

Veillez à exécuter les tâches suivantes :

- Créez un groupe de ressources vide pour l'agent.
- Créez une ressource de cluster de service générique dans le groupe de ressources de l'agent sur les systèmes Windows Server 2008, 2012, 2016 et 2019.
- Vérifiez que l'utilisateur, qui se connecte à l'environnement ou à l'application Microsoft Cluster Server, dispose des privilèges d'administrateur. Utilisez un utilisateur existant disposant des privilèges d'administrateur ou créez-en un nouveau. Ajoutez le nouvel utilisateur au groupe Administrateurs pour qu'il bénéficie des privilèges d'administrateur.

  A faire : Pour configurer l'agent Microsoft Cluster Server, vous pouvez utiliser un utilisateur local ou un utilisateur de domaine à condition que celui-ci dispose des privilèges d'administrateur.

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Microsoft Cluster Server.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Pourquoi et quand exécuter cette tâche

L'agent Microsoft Cluster Server est un agent à instance unique. Vous devez installer et configurer l'agent manuellement de la même manière sur chaque noeud du cluster. Pour configurer l'agent, voir «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 506.

Création d'une ressource de cluster de service générique sur les systèmes Windows Server 2008, 2012, 2016 et 2019

Vous devez ajouter le service d'agent de cluster en tant que ressource pour que l'agent puisse surveiller le serveur en cluster.

Avant de commencer

Vérifiez que l'agent est arrêté sur chaque noeud du cluster.

Procédure

Pour créer une ressource de cluster de service générique, procédez comme suit :

1. Ouvrez le **Gestionnaire du cluster de basculement** sur l'un des noeuds du cluster.
2. Effectuez l'une des étapes suivantes :
   - Pour Windows Server 2008 :

     Dans le panneau de navigation, cliquez avec le bouton droit de la souris sur **Services et applications**, puis cliquez sur **Plus d'actions** > **Créer un service ou une application vide**. Le nouveau service s'affiche dans la liste des services et applications. Renommez le nouveau service créé.
   - Pour Windows Server 2012 :

Dans le panneau de navigation, cliquez avec le bouton droit de la souris sur **Rôles**, puis cliquez sur **Plus d'actions** > **Créer des rôles**. Le nouveau service s'affiche dans la liste des rôles.

- Pour Windows Server 2016 et 2019 :

  Dans le panneau de navigation, cliquez avec le bouton droit de la souris sur **Rôles**, puis cliquez sur **Configurer les rôles**. Le nouveau service s'affiche.

3. Cliquez sur le nouveau service avec le bouton droit de la souris, puis cliquez sur **Ajouter une ressource** > **Service générique**.
4. Dans la fenêtre **Assistant Nouvelle ressource**, sélectionnez **Monitoring Agent for Microsoft Cluster Server**, puis cliquez sur **Suivant**.
5. Cliquez sur **Suivant** dans les fenêtres qui suivent jusqu'à afficher le bouton **Terminer**.
6. Cliquez sur **Terminer**.

   Le service d'agent est ajouté en tant que ressource.
7. Cliquez avec le bouton droit de la souris sur la ressource **Monitoring Agent for Microsoft Cluster Server**, puis cliquez sur **Mettre la ressource en ligne**.

Résultats
L'agent est démarré sur le noeud préférentiel.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration de l'agent Microsoft Cluster Server dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour définir des valeurs différentes pour les paramètres de configuration.

Avant de commencer

Créez un fichier de réponses qui contient les paramètres de configuration que vous voulez modifier. Pour modifier les paramètres de configuration par défaut, éditez le fichier de réponses.

Pourquoi et quand exécuter cette tâche
Vous pouvez configurer l'agent à l'aide du fichier de réponses silencieux.

Procédure

1. Ouvrez le fichier de réponses silencieux disponible à l'emplacement suivant : *rép_install* `\samples\microsoft_cluster_server_silent_config.txt`
2. Pour la variable d'environnement **CTIRA_HOSTNAME**, indiquez le nom de cluster sous forme de valeur.
3. Sur chaque noeud du cluster, exécutez la commande suivante : **rép_install\BIN\microsoft_cluster_server-agent.bat config rép_install\samples\microsoft_cluster_server_silent_config.txt**

Que faire ensuite
Modifiez le compte utilisateur d'utilisateur local à utilisateur de domaine.

Modification du compte utilisateur

Après avoir configuré l'agent Microsoft Cluster Server, vous pouvez modifier le compte utilisateur d'utilisateur local à utilisateur de domaine.

Pourquoi et quand exécuter cette tâche
Par défaut, l'agent s'exécute avec le compte utilisateur local. Il doit s'exécuter avec l'utilisateur de domaine pour pouvoir surveiller tous les noeuds du cluster à partir d'un seul noeud.

Procédure

Pour modifier le compte utilisateur, procédez comme suit :

1. Ouvrez la fenêtre **IBM Performance Management**.
2. Cliquez sur l'agent avec le bouton droit de la souris, puis cliquez sur **Modifier le démarrage**.
3. Entrez les données d'identification de connexion du domaine.
4. Ouvrez le **Gestionnaire du cluster de basculement** sur l'un des noeuds et démarrez le service de cluster.

Résultats
L'agent est démarré sur le noeud.

Que faire ensuite
Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Performance Management, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de la surveillance de Microsoft Exchange

Vous devez configurer Monitoring Agent for Microsoft Exchange Server pour surveiller la disponibilité et les performances des serveurs Exchange.

Avant de commencer
Pour pouvoir configurer l'agent, veillez à exécuter les tâches suivantes :

- «Création d'utilisateurs», à la page 507
- «Affectation des droits d'administrateur à l'utilisateur d'Serveur Exchange », à la page 510
- «Attribution à l'utilisateur de Serveur Exchange des droits d'administrateur local», à la page 512
- «Configuration du Serveur Exchange pour l'accessibilité», à la page 514
- «Configuration de l'agent pour qu'il s'exécute sous l'utilisateur de domaine», à la page 515
- Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Microsoft Exchange Server.

Pourquoi et quand exécuter cette tâche

Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Vous pouvez démarrer l'agent Microsoft Exchange Server une fois installé. Une configuration manuelle est toutefois requise pour afficher les données pour tous les attributs d'agent.

- Pour configurer l'agent en local, voir «Configuration de l'agent en local», à la page 515.
- Pour configurer l'agent en utilisant le fichier de réponses silencieux, voir «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 520.

Création d'utilisateurs

Vous pouvez créer un utilisateur pour l'agent sur le serveur Exchange manuellement ou en exécutant l'utilitaire *Nouvel utilisateur*. Vous devez créer l'utilisateur sur chaque Serveur Exchange à surveiller.

Avant de commencer
Installez l'agent Microsoft Exchange Server. Pour créer un utilisateur, vous devez être un administrateur de domaine ayant des droits d'administration complets sur Microsoft Exchange Server.

Pourquoi et quand exécuter cette tâche

Utilisez l'une des procédures suivantes pour créer des utilisateurs :

- «Création d'utilisateur sur Exchange Server 2007 et 2010», à la page 508
- «Création d'utilisateur sur Exchange Server 2013», à la page 509
- «Création d'utilisateurs à l'aide de l'utilitaire Nouvel utilisateur», à la page 509

Création d'utilisateur sur Exchange Server 2007 et 2010

Vous devez créer un utilisateur pour l'agent sur Exchange Server 2007 et 2010 afin que l'agent puisse communiquer et s'authentifier avec le Serveur Exchange à surveiller.

Procédure

Pour créer un utilisateur, procédez comme suit :

1. Cliquez sur **Démarrer > Tous les programmes > Microsoft Exchange Server 2007 > Exchange Management Console**. La fenêtre **Exchange Management Console** s'ouvre.
2. Dans l'arborescence de la console, cliquez sur **Boîte aux lettres dans la Configuration du destinataire**.
3. Dans le panneau Action, cliquez sur **Nouvelle boîte aux lettres**. L'assistant Nouvelle boîte aux lettres s'ouvre.
4. Dans la page **Introduction**, cliquez sur **Boîte aux lettres de l'utilisateur**.
5. Dans la page **Type d'utilisateur**, cliquez sur **Nouvel utilisateur**.
6. Dans la page **Informations utilisateur**, renseignez les zones suivantes :

   Unité organisationnelle
   Par défaut, le conteneur Utilisateurs d'Active Directory s'affiche. Cliquez sur **Parcourir** pour modifier l'unité organisationnelle par défaut.

   Prénom
   Entrez le prénom de l'utilisateur.

   Second prénom
   Entrez les initiales de l'utilisateur.

   Nom
   Entrez le nom de l'utilisateur.

   Nom
   Par défaut, le prénom, les initiales et le nom de famille sont affichées dans cette zone. Vous pouvez modifier le nom.

   Nom de connexion de l'utilisateur (Nom principal de l'utilisateur)
   Entrez le nom que l'utilisateur devra saisir pour se connecter à la boîte aux lettres.

   Nom de connexion de l'utilisateur (versions antérieures à Windows 2000)
   Entrez le nom d'utilisateur compatible avec Microsoft Windows 2000 Server ou version antérieure.

   Mot de passe
   Entrez le mot de passe que l'utilisateur devra saisir pour se connecter à la boîte aux lettres.

   Confirmer le mot de passe
   Entrez le mot de passe que vous avez entré dans la zone **Mot de passe** une seconde fois.

   L'utilisateur doit changer de mot de passe à la prochaine connexion
   Cochez cette case si vous souhaitez que l'utilisateur réinitialise le mot de passe.
7. Dans la page **Paramètres de la boîte aux lettres**, renseignez les zones suivantes :

   Alias
   Par défaut, la valeur de cette zone est identique à celle que vous avez spécifiée dans la zone **Nom de connexion de l'utilisateur (Nom principal de l'utilisateur)**.

Base de données de la boîte aux lettres
Cliquez sur **Parcourir** pour ouvrir la fenêtre **Sélectionnez la base de données de boîtes aux lettres**. Sélectionnez la base de données que vous souhaitez utiliser, puis cliquez sur **OK**.

Stratégie de boîte aux lettres de dossier géré
Cochez cette case pour définir une stratégie de gestion des enregistrements de messagerie (MRM). Cliquez sur **Parcourir** pour sélectionner la stratégie de boîtes aux lettres de dossier géré à associer à cette boîte aux lettres.

Stratégie de boîte aux lettres Exchange ActiveSync
Cochez cette case pour définir une stratégie de boîte aux lettres Exchange ActiveSync. Cliquez sur **Parcourir** pour sélectionner la stratégie de boîtes aux lettres Exchange ActiveSync à associer à cette boîte aux lettres.

8. Sur la page **Nouvelle boîte aux lettres**, vérifiez le récapitulatif de configuration. Cliquez sur **Nouveau** pour créer une boîte aux lettres. Dans la page d'**achèvement**, la section de résumé indique si la boîte aux lettres a été créée.
9. Cliquez sur **Terminer**.

Que faire ensuite

Attribuez des droits d'administrateur à l'utilisateur Exchange que vous avez créé.

Création d'utilisateur sur Exchange Server 2013
Vous devez créer un utilisateur pour l'agent sur Exchange Server 2013 afin que l'agent puisse communiquer et s'authentifier avec le Serveur Exchange à surveiller.

Procédure

Pour créer un utilisateur sous Exchange Server 2013, procédez comme suit :

1. Connectez-vous au centre d'administration Exchange à l'aide de vos informations d'identification.
2. Sur la page **Centre d'administration Exchange**, cliquez sur **destinataires**, puis sur **boîtes aux lettres**.
3. Cliquez sur la flèche vers le bas en regard du signe (+) qui se trouve sous l'option **boîtes aux lettres**, puis cliquez sur **Boîte aux lettres de l'utilisateur**.
4. Dans la page "Nouvelle boîte aux lettres de l'utilisateur", cliquez sur **Nouvel utilisateur**, puis indiquez des valeurs pour les autres zones.
5. Cliquez sur **Sauvegarder**.

Que faire ensuite

Attribuez des droits d'administrateur à l'utilisateur Exchange que vous avez créé.

Création d'utilisateurs à l'aide de l'utilitaire Nouvel utilisateur
Vous pouvez exécuter l'utilitaire Nouvel utilisateur pour créer des utilisateurs sous Exchange Server 2007 ou version ultérieure. L'utilisateur créé à l'aide de cet utilitaire dispose de toutes les autorisations requises pour exécuter l'agent. Cet utilitaire s'installe en même temps que l'agent.

Avant de commencer
Vérifiez que l'agent est installé. Pour exécuter l'utilitaire Nouvel utilisateur, vous devez être un administrateur de domaine doté de tous les droits d'administrateur sur Microsoft Exchange Server.

Pourquoi et quand exécuter cette tâche
Lorsque vous exécutez cet utilitaire, l'utilisateur est créé dans le groupe Users d'Active Directory et dispose des droits d'accès suivants :

- Sous Exchange Server 2007 :
  - Administrateur local
  - Utilisateur du bureau à distance

  - Administrateur des destinataires Exchange
- Sous Exchange Server 2010, ou version ultérieure :
  - Administrateur local
  - Utilisateur du bureau à distance
  - Serveurs Exchange ou Gestion des dossiers publics.

Procédure

Pour exécuter l'utilitaire Nouvel utilisateur, procédez comme suit :

1. Cliquez deux fois sur le fichier `kexnewuser.exe` qui est disponible à l'emplacement suivant : *rép_install*\TMAITM6_x64, où *rép_install* correspond au chemin où l'agent est installé.
2. Dans la fenêtre **Nouvel utilisateur**, procédez comme suit :
   a) Entrez le **prénom** et le **nom** de l'utilisateur.

      Restriction : La longueur du prénom et du nom ne doit pas dépasser 28 caractères.

   b) Dans la zone **Nom de connexion de l'utilisateur**, entrez le nom que l'utilisateur doit taper lors de la connexion.

      Restriction : La longueur du nom de connexion de l'utilisateur ne doit pas dépasser 256 caractères.

   c) Dans la zone **Mot de passe**, entrez votre mot de passe.

   d) Dans la zone **Confirmez le mot de passe**, entrez à nouveau votre mot de passe.

   e) Sélectionnez **L'utilisateur doit changer de mot de passe à la prochaine connexion** si vous souhaitez que le mot de passe indiqué soit réinitialisé lors de la prochaine connexion de l'utilisateur.

   f) Cliquez sur **Suivant**.

   Les valeurs de configuration que vous spécifiez sont validées et des messages d'erreur s'affichent en cas de valeurs incorrectes.
3. Dans la liste des bases de données de la boîte aux lettres, sélectionnez la base de données de la boîte aux lettres requise, puis cliquez sur **Suivant**.

   Un récapitulatif des valeurs de configuration s'affiche.
4. Cliquez sur **Terminer**.

Résultats

Les paramètres sont enregistrés et l'utilisateur est créé.

Affectation des droits d'administrateur à l'utilisateur d'Serveur Exchange

L'utilisateur que vous avez créé pour l'agent Microsoft Exchange Server doit être un administrateur de domaine disposant de tous les droits d'administrateur sous Microsoft Exchange Server. Les droits d'administrateur sont nécessaires pour pouvoir accéder aux composants agent Microsoft Exchange Server.

Avant de commencer

Créez un utilisateur de Serveur Exchange dont la boîte aux lettres se trouve sur le Serveur Exchange qui est surveillé.

Pourquoi et quand exécuter cette tâche

Utilisez l'une des procédures ci-dessous pour affecter des droits administrateur à l'utilisateur :

- «Affectation des droits d'administrateur sous Exchange Server 2007», à la page 511
- «Affectation des droits d'administrateur sous Exchange Server 2010», à la page 511
- «Affectation des droits d'administrateur sous Exchange Server 2013», à la page 511
- «Affectation des droits d'administrateur sous Exchange Server 2016», à la page 512

Affectation des droits d'administrateur sous Exchange Server 2007
Sous Exchange Server 2007, vous devez affecter à l'utilisateur des droits d'Administrateur des destinataires Exchange.

Procédure

1. Cliquez sur **Démarrer > Tous les programmes > Microsoft Exchange Server 2007 > Exchange Management Console**. La fenêtre **Exchange Management Console** s'ouvre.
2. Dans l'arborescence de la console, cliquez sur **Configuration de l'organisation**.
3. Dans le panneau Action, cliquez sur **Ajouter un administrateur Exchange**.
4. Sur la page **Ajouter un administrateur Exchange**, cliquez sur **Parcourir**. Sélectionnez le nouvel utilisateur que vous avez créé, puis sélectionnez le rôle **Administrateur des destinataires Exchange**.
5. Cliquez sur **Ajouter**.
6. Sur la page **Achèvement**, cliquez sur **Terminer**.

Affectation des droits d'administrateur sous Exchange Server 2010
Sous Exchange Server 2010, vous devez affecter à l'utilisateur les droits Serveurs Exchange ou Gestion des dossiers publics.

Procédure

1. Connectez-vous au serveur Exchange avec des privilèges d'administrateur.
2. Cliquez sur **Démarrer > Outils d'administration > Gestionnaire de serveur.**
3. Développez les **Outils**.
4. Cliquez sur **Utilisateurs et ordinateurs Active Directory**.
5. Développez **Domaine**, puis cliquez sur **Groupes de sécurité Microsoft Exchange Security**.
6. Cliquez avec le bouton droit de la souris sur **Serveurs Exchange ou Gestion des dossiers publics** et sélectionnez **Propriétés**.
7. Dans la fenêtre **Propriétés des serveurs Exchange ou Propriétés de la gestion des dossiers publics**, accédez à **Membres** et cliquez sur **Ajouter**.
8. De la liste des utilisateurs, sélectionnez l'utilisateur que vous voulez ajouter au groupe, puis cliquez sur **OK**.
9. Cliquez sur **OK**.

Affectation des droits d'administrateur sous Exchange Server 2013
Sous Exchange Server 2013, vous devez affecter à l'utilisateur les droits Serveurs Exchange ou Gestion des dossiers publics.

Procédure

1. Connectez-vous au serveur Exchange avec des privilèges d'administrateur.
2. Cliquez sur **Démarrer > Outils d'administration > Gestionnaire de serveur.**
3. Développez les **Outils**.
4. Cliquez sur **Utilisateurs et ordinateurs Active Directory**.
5. Développez **Domaine**, puis cliquez sur **Groupes de sécurité Microsoft Exchange Security**.
6. Cliquez avec le bouton droit de la souris sur **Serveurs Exchange ou Gestion des dossiers publics** et sélectionnez **Propriétés**.
7. Dans la fenêtre **Propriétés des serveurs Exchange ou Propriétés de la gestion des dossiers publics**, accédez à **Membres** et cliquez sur **Ajouter**.
8. De la liste des utilisateurs, sélectionnez l'utilisateur que vous voulez ajouter au groupe, puis cliquez sur **OK**.
9. Cliquez sur **OK**.

Affectation des droits d'administrateur sous Exchange Server 2016
Sous Exchange Server 2016, vous devez affecter à l'utilisateur les droits Serveurs Exchange ou Gestion des dossiers publics.

Procédure

1. Connectez-vous au serveur Exchange avec des privilèges d'administrateur.
2. Cliquez sur **Démarrer > Outils d'administration > Gestionnaire de serveur.**
3. Développez les **Outils**.
4. Cliquez sur **Utilisateurs et ordinateurs Active Directory**.
5. Développez **Domaine**, puis cliquez sur **Groupes de sécurité Microsoft Exchange Security**.
6. Cliquez avec le bouton droit de la souris sur **Serveurs Exchange ou Gestion des dossiers publics** et sélectionnez **Propriétés**.
7. Dans la fenêtre **Propriétés des serveurs Exchange ou Propriétés de la gestion des dossiers publics**, accédez à **Membres** et cliquez sur **Ajouter**.
8. De la liste des utilisateurs, sélectionnez l'utilisateur que vous voulez ajouter au groupe, puis cliquez sur **OK**.
9. Cliquez sur **OK**.

Que faire ensuite
Attribuez à l'utilisateur des droits d'administrateur local sur l'ordinateur sur lequel est installé le Serveur Exchange .

Attribution à l'utilisateur de Serveur Exchange des droits d'administrateur local

Pour accéder aux données du Serveur Exchange , l'utilisateur que vous avez créé pour l'agent Microsoft Exchange Server doit être un administrateur local de l'ordinateur sur lequel le Serveur Exchange est installé.

Avant de commencer
Créez un utilisateur de Serveur Exchange .

Pourquoi et quand exécuter cette tâche
Utilisez l'une des procédures ci-dessous pour attribuer à l'utilisateur des droits d'administrateur local :

- «Attribution à l'utilisateur des droits d'administrateur local sur l'ordinateur Windows 2003», à la page 512
- «Attribution à l'utilisateur des droits d'administrateur local sur l'ordinateur Windows 2008», à la page 513
- «Attribution à l'utilisateur des droits d'administrateur local sur l'ordinateur Windows 2012», à la page 513
- «Attribution à l'utilisateur des droits d'administrateur local sur l'ordinateur Windows 2016», à la page 513

Attribution à l'utilisateur des droits d'administrateur local sur l'ordinateur Windows 2003
Vous devez attribuer à l'utilisateur que vous avez créé pour le Serveur Exchange des droits d'administrateur local de l'ordinateur qui s'exécute sur le système d'exploitation Windows 2003 et sur lequel le Serveur Exchange est installé.

Procédure

1. Cliquez avec le bouton droit de la souris sur **Poste de travail** sur le bureau de l'ordinateur et sélectionnez **Gérer**.
2. Développez **Utilisateurs et groupes locaux**.
3. Cliquez sur **Groupes**.

4. Cliquez deux fois sur **Administrateurs** pour afficher la fenêtre **Propriétés des administrateurs**.
5. Cliquez sur **Ajouter**.
6. Sélectionnez **Tout l'annuaire** dans la liste **Rechercher dans**.
7. Sélectionnez le nom de l'utilisateur que vous avez créé et cliquez sur **Ajouter**.
8. Cliquez sur **OK**.
9. Cliquez sur **OK**.

Attribution à l'utilisateur des droits d'administrateur local sur l'ordinateur Windows 2008
Vous devez attribuer à l'utilisateur que vous avez créé pour le Serveur Exchange des droits d'administrateur local de l'ordinateur qui s'exécute sur le système d'exploitation Windows Server 2008 et sur lequel le Serveur Exchange est installé.

Procédure

1. Cliquez sur **Démarrer > Outils d'administration > Gestionnaire de serveur**.
2. Dans le panneau de navigation, développez **Configuration**.
3. Cliquez deux fois sur **Utilisateurs et groupes locaux**.
4. Cliquez sur **Groupes**.
5. Cliquez avec le bouton droit de la souris sur le groupe auquel vous voulez ajouter le compte utilisateur, puis cliquez sur **Ajouter au groupe**.
6. Cliquez sur **Ajouter**, puis tapez le nom du compte utilisateur.
7. Cliquez sur **Vérifier les noms**, puis cliquez sur **OK**.

Attribution à l'utilisateur des droits d'administrateur local sur l'ordinateur Windows 2012
Vous devez attribuer à l'utilisateur que vous avez créé pour le Serveur Exchange des droits d'administrateur local de l'ordinateur qui s'exécute sur le système d'exploitation Windows Server 2012 et sur lequel le Serveur Exchange est installé.

Procédure

1. Cliquez sur **Démarrer > Gestionnaire de serveur**.
2. Dans la page **Tableau de bord du Gestionnaire de serveur**, cliquez sur **Outils > Gestion de l'ordinateur**.
3. Dans le panneau de navigation de la page **Gestion de l'ordinateur**, développez **Utilisateurs et groupes locaux**, puis cliquez sur **Utilisateurs**.
4. Dans la liste des utilisateurs, cliquez avec le bouton droit de la souris sur l'utilisateur auquel vous voulez attribuer des droits d'administrateur, puis cliquez sur **Propriétés**.
5. Cliquez sur l'onglet **Appartient à**, puis sur **Ajouter**.
6. Dans la page **Sélectionner un groupe**, entrez `Administrateurs`, puis cliquez sur **OK**.
7. Cliquez sur **Appliquer** et sur **OK**.

Attribution à l'utilisateur des droits d'administrateur local sur l'ordinateur Windows 2016
Vous devez attribuer à l'utilisateur que vous avez créé pour le Serveur Exchange des droits d'administrateur local de l'ordinateur qui s'exécute sur le système d'exploitation Windows Server 2016 et sur lequel le Serveur Exchange est installé.

Procédure

1. Cliquez sur **Démarrer > Gestionnaire de serveur**.
2. Dans la page **Tableau de bord du Gestionnaire de serveur**, cliquez sur **Outils > Gestion de l'ordinateur**.
3. Dans le panneau de navigation de la page **Gestion de l'ordinateur**, développez **Utilisateurs et groupes locaux**, puis cliquez sur **Utilisateurs**.

4. Dans la liste des utilisateurs, cliquez avec le bouton droit de la souris sur l'utilisateur auquel vous voulez attribuer des droits d'administrateur, puis cliquez sur **Propriétés**.
5. Cliquez sur l'onglet **Appartient à**, puis sur **Ajouter**.
6. Dans la page **Sélectionner un groupe**, entrez `Administrateurs`, puis cliquez sur **OK**.
7. Cliquez sur **Appliquer** et sur **OK**.

Configuration du Serveur Exchange pour l'accessibilité

Pour vérifier l'accessibilité, l'agent Microsoft Exchange Server envoie un message électronique au serveur et mesure le temps nécessaire pour recevoir une réponse automatique. Avant de démarrer l'agent, vous devez configurer le Serveur Exchange pour la réponse automatique aux messages électroniques.

Avant de commencer

Avant de configurer le Serveur Exchange , vérifiez que les tâches suivantes ont été effectuées :

- Une boîte aux lettres est créée pour l'utilisateur sur le Serveur Exchange que vous souhaitez surveiller.
- L'utilisateur que vous avez créé pour l'agent est un utilisateur de domaine.
- Les serveurs de votre organisation Microsoft Exchange sont configurés pour le flux de messagerie entre les serveurs.

Procédure

Utilisez la procédure suivante pour chaque Serveur Exchange dont vous souhaitez vérifier l'accessibilité :

1. Connectez-vous à Microsoft Outlook en indiquant les données d'identification de l'utilisateur que vous avez créé.
2. Cliquez sur le bouton **Suivant** de la fenêtre **Bienvenue**.
3. Sélectionnez **Oui**, puis cliquez sur **Suivant**.
4. Dans la zone **Microsoft Exchange Server**, indiquez le nom du Serveur Exchange .
5. Dans la zone **Boîte aux lettres**, entrez le nom de l'utilisateur que vous avez créé.
6. Cliquez sur **Terminer**.
7. Cliquez sur **OK**.
8. Cliquez sur **Outils > Règles et alertes > Nouvelle règle**.
9. Sélectionnez **Commencer à partir d'une règle vide**.
10. Sélectionnez **Vérifier les messages à leur arrivée**, puis cliquez sur **Suivant**.
11. Sélectionnez les options suivantes :
    - **Lorsque mon nom est dans la zone A :**
    - **Qui contiennent des mots spécifiques dans l'objet ou dans le corps**
12. Sous **Etape 2** dans cette fenêtre, cliquez sur **Mots spécifiques**.
13. Dans la zone **Spécifier un mot/une expression à rechercher dans l'objet/le corps du texte**, entrez `AVAILABILITY CHECK`.
14. Cliquez sur **Ajouter**.
15. Cliquez sur **OK**, puis sur **Suivant**.
16. Sélectionnez **Faire répondre le serveur avec un message spécifique** et cliquez sur **un message spécifique**.
17. Dans l'éditeur de message électronique, entrez le texte suivant dans la zone d'objet du message : `CHECK RECEIVED: MAILBOX AVAILABLE.`
18. Fermez l'éditeur de message électronique et cliquez sur **Oui** pour sauvegarder ces modifications.
19. Cliquez sur **Suivant**.
20. Lorsque vous êtes invité à définir des exceptions éventuelles, n'indiquez aucune restriction.
21. Cliquez sur **Suivant**.
22. Cliquez sur **Terminer**, puis sur **OK**.

Que faire ensuite
Configurez l'agent Microsoft Exchange Server.

Configuration de l'agent pour qu'il s'exécute sous l'utilisateur de domaine

Par défaut, l'agent Microsoft Exchange Server est configuré pour s'exécuter sous le compte de l'utilisateur local mais il doit s'exécuter sous le compte de l'utilisateur de domaine que vous avez créé.

Avant de commencer
Assurez-vous que :

- L'utilisateur que vous avez créé est un utilisateur de domaine qui dispose des droits d'administrateur local.
- L'utilisateur dispose de droits d'administrateur sur le serveur où l'agent est installé.

Pourquoi et quand exécuter cette tâche
Lorsque l'agent s'exécute sous l'utilisateur de domaine, il peut surveiller tous les composants du Serveur Exchange .

Procédure

Pour modifier l'utilisateur sous lequel l'agent s'exécute, effectuez les étapes suivantes :

1. Exécutez la commande suivante pour vérifier l'ID utilisateur qui est utilisé pour démarrer l'agent.
   `rép_install\InstallITM\KinCinfo.exe -r`
2. Si l'agent de surveillance a été démarré avec un ID utilisateur qui n'appartient pas au groupe Administrateur, arrêtez l'agent.
3. Ouvrez la fenêtre **Manage Monitoring Services**.
4. Cliquez avec le bouton droit de la souris sur l'instance de l'agent, puis cliquez sur **Modifier le démarrage**.
5. Indiquez l'ID utilisateur complet sous la forme `<Domaine\ID_utilisateur>`, puis indiquez le mot de passe.
6. Démarrez l'agent de surveillance.

Configuration de l'agent en local

Vous pouvez configurer l'agent en local dans la fenêtre IBM Cloud Application Performance Management.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Monitoring Agent for Microsoft Exchange Server**, puis cliquez sur **Configuration de l'agent**.

   Avertissement : Cliquez sur **Reconfigurer** si **Configuration de l'agent** est désactivé.
3. Dans la fenêtre **Monitoring Agent for Microsoft Exchange Server: Configuration avancée de l'agent**, cliquez sur **OK**.
4. Dans la fenêtre **Configuration d'agent**, procédez comme suit :
   a) Cliquez sur l'onglet **Propriétés Exchange Server**, puis indiquez des valeurs pour les paramètres de configuration. Lorsque vous cliquez sur **OK**, les valeurs spécifiées sont validées.
   b) Cliquez sur l'onglet **Surveillance des services Exchange**, puis indiquez des valeurs pour les paramètres de configuration. Lorsque vous cliquez sur **OK**, les valeurs spécifiées sont validées.
   c) Cliquez sur l'onglet **Propriétés de configuration avancées**, puis indiquez des valeurs pour les paramètres de configuration. Lorsque vous cliquez sur **OK**, les valeurs spécifiées sont validées.

Pour plus d'informations sur les paramètres de configuration dans chaque onglet de la fenêtre **Configuration d'agent**, consultez les rubriques suivantes :

- «Paramètres de configuration des propriétés du serveur Exchange», à la page 516
- «Paramètres de configuration des services Exchange», à la page 517
- «Paramètres de configuration de l'accessibilité», à la page 518

Pour plus d'informations sur la validation des valeurs de configuration, voir «Validation des valeurs de configuration», à la page 519.

5. Recyclez l'agent.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Restriction : Dans le tableau de bord Cloud APM, les instances de l'un des types de composant Exchange uniquement (Microsoft Exchange Server ou Microsoft Exchange Server 2013) s'affichent sous Mes composants.

Paramètres de configuration des propriétés du serveur Exchange

Dans l'onglet **Propriétés Exchange Server** de la fenêtre **Configuration d'agent**, vous pouvez configurer les propriétés du serveur Exchange, comme le nom de serveur, le nom de domaine et le nom d'utilisateur.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de l'onglet **Propriétés Exchange Server**.

Tableau 173. Noms et descriptions des paramètres de configuration de l'onglet Propriétés Exchange Server

Nom de paramètre	Description	Zone obligatoire	Exemples
Nom du serveur Exchange	Nom du Serveur Exchange . Pendant l'installation du serveur Exchange, le nom par défaut du serveur Exchange est le nom d'hôte du serveur Windows. Si vous modifiez le nom par défaut, vous devez alors utiliser le nouveau nom lors de la configuration de l'agent Exchange Server. **A faire :** Dans les environnements répartis ou en cluster, indiquez le nom du serveur de boîtes aux lettres pour Exchange Server 2007.	Oui **Important :** N'indiquez aucune valeur si l'agent est installé sur un serveur disposant d'un cluster à copie unique doté de plus de deux noeuds.	Si le nom du serveur Exchange est `popcorn`, entrez `popcorn` dans la zone **Nom du serveur Exchange**.
Nom du domaine Exchange	Nom du domaine où le Serveur Exchange est installé.	Oui	Si le serveur Exchange se trouve dans le domaine `LAB.XYZ.com`, entrez le nom qui précède le premier point, LAB par exemple.

Tableau 173. Noms et descriptions des paramètres de configuration de l'onglet Propriétés Exchange Server (suite)

Nom de paramètre	Description	Zone obligatoire	Exemples
Nom d'utilisateur Exchange	Nom de l'utilisateur qui est configuré pour accéder au Serveur Exchange . **A faire :** L'utilisateur doit avoir une boîte aux lettres sur le même serveur Exchange.	Oui	
Mot de passe de l'utilisateur Exchange	Mot de passe de l'utilisateur qui est configuré pour accéder au Serveur Exchange .	Oui	
Confirmer le mot de passe	Même mot de passe que celui indiqué pour l'utilisateur du serveur Exchange.	Oui	
Nom de profil MAPI Exchange	Les profils MAPI sont les paramètres de configuration principaux requis pour l'accès au serveur Exchange. Cette zone est désactivée si vous utilisez un agent Microsoft Exchange Server 64 bits pour surveiller le Serveur Exchange 2007 ou version ultérieure.	Non	
Configuration en cluster	Cochez cette case pour configurer le agent Microsoft Exchange Server dans un environnement cluster.	Sans objet	
Nom du serveur en cluster	Nom du serveur en cluster. Cette zone est activée lorsque vous sélectionnez la case à cocher **Configuration en cluster**.	Oui, si la zone est activée.	`SCCCluster`
ID du sous-système Exchange	Nom du noeud de serveur en cluster. Cette zone est activée lorsque vous sélectionnez la case à cocher **Configuration en cluster**.	Oui, si la zone est activée.	`node1`
Répertoire de données historiques de l'agent Exchange	Emplacement sur le disque où sont stockées les données d'historique. Cette zone est activée lorsque vous sélectionnez la case à cocher **Configuration en cluster**.	Oui, si la zone est activée.	`c:\history`

Paramètres de configuration des services Exchange
Dans l'onglet **Surveillance des services Exchange** de la fenêtre **Configuration d'agent**, vous pouvez sélectionner les services Exchange pour connaître l'état du serveur Exchange.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de l'onglet **Surveillance des services Exchange**.

Tableau 174. Noms et descriptions des paramètres de configuration de l'onglet Surveillance des services Exchange

Nom de paramètre	Description	Zone obligatoire
Services Exchange	Sélectionnez les services Exchange dans la liste des services disponibles et cliquez sur la flèche pour déplacer les services sélectionnés vers la liste **Services Configured for Server Status** de sorte que l'agent Microsoft Exchange Server puisse les surveiller. **A faire :** La liste des services disponibles change en fonction de la version du serveur Exchange et des rôles installés.	Sans objet
Services configurés pour le statut du serveur	Les services déjà disponibles dans cette liste déterminent le statut du Serveur Exchange . Ces services sont obligatoires et ne peuvent pas être déplacés de la liste **Services Configured for Server Status** vers la liste **Services Exchange**. Vous pouvez ajouter des services à la liste **Services Configured for Server Status** en déplaçant les services depuis la liste **Services Exchange**. Vous pouvez également redéplacer ces services supplémentaires vers la liste **Services Exchange**.	Sans objet

Paramètres de configuration de l'accessibilité

Dans l'onglet **Advanced Configuration Properties** de la fenêtre **Configuration d'agent**, vous pouvez configurer les paramètres liés à l'accessibilité, comme l'adresse électronique cible et l'intervalle d'accessibilité.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de l'onglet **Propriétés de configuration avancée**.

Tableau 175. Noms et descriptions des paramètres de configuration de l'onglet Propriétés de configuration avancées

Nom de paramètre	Description	Zone obligatoire
Activer la surveillance de l'accessibilité de la boîte aux lettres	Sélectionnez cette case à cocher si vous souhaitez que l'agent capture les données de mesure de l'accessibilité.	Sans objet
Adresse électronique cible	Adresse électronique permettant de vérifier l'accessibilité. Séparez les adresses électroniques par des points-virgules (;). **Restriction :** Le nombre total de caractères dans cette zone ne doit pas dépasser 1023.	Oui, si cette zone est activée.
Intervalle de transmission des courriers électroniques (en secondes)	Délai d'attente (en secondes) de l'agent Exchange Server entre l'envoi de courriers électroniques.	Oui, si cette zone est activée.
Délai d'attente de transmission des courriers électroniques (secondes)	Intervalle (en secondes) pendant lequel l'agent attend une réponse au courrier électronique envoyé pour tester si le serveur de boîte aux lettres est accessible.	Non

Tableau 175. Noms et descriptions des paramètres de configuration de l'onglet Propriétés de configuration avancées (suite)

Nom de paramètre	Description	Zone obligatoire
Activer la surveillance des détails de la boîte aux lettres	Sélectionnez cette case à cocher si vous souhaitez collecter des données pour les mesures détaillées de la boîte aux lettres.	Sans objet
Heure de début de la collecte des détails de la boîte aux lettres	Heure (au format hh:mm:ss) à laquelle les indicateurs de détails de la boîte aux lettres sont collectés.	Non
Intervalle de collecte des détails de la boîte aux lettres (en secondes)	Intervalle (en secondes) entre les collectes des indicateurs de détails de la boîte aux lettres.	Non
Durée de collecte des journaux d'événements (en minutes)	Durée (en minutes) pendant laquelle l'agent collecte des enregistrements d'événements.	Non
Nombre maximal d'événements	Nombre maximal d'enregistrements d'événements à collecter. La collecte des enregistrements d'événements s'arrête lorsque le nombre d'enregistrements d'événements collectés dépasse le nombre maximal.	Non
Intervalle de collecte (en secondes)	Intervalle (en secondes) entre les cycles de l'agent.	Non
Intervalle de topologie Exchange (en secondes)	Intervalle (en secondes) entre les collectes des informations détaillées sur la topologie.	Non
Intervalle de collecte de suivi des messages (heures)	Intervalle (en heures) de collecte des journaux de suivi des messages. **Restriction :** La valeur d'intervalle doit être comprise entre 1 et 12. Si vous indiquez une valeur d'intervalle supérieure à 12, la valeur enregistrée sera 12. Si vous entrez une valeur non valide qui contient des caractères alphabétiques ou des caractères spéciaux, la valeur est sauvegardée comme étant 0, ce qui signifie que la collecte de suivi des messages est désactivée. Cette zone est désactivée si l'une des conditions suivantes est vraie : • Le rôle Mailbox Server ou Hub Transport n'est pas installé sur le serveur Exchange. • La fonction de suivi de messages est désactivée sur le Serveur Exchange .	Non

Validation des valeurs de configuration

Les valeurs que vous indiquez lors de la configuration de l'agent sont validées. La validation consiste à vérifier que les valeurs sont spécifiées pour tous les paramètres obligatoires et que certaines conditions sont remplies, comme les droits d'administrateur local de l'utilisateur.

Le tableau ci-après indique les tests de validation appliqués aux valeurs de configuration spécifiées.

Tableau 176. Tests de validation	
Test de validation	**Vérifie si**
Nom du serveur Exchange	Le nom du serveur de boîte aux lettres de l'utilisateur correspond au nom Serveur Exchange indiqué.
Droits du serveur Exchange	L'utilisateur dispose des droits requis du Serveur Exchange . Sur le Serveur Exchange 2007, l'utilisateur doit avoir les droits d'administrateur de destinataire et sur Serveur Exchange 2010, ou version ultérieure, l'utilisateur doit avoir des droits de gestion de destinataire.
Administrateur local	L'utilisateur dispose de droits d'administrateur local.
Connexion au service d'agent	Le service d'agent est configuré pour s'exécuter avec le compte utilisateur indiqué.

En cas d'échec d'un ou plusieurs tests de validation, un message d'erreur est généré. Vous devez spécifier des valeurs pour tous les paramètres obligatoires faute de quoi vous ne pourrez pas sauvegarder les valeurs configurées.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour définir des valeurs différentes pour les paramètres de configuration.

Pourquoi et quand exécuter cette tâche

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

1. Ouvrez le fichier `msex_silent_config.txt` situé dans *`rép_install`*`\samples` et spécifiez des valeurs pour tous les paramètres obligatoires.

   Vous pouvez également modifier les valeurs par défaut d'autres paramètres.
2. Exécutez la commande suivante :

   `rép_install\BIN\msexch-agent.bat config rép_install\samples \msex_silent_config.txt`

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Restriction : Dans le tableau de bord Cloud APM, les instances de l'un des types de composant Exchange uniquement (Microsoft Exchange Server ou Microsoft Exchange Server 2013) s'affichent sous Mes composants.

Configuration des variables de l'environnement local pour l'agent

Vous pouvez configurer les variables de l'environnement local pour l'agent Microsoft Exchange Server afin d'activer ou de désactiver la régulation d'événement pour les événements en double.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **Agents IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, dans le menu **Actions**, cliquez sur **Advanced** > **Edit ENV File**.

3. Dans le fichier KEXENV, modifiez les valeurs des variables d'environnement suivantes :

   EX_EVENT_THROTTLE_ENABLE
   Cette variable vous permet de réguler les événements en double. La valeur par défaut est `False`. Pour activer la régulation d'événement afin d'éviter l'apparition d'événements en double, affectez à cette variable la valeur True.

   EX_EVENT_THROTTLE_DURATION
   Cette variable indique la durée (en minutes) de la régulation d'événement. La valeur par défaut est `0` minutes.

Configuration de la surveillance de Microsoft Hyper-V

Lorsque vous installez Monitoring Agent for Microsoft Hyper-V Server, il est configuré et démarré automatiquement avec les paramètres de configuration par défaut. Utilisez le fichier de réponses silencieux pour modifier les paramètres de configuration par défaut.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Microsoft Hyper-V Server.
- Créez un fichier de réponses qui contient les paramètres de configuration que vous voulez modifier.
- Pour afficher les données de machine virtuelle sur la page de la machine virtuelle, assurez-vous d'avoir installé le composant d'intégration et l'agent de système d'exploitation sur chaque machine virtuelle. Pour les machines virtuelles exécutées sur le système Linux, veillez à exécuter les tâches suivantes :
  - Mettez à niveau le système Linux.
  - Installez le package `hypervkvpd` ou `hyperv-daemons rpm` mis à jour sur la machine virtuelle.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'agent lorsqu'il est arrêté ou en cours d'exécution. L'agent reste au même état après la configuration. Par exemple, si l'agent est en cours d'exécution, il reste à l'état en cours d'exécution après la configuration.

Important : Pour l'édition 8.1.3 de Performance Management, la fenêtre de configuration d'agent est supprimée car elle n'est pas requise. La fenêtre de configuration d'agent est disponible pour la version 8.1.2 ou antérieure de Performance Management.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Procédure

Pour configurer l'agent, procédez comme suit :

1. Ouvrez le fichier `microsoft_hyper-v_server_silent_config.txt` situé dans *rép_install* `\samples` et spécifiez des valeurs pour tous les paramètres obligatoires.

   Vous pouvez également modifier les valeurs par défaut d'autres paramètres.
2. Ouvrez l'invite de commande et entrez la commande suivante :

   rép_install\BIN\microsoft_hyper-v_server-agent.bat config rép_install \samples\microsoft_hyper-v_server_silent_config.txt

   Le fichier de réponses contient les paramètres suivants :

   - KHV_DIRECTOR_PORT

- KHV_DIRECTOR_SERVER

A faire : La configuration d'agent est organisée par groupes :

Configuration d'IBM Systems Director (IBM_DIRECTOR_CONFIGURATION)
Les éléments de configuration définis dans ce groupe sont toujours présents dans la configuration de l'agent. Ce groupe définit des informations qui s'appliquent à l'ensemble de l'agent.

Numéro de port d'IBM Systems Director Server (KHV_DIRECTOR_PORT)
Numéro de port d'IBM Systems Director Server. La valeur par défaut est aucun.

Nom d'hôte d'IBM Systems Director Server (KHV_DIRECTOR_SERVER)
Nom d'hôte ou adresse IP du serveur IBM Systems Director Server qui gère l'environnement. La valeur par défaut est aucun.

3. Démarrez l'agent s'il est à l'état arrêté.

Que faire ensuite
Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Saisie de la stratégie de sécurité locale pour l'exécution de Monitoring Agent for Microsoft Hyper-V Server sous Windows par un utilisateur non-administrateur

Des stratégies de sécurité locales sont disponibles pour permettre à un utilisateur non-administrateur d'exécuter Monitoring Agent for Microsoft Hyper-V Server sous Windows.

Pourquoi et quand exécuter cette tâche

La combinaison des deux stratégies de sécurité locales suivantes permet à un utilisateur non-administrateur d'exécuter l'agent Microsoft Hyper-V Server sous Windows. Utilisez les deux stratégies suivantes permettant à l'agent Microsoft Hyper-V Server de démarrer/arrêter, configurer et vérifier les données.

- Déboguer les programmes
- Ouvrir une session en tant que service

Les groupes d'attributs suivants doivent également disposer de droits d'administrateur pour obtenir les données sur le portail APM :

- Disponibilité
- Migration
- Migration de la machine virtuelle sans le cluster
- Migration du stockage de la machine virtuelle

Procédez comme suit pour accorder les droits de sécurité locale à un utilisateur non-administrateur.

Procédure

1. Installez l'agent Microsoft Hyper-V Server en tant qu'administrateur local.
2. Ajoutez l'utilisateur non-administrateur dans le répertoire `rép_install` et accordez-lui les droits suivants :
   a) Accordez un accès complet au registre `HKEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring`.
   b) Accordez un accès en lecture au registre `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Windows NT\CurrentVersion\Perflib` pour l'utilisateur non-administrateur.
   c) Accordez un accès complet au répertoire `rép_install` pour l'utilisateur non-administrateur.
3. Accédez au menu **Démarrer** et exécutez la commande **`secpol.msc`** pour ouvrir les stratégies de sécurité locale.

4. Pour ajouter un utilisateur non-administrateur aux stratégies, voir «Octroi de droits de la stratégie de sécurité locale», à la page 523.
5. Pour ajouter un utilisateur non-administrateur au groupe d'utilisateurs administrateurs Hyper-V, voir «Ajout d'un utilisateur non-administrateur dans le groupe d'utilisateurs administrateurs Hyper-V», à la page 524.
6. Pour ajouter un utilisateur non-administrateur au groupe d'utilisateurs Analyseur de performances, voir «Ajout d'un utilisateur non-administrateur dans le groupe d'utilisateurs Performance Business Monitor», à la page 525.
7. Pour modifier le droit de sécurité DCOM pour un utilisateur non-administrateur, voir «Modification des droits DCOM», à la page 524.
8. Redémarrez l'agent Microsoft Hyper-V Server et vérifiez les données sur le portail APM.

Octroi de droits de la stratégie de sécurité locale

Pour démarrer/arrêter, configurer et vérifier les données de l'agent Microsoft Hyper-V Server, vous devez octroyer des droits d'accès aux deux stratégies de sécurité locales suivantes : Déboguer les programmes et Ouvrir une session en tant que service.

Octroi du droit Déboguer les programmes

Pourquoi et quand exécuter cette tâche

Pour accorder le droit Déboguer les programmes, suivez la procédure ci-dessous.

Procédure

1. Cliquez sur **Démarrer > Panneau de configuration > Outils d'administration > Stratégie de sécurité locale**. La fenêtre **Stratégie de sécurité locale** s'affiche.
2. Développez **Stratégies locales**, puis cliquez sur **Attribution des droits utilisateur**. La liste des stratégies s'affiche.
3. Cliquez deux fois sur la stratégie **Déboguer les programmes**. La fenêtre **Propriétés de Déboguer les programmes** apparaît.
4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre **Sélectionner des utilisateurs ou des groupes** apparaît.
5. Dans la zone **Entrer les noms d'objet à sélectionner**, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **Appliquer**, puis sur **OK**.

Octroi du droit Ouvrir une session en tant que service

Pourquoi et quand exécuter cette tâche

Pour accorder le droit Ouvrir une session en tant que Service, suivez la procédure ci-dessous.

Procédure

1. Cliquez sur **Démarrer > Outils d'administration > Stratégie de sécurité locale**. La fenêtre **Stratégie de sécurité locale** s'affiche.
2. Développez **Stratégies locales**, puis cliquez sur **Attribution des droits utilisateur**. La liste des stratégies s'affiche.
3. Cliquez deux fois sur la stratégie **Ouvrir une session en tant que service**. La fenêtre **Propriétés de Ouvrir une session en tant que service** apparaît.
4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre **Sélectionner des utilisateurs ou des groupes** apparaît.
5. Dans la zone **Entrer les noms d'objet à sélectionner**, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **Appliquer**, puis sur **OK**.

Modification des droits DCOM

Vous devez modifier les droits DCOM pour pouvoir exécuter l'agent Microsoft Hyper-V Server avec un accès utilisateur non-administrateur.

Pourquoi et quand exécuter cette tâche

Pour modifier les droits DCOM, vérifiez que l'utilisateur possède les droits appropriés lui permettant de démarrer le serveur DCOM. Pour modifier les droits, procédez comme suit.

Procédure

1. A l'aide de la commande **Regedit**, accédez à la valeur de registre `HKCR\Clsid\*clsid value`.

   Remarque : Lorsque vous configurez l'agent avec un utilisateur non-administrateur, la valeur CLSID s'affiche dans l'observateur d'événements, sous l'ID d'événement 10016.
2. Dans le panneau Editeur du registre, cliquez deux fois sur **Par défaut**.
3. Dans la boîte de dialogue **Modification de la chaîne**, copiez la chaîne Données de la valeur.
4. Cliquez sur **Démarrer > Panneau de configuration > Outils d'administration > Services de composants**.
5. Dans la fenêtre **Services de composants**, développez **Services de composants > Ordinateurs > Mon ordinateur** et cliquez deux fois sur **DCOM**.
6. Dans le panneau de configuration DCOM, localisez la chaîne copiée (nom du programme), cliquez avec le bouton droit de la souris sur le nom du programme et cliquez sur **Propriétés**.
7. Dans la fenêtre **Propriétés**, cliquez sur l'onglet **Sécurité**.
8. Dans la zone **Autorisations d'exécution et d'activation**, sélectionnez **Personnaliser**, puis cliquez sur **Modifier**. La fenêtre **Autorisations d'exécution et d'activation** s'affiche.
9. Cliquez sur **Ajouter**, entrez un utilisateur non-administrateur dans la liste des droits, puis cliquez sur **OK**.
10. Cochez la case **Autoriser** en regard de Exécution locale et Activation locale, puis cliquez sur **OK**.

Ajout d'un utilisateur non-administrateur dans le groupe d'utilisateurs administrateurs Hyper-V

Vous devez ajouter un utilisateur non-administrateur dans le groupe d'utilisateurs administrateurs Hyper-V pour obtenir des données sur le portail APM.

Pourquoi et quand exécuter cette tâche

Pour ajouter un utilisateur non-administrateur dans le groupe d'utilisateurs administrateurs Hyper-V, procédez comme suit.

Procédure

1. Cliquez sur **Démarrer > Panneau de configuration > Outils d'administration > Gestion de l'ordinateur**. La fenêtre **Gestion de l'ordinateur** s'ouvre.
2. Cliquez sur **Outils système > Utilisateurs et groupes locaux > Groupes**. La liste des groupes s'affiche.
3. Cliquez deux fois sur le groupe **Administrateurs Hyper-V**. La fenêtre **Hyper-V Administrators Properties** s'affiche.
4. Cliquez sur **Ajouter**. La fenêtre **Sélectionner des utilisateurs ou des groupes** apparaît.
5. Dans la zone **Entrer les noms d'objet à sélectionner**, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **Appliquer**, puis sur **OK**.

Ajout d'un utilisateur non-administrateur dans le groupe d'utilisateurs Performance Business Monitor

Vous devez ajouter un utilisateur non-administrateur dans le groupe d'utilisateurs Analyseur de performances pour obtenir des données sur le portail APM.

Pourquoi et quand exécuter cette tâche

Pour ajouter un utilisateur non-administrateur dans le groupe d'utilisateurs Performance Business Monitor, procédez comme suit.

Procédure

1. Cliquez sur **Démarrer > Panneau de configuration > Outils d'administration > Gestion de l'ordinateur**. La fenêtre **Gestion de l'ordinateur** s'ouvre.
2. Cliquez sur **Outils système > Utilisateurs et groupes locaux > Groupes**. La liste des groupes s'affiche.
3. Cliquez deux fois sur le groupe **Utilisateurs de l'Analyseur de performances**. La fenêtre **Performance Business Monitor Users Properties** s'ouvre.
4. Cliquez sur **Ajouter**. La fenêtre **Sélectionner des utilisateurs ou des groupes** apparaît.
5. Dans la zone **Entrer les noms d'objet à sélectionner**, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **Appliquer**, puis sur **OK**.

Configuration de la surveillance de Microsoft IIS

Lorsque vous installez Monitoring Agent for Microsoft Internet Information Services, il est configuré automatiquement et démarre avec les paramètres de configuration par défaut.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Microsoft IIS.
- Vérifiez que l'utilisateur, qui se connecte à l'environnement ou à l'application Microsoft Internet Information Server, dispose des privilèges d'administrateur. Utilisez un utilisateur existant disposant des privilèges d'administrateur ou créez-en un nouveau. Ajoutez le nouvel utilisateur au groupe Administrateurs pour qu'il bénéficie des privilèges d'administrateur.

  A faire : Pour configurer l'agent Microsoft IIS, vous pouvez utiliser un utilisateur local ou un utilisateur de domaine à condition que celui-ci dispose des privilèges d'administrateur.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'agent lorsqu'il est arrêté ou en cours d'exécution. L'agent reste au même état après la configuration. Par exemple, si l'agent est en cours d'exécution, il reste à l'état en cours d'exécution après la configuration.

Pour configurer l'agent, vous pouvez utiliser la fenêtre **IBM Performance Management** ou le fichier de réponses silencieux.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Que faire ensuite
Après avoir configuré l'agent, vous pouvez modifier le compte utilisateur d'utilisateur local à utilisateur de domaine. Pour connaître les étapes de modification du compte utilisateur, voir «Modification du compte utilisateur», à la page 527.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent Microsoft IIS sur des systèmes d'exploitation Windows à l'aide de la fenêtre **IBM Performance Management**. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Pourquoi et quand exécuter cette tâche
Vous pouvez configurer l'agent lorsqu'il est arrêté ou en cours d'exécution. L'agent reste au même état après la configuration. Par exemple, si l'agent est en cours d'exécution, il reste à l'état en cours d'exécution après la configuration.

L'agent Microsoft IIS fournit des valeurs par défaut pour certains paramètres. Vous pouvez spécifier différentes valeurs pour ces paramètres.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Monitoring Agent for Microsoft Internet Information Services**, puis sur **Configuration de l'agent**.
3. Dans la fenêtre de Monitoring Agent for Microsoft Internet Information Services, procédez comme suit :
   a) Dans l'onglet **HTTP Error Log Configuration**, spécifiez un emplacement où sauvegarder le fichier journal et cliquez sur **Suivant**.

      Remarque : Par défaut, ce fichier journal est sauvegardé à l'emplacement suivant : `C:\WINDOWS\system32\LogFiles\HTTPERR`. L'administrateur peut modifier l'emplacement du fichier journal.
   b) Dans l'onglet **Site Log Configuration**, spécifiez un emplacement où sauvegarder le fichier journal et cliquez sur **OK**.

      Remarque : Par défaut, ce fichier journal est sauvegardé à l'emplacement suivant : `C:\inetpub\logs\LogFiles`. L'administrateur peut modifier l'emplacement du fichier journal.
4. Dans la fenêtre **Restart of Monitoring Agent for Microsoft IIS**, cliquez sur **Yes**.

Que faire ensuite
Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Lorsque vous installez l'agent Microsoft IIS, il est configuré automatiquement et démarre avec les paramètres de configuration par défaut. Utilisez le fichier de réponses silencieux pour modifier les paramètres de configuration par défaut.

Avant de commencer

Créez un fichier de réponses qui contient les paramètres de configuration que vous voulez modifier. Pour modifier les paramètres de configuration par défaut, éditez le fichier de réponses.

Pourquoi et quand exécuter cette tâche
Vous pouvez configurer l'agent lorsqu'il est arrêté ou en cours d'exécution. L'agent reste au même état après la configuration. Par exemple, si l'agent est en cours d'exécution, il reste à l'état en cours d'exécution après la configuration.

Procédure

Pour configurer l'agent Microsoft IIS, procédez comme suit :

1. Sur la ligne de commande, accédez au répertoire qui contient le fichier `msiis-agent.bat`.
2. Entrez la commande **`msiis-agent.bat config`** *chemin d'accès absolu au fichier de réponses*.

   Le fichier de réponses contient les paramètres suivants :

   KQ7_SITE_LOG_FILE
   C:\inetpub\logs\LogFiles

   KQ7_HTTP_ERROR_LOG_FILE
   C:\WINDOWS\system32\LogFiles\HTTPERR

   A faire : La configuration d'agent est organisée par groupes :

   Configuration du journal du site (SITE_LOG)
   Ce groupe contient les paramètres de configuration liés au fichier journal du site (KQ7_SITE_LOG_FILE). Un administrateur peut spécifier un emplacement où sauvegarder le fichier journal. Par défaut, ce fichier journal est sauvegardé à l'emplacement suivant : `C:\inetpub\logs\LogFiles`

   Configuration du journal des erreurs HTTP (HTTP_ERROR_LOG)
   Ce groupe contient les paramètres de configuration liés au fichier du journal des erreurs HTTP (KQ7_HTTP_ERROR_LOG_FILE). Un administrateur peut spécifier un emplacement où sauvegarder le fichier journal. Par défaut, ce fichier journal est sauvegardé à l'emplacement suivant : `C:\WINDOWS\system32\LogFiles\HTTPERR`.
3. Si l'agent est arrêté, démarrez-le.

Que faire ensuite
Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Modification du compte utilisateur

Après avoir configuré l'agent Microsoft IIS, vous pouvez modifier le compte utilisateur d'utilisateur local à utilisateur de domaine.

Pourquoi et quand exécuter cette tâche
Par défaut, l'agent Microsoft IIS s'exécute sous le compte utilisateur local.

Procédure

1. Exécutez la commande suivante pour vérifier l'ID utilisateur qui est utilisé pour démarrer l'agent :

   `rép_install\InstallITM\KinCinfo.exe -r`
2. Si l'agent de surveillance a été démarré avec un ID utilisateur qui n'appartient pas au groupe Administrateur, arrêtez l'agent.
3. Ouvrez la fenêtre **Manage Monitoring Services**.
4. Cliquez avec le bouton droit de la souris sur l'instance de l'agent, puis cliquez sur **Modifier le démarrage**.

5. Indiquez l'ID utilisateur complet sous la forme <Domaine\ID_utilisateur>, puis indiquez le mot de passe.
6. Lancez la agent Microsoft IIS.

Configuration de la surveillance de Skype for Business Server (anciennement Microsoft Lync Server)

Lorsque vous installez Monitoring Agent for Skype for Business Server (anciennement MS Lync Server), l'agent est à l'état non configuré. Pour le démarrer, vous devez le configurer.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent Skype for Business Server.
- Assurez-vous que l'utilisateur que vous utilisez pour exécuter l'Agent Skype for Business Server est un utilisateur de domaine disposant des privilèges d'administrateur et des droits d'accès à tous les serveurs distants répertoriés dans la topologie de Lync ou Skype for Business Server. Utilisez un utilisateur de domaine disposant des privilèges d'administrateur, ou créez un nouvel utilisateur de domaine et affectez-lui des privilèges d'administrateur.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'agent lorsqu'il est arrêté ou en cours d'exécution. L'agent reste au même état après la configuration. Par exemple, si l'agent est en cours d'exécution, il reste à l'état en cours d'exécution après la configuration.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Pour configurer l'agent, vous pouvez utiliser la fenêtre **IBM Performance Management** ou le fichier de réponses silencieux.

Que faire ensuite

Après avoir configuré l'agent, vous pouvez modifier le compte utilisateur d'utilisateur local à utilisateur de domaine. Pour connaître les étapes de modification du compte utilisateur, voir «Modification du compte utilisateur», à la page 531.

Droits et droits d'accès d'un utilisateur non-administrateur

Vous pouvez exécuter l'agent de surveillance pour l'Agent Skype for Business Server en tant qu'utilisateur non-administrateur, mais certaines fonctions ne seront pas accessibles.

Droits du Registre

Pour créer un utilisateur non-administrateur, créez-en un et configurez les droits du Registre associés de la manière suivante.

- Accès complet à KEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring
- Accès complet au répertoire CANDLE_HOME

L'utilisateur non-administrateur doit appartenir aux groupes Utilisateurs de l'Analyseur des performances et Utilisateurs du journal des performances. Si vous définissez ces autorisations pour un utilisateur non-administrateur, les données s'affichent pour tous les groupes d'attributs basés sur Perfmon.

Pour afficher les données des groupes d'attributs collectées de la base de données, procédez comme suit :

Si vous voulez afficher les données des groupes d'attributs collectées de la base de données, vous devez configurer les droits suivants pour l'utilisateur non-administrateur.

- Le compte utilisateur non-administrateur que vous utilisez pour exécuter l'Agent Skype for Business Server doit disposer du droit Déboguer les programmes pour pouvoir ajouter un débogueur à un processus.

  Par défaut, le droit Déboguer les programmes est affecté uniquement aux comptes Administrateur et Système local. Pour accorder le droit Déboguer les programmes, vous devez exécuter les étapes suivantes sur le serveur Lync ou Skype for Business :

  1. Cliquez sur **Démarrer > Outils d'administration > Stratégie de sécurité locale**. La fenêtre **Stratégie de sécurité locale** s'affiche.
  2. Développez **Stratégies locales**, puis cliquez sur **Attribution des droits utilisateur**. La liste des droits utilisateur s'affiche.
  3. Cliquez deux fois sur la stratégie **Déboguer les programmes**. La fenêtre **Propriétés de Déboguer les programmes** apparaît.
  4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre **Sélectionner des utilisateurs ou des groupes** apparaît.
  5. Dans la zone Entrer les noms d'objet à sélectionner, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
  6. Cliquez sur **OK**.
- Accordez le droit Ouvrir une session en tant que service

  Pour accorder le droit Ouvrir une session en tant que service, vous devez exécuter les étapes suivantes sur le serveur Lync ou Skype for Business :

  1. Cliquez sur **Démarrer > Outils d'administration > Stratégie de sécurité locale**. La fenêtre **Stratégie de sécurité locale** s'affiche.
  2. Développez **Stratégies locales**, puis cliquez sur **Attribution des droits utilisateur**. La liste des droits utilisateur s'affiche.
  3. Cliquez deux fois sur la stratégie **Ouvrir une session en tant que service**. La fenêtre **Propriétés de Ouvrir une session en tant que service** apparaît.
  4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre **Sélectionner des utilisateurs ou des groupes** apparaît.
  5. Dans la zone Entrer les noms d'objet à sélectionner, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
  6. Cliquez sur **OK**.

Le groupe d'attributs Disponibilité affiche les données propres aux membres du groupe Administrateurs.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'Agent Skype for Business Server (anciennement agent MS Lync Server) sur les systèmes d'exploitation Windows à l'aide de la fenêtre **IBM Performance Management**. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'agent lorsqu'il est arrêté ou en cours d'exécution. L'agent reste au même état après la configuration. Par exemple, si l'agent est en cours d'exécution, il reste à l'état en cours d'exécution après la configuration.

L'Agent Skype for Business Server fournit des valeurs par défaut pour certains paramètres. Vous pouvez spécifier différentes valeurs pour ces paramètres.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Monitoring Agent for Skype for Business Server**, puis sur **Configuration de l'agent**.
3. Dans la fenêtre Monitoring Agent for Skype for Business Server, procédez comme suit :
   a) Dans l'onglet **SQL Configuration for Skype for Business Topology**, pour vous connecter au Central Management Store de Microsoft Lync Server ou Skype for Business Server, indiquez des valeurs pour les paramètres de configuration, puis cliquez sur **Suivant**.

      Remarque : Vous pouvez ignorer cet onglet, car SQL Configuration for Skype for Business Topology ne s'applique pas à IBM Cloud Application Performance Management.

      Important : La configuration des transactions synthétiques est facultative. Si vous avez besoin des données de transaction synthétique, spécifiez les paramètres de configuration dans les onglets **Setup Information** et **Scheduler Configuration**.
   b) Dans l'onglet **Administrator Login Credentials**, spécifiez les données d'identification de l'administrateur, puis cliquez sur **Suivant**.
   c) Dans l'onglet **Setup Information**, pour exécuter les commandes des transactions synthétiques, indiquez des valeurs pour les paramètres de configuration, puis cliquez sur **Suivant**.
   d) Dans l'onglet **Scheduler Configuration**, pour planifier les transactions synthétiques, spécifiez les valeurs des paramètres de configuration, puis cliquez sur **Suivant**.
   e) Dans l'onglet **SQL Server Configuration for Skype for Business Monitoring Role**, pour vous connecter au rôle de surveillance de Microsoft Lync Server ou Skype for Business Server, indiquez des valeurs pour les paramètres de configuration, puis cliquez sur **Suivant**.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 531.
4. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Monitoring Agent for Skype for Business Server**, puis sur **Démarrer**.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Lorsque vous installez l'Agent Skype for Business Server (anciennement agent MS Lync Server), l'agent est à l'état non configuré. Pour le démarrer, vous devez le configurer.
Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Avant de commencer

Créez un fichier de réponses qui contient les paramètres de configuration que vous voulez modifier. Pour modifier les paramètres de configuration par défaut, éditez le fichier de réponses.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'agent lorsqu'il est arrêté ou en cours d'exécution. L'agent reste au même état après la configuration. Par exemple, si l'agent est en cours d'exécution, il reste à l'état en cours d'exécution après la configuration.

Procédure

Pour configurer l'Agent Skype for Business Server, procédez comme suit :

1. Ouvrez l'invite de commande.
2. Modifiez le chemin d'accès au répertoire qui contient le fichier `skype_for_business_server-agent.bat`.
3. Entrez la commande **`skype_for_business_server-agent.bat config`** *chemin absolu du fichier de réponses*.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 531.
4. Démarrez l'agent s'il est à l'état arrêté.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Modification du compte utilisateur

Après avoir configuré l'Agent Skype for Business Server, vous pouvez modifier le compte utilisateur d'utilisateur local à utilisateur de domaine.

Pourquoi et quand exécuter cette tâche

Par défaut, l'Agent Skype for Business Server s'exécute sous le compte utilisateur local. Lorsque l'agent s'exécute sous l'utilisateur de domaine, il peut collecter les données des serveurs distants.

Procédure

1. Exécutez la commande suivante pour vérifier l'ID utilisateur qui est utilisé pour démarrer l'agent :

   `rép_install\InstallITM\KinCinfo.exe -r`
2. Si l'agent de surveillance a été démarré avec un ID utilisateur qui n'appartient pas au groupe Administrateur, arrêtez l'agent.
3. Ouvrez la fenêtre **Manage Monitoring Services**.
4. Cliquez avec le bouton droit de la souris sur l'instance de l'agent, puis cliquez sur **Modifier le démarrage**.
5. Indiquez l'ID utilisateur complet sous la forme <Domaine\ID_utilisateur>, puis indiquez le mot de passe.
6. Lancez la Agent Skype for Business Server.

Paramètres de configuration de l'agent

Lorsque vous configurez l'Agent Skype for Business Server (anciennement agent MS Lync Server), vous pouvez modifier les valeurs par défaut des paramètres de configuration, comme le nom du serveur de base de données, le nom de l'instance de base de données, le nom de la base de données et d'autres paramètres.

Le tableau ci-après contient les descriptions des paramètres de configuration de l'Agent Skype for Business Server.

Remarque : La zone Pool FQDN est obligatoire dans le tableau suivant.

Tableau 177. Noms et descriptions des paramètres de configuration de l'agent

Nom du paramètre	Description
Nom de serveur de base de données (par exemple, PS6877)	• Onglet **SQL Configuration for Skype for Business Topology** : nom du serveur de base de données sur lequel le Central Management Store de Lync ou Skype for Business Server est installé. • Onglet **SQL Server Configuration for Skype for Business Monitoring Role** : nom du serveur de base de données sur lequel le rôle de surveillance est installé.
Nom de l'instance de base de données	• Onglet **SQL Configuration for Skype for Business Topology** : nom de l'instance. • Onglet **SQL Server Configuration for Skype for Business Monitoring Role** : nom de l'instance de base de données sur laquelle le rôle de surveillance est installé.
Nom de la base de données	Nom de la base de données.
ID utilisateur de base de données	ID utilisateur de la base de données. Cet utilisateur doit disposer de droits d'accès à l'instance Microsoft SQL Server requise. Cet utilisateur n'a pas besoin d'être un utilisateur Active Directory.
Mot de passe Base de données	Mot de passe de la base de données dans laquelle le rôle de surveillance est installé.
Nom d'utilisateur (par ex. : skype \administrator)	ID utilisateur de l'administrateur. Ce doit être un utilisateur de domaine disposant de privilèges d'administrateur et de droits d'accès à tous les serveurs distants répertoriés dans la topologie Lync ou Skype for Business Server. Les données d'identification de cet utilisateur sont également utilisées dans la fonction Transaction synthétique. Cet utilisateur devrait donc être autorisé à créer une planification Windows dans le Planificateur de tâches et à exécuter des commandes de transaction synthétique.
Mot de passe	Mot de passe de connexion de l'administrateur.
Confirmer le mot de passe de domaine	Entrez le mot de passe indiqué dans la zone Mot de passe de domaine.
Nom de domaine complet du pool	Nom de domaine complet du pool Skype pour lequel les commandes synthétiques sont exécutées.
Zone géographique	Zone géographique du système de production.
Utilisateur1 de test (par exemple, user1@skype.com)	Premier nom d'utilisateur pouvant être utilisé lors de l'exécution des cmdlets de transaction synthétique. Le format du nom d'utilisateur est SAMAccountName@domain.com. Ne saisissez pas d'adresse SIP.
Mot de passe Utilisateur1 de test	Mot de passe de l'Utilisateur1 de test.
Confirmer le mot de passe Utilisateur1 de test	Entrez le même mot de passe que celui indiqué dans la zone **`Mot de passe Utilisateur1 de test`**.
Utilisateur2 de test (par exemple, user2@skype.com)	Deuxième nom d'utilisateur pouvant être utilisé lors de l'exécution des cmdlets de transaction synthétique. Le format du nom d'utilisateur est SAMAccountName@domain.com. Ne saisissez pas d'adresse SIP.

Tableau 177. Noms et descriptions des paramètres de configuration de l'agent (suite)	
Nom du paramètre	**Description**
Mot de passe Utilisateur2 de test	Mot de passe de l'Utilisateur2 de test.
Confirmer le mot de passe Utilisateur2 de test	Entrez le même mot de passe que celui indiqué dans la zone **Mot de passe Utilisateur2 de test**.
Utiliser les valeurs de configuration de l'agent	Laissez cette option activée si vous souhaitez exécuter des commandes synthétiques en utilisant l'ensemble des zones fournies dans le panneau de configuration. Désactivez-la pour utiliser les valeurs définies par New-CsHealthMonitoringConfiguration. Si l'option est désactivée, la valeur de **Pool FQDN** est utilisée pour identifier Get-CsHealthMonitoringConfiguration. Veillez à fournir des données d'identification valides pour l'utilisateur de test pour exécuter la commande **Test-CsMcxP2PIM**.
Fréquence	Fréquence d'exécution de l'utilitaire planifié qui extrait les données des transactions synthétiques. La fréquence peut avoir les valeurs suivantes : • Quotidien (DAY_FREQUENCY) • Hebdomadaire (WEEK_FREQUENCY) • Mensuel (MONTHLY_FREQUENCY)
Heure de collecte	Partie de l'horodatage représentant les heures, dans une horloge au format 24 heures que vous sélectionnez pour planifier l'exécution de l'utilitaire.
Minute de collecte	Partie de l'horodatage représentant les minutes, dans une horloge au format 24 heures que vous sélectionnez pour planifier l'exécution de l'utilitaire.
Date de début (AAAA-MM-JJ)	Date d'activation du planificateur.
Date de fin (AAAA-MM-JJ)	Date de désactivation du planificateur.

Configuration de la surveillance de Microsoft .NET

Monitoring Agent for Microsoft .NET surveille les applications .NET. Il démarre automatiquement après l'installation pour collecter les données de surveillance des ressources. Cependant, pour la collecte des données de diagnostic et de suivi des transactions, vous devez effectuer certaines tâches de configuration.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Microsoft .NET.

Pourquoi et quand exécuter cette tâche

Une fois que l'agent est installé, effectuez les tâches de configuration suivantes pour que l'agent puisse collecter les données de diagnostic et de suivi des transactions :

1. Enregistrement du collecteur de données
   Le collecteur de données est un composant de l'agent Microsoft .NET. Il collecte les données de suivi des transactions et de diagnostic et les envoie à l'agent Microsoft .NET. Vous devez enregistrer le

collecteur de données pour la collecte de ces données. Pour plus de détails, voir «Enregistrement du collecteur de données», à la page 535.

2. Configuration de la collecte des données de suivi des transactions et de diagnostic
   Après avoir enregistré le collecteur de données, activez la collecte des données de diagnostic et de suivi des transactions sur la console Cloud APM. Vous pouvez également activer la collecte des données de diagnostic à l'aide de la commande **configdc**. Pour plus d'informations, voir «Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 538 et «Activation de la collecte des données de diagnostic à l'aide de la commande configdc», à la page 539.
3. Activation des mises à jour de configuration
   Si vous activez la collecte de données de diagnostic à l'aide de la commande **configdc**, vous devez activer la configuration de telle sorte que les mises à jour soient sauvegardées dans le fichier de configuration. Pour plus d'informations sur l'activation des changements de configuration, voir «Activation des mises à jour de configuration», à la page 540.
4. Optimisation des performances du collecteur de données
   Vous pourriez avoir besoin d'effectuer certaines tâches pour réajuster les performances du collecteur de données. Pour plus de détails, voir «Optimisation des performances du collecteur de données», à la page 541.

Coexistence des agents
Dans un environnement de coexistence d'agent, vous pouvez afficher les données de suivi des transactions à partir de la console Cloud APM ou de Tivoli® Enterprise Portal. Pour plus d'informations sur l'activation de la collecte de données pour le suivi des transactions dans l'environnement de coexistence d'agent, voir «Activation du suivi des transactions dans l'environnement de coexistence d'agent», à la page 540.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau ci-après.

Tableau 178. Versions d'agent et documentation

Version de l'agent Microsoft .NET	Documentation
8.1.3.2	IBM Cloud Application Performance Management
8.1.3 et 8.1.2	IBM Performance Management 8.1.3

Le lien permet d'ouvrir une rubrique Knowledge Center sur site.

Droits nécessaires pour exécuter un agent à l'aide d'un compte local ou de domaine

Seul un utilisateur local ou du domaine qui est membre du groupe Administrateurs est autorisé à exécuter l'agent Microsoft .NET. Cette rubrique fournit les conditions à remplir si l'utilisateur local ou du domaine n'est pas membre du groupe Administrateurs.

L'utilisateur doit disposer des droits suivants sur l'unité système et l'unité d'installation de l'agent :

1. Lecture
2. Ecriture
3. Exécution
4. Modification

L'utilisateur doit disposer du droit suivant sur la clé de registre HKEY_LOCAL_MACHINE

- Lecture

L'utilisateur doit être membre des groupes suivants sur le serveur surveillé :

1. Utilisateurs
2. IIS_IUSRS
3. Utilisateurs de l'Analyseur de performances
4. Utilisateurs du journal de performances

Remarque : Il est toutefois conseillé d'exécuter l'agent Microsoft .NET avec un utilisateur local ou de domaine qui soit membre du groupe Administrateurs local.

Enregistrement du collecteur de données

Vous devez enregistrer le collecteur de données pour qu'il collecte les données de suivi des transactions et les données de diagnostic. Pour collecter les données de surveillance des ressources, aucune configuration spécifique n'est requise.

Pourquoi et quand exécuter cette tâche

Enregistrez les composants suivants du collecteur de données, en fonction du type de données (transaction et/ou diagnostics) que le collecteur de données doit collecter :

Tableau 179. Composants du collecteur de données et leurs fonctions

Nom du composant	Surveille
httpmodule	Les transactions ASP.NET et collecte le temps de réponse aux demandes et le temps UC
profiler	Les transactions ADO.NET et collecte les données de méthode, de trace de pile et de contexte de demande à des fins de diagnostic
isapi	Les transactions ASP.NET et collecte le temps de réponse aux demandes et le temps UC
soap	Les transactions de service ASMX ou WCF et le temps de réponse des services WCF

A faire :

- Utilisez `isapi32` pour filtrer les applications 32 bits sur un serveur Microsoft IIS Server 64 bits.
- Enregistrez tous les composants pour suivre toutes les transactions et affichez la topologie complète des transactions.

Procédure

1. Sur le serveur où l'agent est installé, exécutez la commande suivante en tant qu'administrateur :

   ```
   cd rép_install\qe\bin
   configdc.exe registerdc [all|isapi|isapi32|profiler|httpmodule|soap]
   ```

   A faire :

   - Lorsque vous exécutez la commande **`configdc.exe registerdc`** sans spécifier de composant à enregistrer, seul httpmodule est enregistré.
   - Pour enregistrer tous les composants, exécutez la commande **`configdc.exe registerdc all`**.
   - Pour enregistrer n'importe quels composants ensemble, exécutez cette commande : **`configdc.exe registerdc`** *nom_composant nom_composant*. Par exemple, **`configdc.exe registerdc`** httpmodule profiler
2. Redémarrez les applications .NET.

Que faire ensuite
Après avoir enregistré le collecteur de données, vous devez activer la collecte de données pour le suivi des transactions et les diagnostics. Pour plus d'informations sur l'activation de la collecte de données, voir «Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 538.

Si vous souhaitez arrêter la surveillance des applications .NET, annulez l'enregistrement du collecteur de données. Répétez les étapes indiquées en utilisant la commande **`configdc.exe unregisterdc`** pour annuler l'enregistrement de tous les composants du collecteur de données.

Utilisation du module de temps de réponse IIS de l'agent .NET

A partir de l'édition 8.1.4.0.2, l'agent .NET inclut le "module de temps de réponse IIS", qui fonctionne avec l'agent de temps de réponse pour afficher les données de transaction des utilisateurs finaux pour le serveur IIS.

Activation du module de temps de réponse

Vous devez activer le module de temps de réponse avant de l'utiliser.

Procédure

Pour activer le module de temps de réponse, procédez comme suit :

1. Ouvrez l'invite de commande en mode administrateur.
2. Pour arrêter IIS, exécutez la commande suivante :

   ```
   iisreset /stop
   ```
3. Accédez au répertoire `rép_install\qe\bin` à partir de l'invite de commande.
4. Pour enregistrer le module de temps de réponse pour IIS, exécutez la commande suivante :

   ```
   configdc registerdc rtmodule
   ```
5. Pour démarrer IIS, exécutez la commande suivante :

   ```
   iisreset /start
   ```

Résultats

Le module de temps de réponse est activé.

Configuration de l'agent de temps de réponse pour une utilisation avec le module de temps de réponse IIS de l'agent .NET

Vous devez configurer l'agent de temps de réponse pour l'utiliser avec le module de temps de réponse IIS de l'agent .NET.

Avant de commencer

Installez l'agent de temps de réponse (version 8.1.4). Pour plus d'informations, voir Chapitre 6, «Installation des agents», à la page 123.

Procédure

Pour configurer l'agent de temps de réponse pour l'utiliser avec le module de temps de réponse IIS de l'agent .NET, procédez comme suit :

1. Ouvrez un éditeur de texte en mode administrateur.
2. Ouvrez le fichier suivant dans un éditeur de texte :

   rép_config`\TMAITM6_x64\`*nom_hôte*`_T5.config`

   où *rép_config* est le répertoire de base d'APM et *nom_hôte* est le nom du serveur.
3. Mettez à jour la propriété suivante :

   ```
   { KT5DISABLEANALYZER=YES } { KT5ENABLEWEBPLUGIN=YES }
   ```
4. Ajoutez la propriété suivante dans la section `SECTION=analyzerconfig [ ]` :

{KT5WEBPLUGINIPCNAME=KFC1}

5. Redémarrez l'agent de temps de réponse.
6. Connectez-vous à la console Performance Management pour vérifier les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Performance Management, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de l'injection JavaScript pour le module de temps de réponse IIS
Vous devez configurer l'injection JavaScript (JS) pour qu'elle fonctionne avec le module de temps de réponse IIS (Internet Information Services) de l'agent .NET.

Procédure

Pour configurer l'injection JS de sorte qu'elle fonctionne avec le module de temps de réponse IIS de l'agent .NET, procédez comme suit :

1. Ouvrez un éditeur de texte en mode administrateur.
2. Ouvrez le fichier suivant dans un éditeur de texte :

   <APM_HOME>\qe\config\dotNetDcConfig.properties.inactive
3. Pour activer l'injection JS pour le module de temps de réponse, définissez la propriété **RTModule.JSInjection.Enabled** sur **true**.
4. Pour désactiver l'injection JS pour le module de temps de réponse, définissez la propriété **RTModule.JSInjection.Enabled** sur **false**.
5. Ouvrez l'invite de commande en mode administrateur, puis accédez au répertoire <APM_HOME>\qe\bin.
6. Exécutez les commandes suivantes :
   - configdc activateconfig
   - iisreset

Désactivation du module de temps de réponse IIS
Vous pouvez désactiver le module de temps de réponse IIS lorsque vous ne souhaitez plus afficher les données de transaction des utilisateurs finaux pour le serveur IIS.

Procédure

Pour désactiver le module de temps de réponse IIS, procédez comme suit :

1. Ouvrez l'invite de commande en mode administrateur.
2. Pour arrêter IIS, exécutez la commande suivante :

   iisreset /stop
3. Accédez au répertoire *rép_install*\qe\bin à partir de l'invite de commande.
4. Pour annuler l'enregistrement du module de temps de réponse pour ISS, procédez comme suit :
   - Exécutez la commande suivante :

     configdc unregisterdc rtmodule
   - Pour annuler l'enregistrement de tous les composants du collecteur de données, y compris le module de temps de réponse, exécutez la commande suivante :

     configdc unregisterdc all
5. Pour démarrer IIS, exécutez la commande suivante :

   iisreset /start

Résultats
Le module de temps de réponse IIS est désactivé.

Limitations du module de temps de réponse IIS
Les limitations du module de temps de réponse IIS sont répertoriées ici.

- Les informations utilisateur ne sont pas suivies par le module de temps de réponse IIS et le nom d'utilisateur affiché est actuellement "Unknown".

Activation de la collecte des données de suivi des transactions et de diagnostic

Sur la page **Configuration d'agent**, vous pouvez activer ou désactiver la collecte des données de suivi des transactions et de diagnostic.

Avant de commencer
Vérifiez que vous avez enregistré le collecteur de données. Pour plus de détails, voir «Enregistrement du collecteur de données», à la page 535.

Procédure

Procédez comme suit pour configurer la collecte des données pour chaque système géré.

1. Connectez vous à console Cloud APM.
2. A partir de la barre de navigation, cliquez sur **Configuration système** > **Configuration d'agent**.
   La page **Configuration d'agent** s'affiche.
3. Cliquez sur l'onglet **MS .NET**.
4. Cochez les cases des systèmes gérés pour lesquels vous voulez configurer la collecte de données et effectuez l'une des actions suivantes de la liste **Actions**.
   - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Enabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour sur Enabled pour chaque système géré sélectionné.
   - Pour activer la collecte des données de diagnostic, sélectionnez **Set Diagnostic Mode** (Définir le mode diagnostic) et cliquez sur le niveau de votre choix. Le statut indiqué dans la colonne **Diagnostic Mode** est mis à jour de manière à afficher le niveau spécifié pour chaque système géré sélectionné.
     - Niveau 1 : Le module HTTP collecte les données d'instance de demande et de récapitulatif des demandes.
     - Niveau 2 : Le module HTTP collecte les données d'instance de demande et de récapitulatif des demandes. Le profileur collecte les données de méthode et de trace de pile.
   - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Disabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour et défini sur Disabled pour chaque système géré sélectionné.
   - Pour désactiver la collecte des données de diagnostic, cliquez sur **Set Diagnostic Mode** > **Disabled**. Le statut indiqué dans la colonne **Diagnostic Mode** est mis à jour et défini sur Disabled pour chaque système géré sélectionné.

Résultats
La collecte de données est configurée pour chaque système géré.

Que faire ensuite
Connectez-vous à la console Cloud APM pour afficher les données de suivi des transactions et de diagnostic collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Activation de la collecte des données de diagnostic à l'aide de la commande configdc

Vous pouvez également activer ou désactiver la collecte des données de diagnostic à l'aide de la commande **configdc**. Ce processus est facultatif.

Avant de commencer

- Vérifiez que vous avez enregistré le collecteur de données. Pour plus de détails, voir «Enregistrement du collecteur de données», à la page 535.
- Assurez-vous d'avoir effectué la procédure «Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 538.
- Vérifiez que le fichier qe_custom.properties est traité par le serveur APM dans <APM_Home>\localconfig\qe et qu'il contient les propriétés suivantes :
  - transaction_tracking=ENABLED
  - diagnostic_mode=LEVEL2

Procédure

1. Exécutez la commande suivante :

   ```
   cd rép_install\qe\bin configdc deepdivedc -tracelevel niveau_trace
   ```

   Où,

   rép_install
   Répertoire d'installation de l'agent Microsoft .NET.

   niveau_trace
   Niveau de trace qui indique la quantité de données de diagnostic collectées par l'.NET Data Collector. Spécifiez l'une des valeurs suivantes :

   0
   La collecte des données de diagnostic est désactivée.

   1
   La collecte des données de diagnostic est activée. Le module HTTP collecte les données d'instance de demande et de récapitulatif des demandes.

   2
   La collecte des données de diagnostic est activée. Le module HTTP collecte les données d'instance de demande et de récapitulatif des demandes. Le profileur collecte les données de méthode et de trace de pile.

   Conseil : La définition du niveau de trace en utilisant la commande **configdc.exe deepdivedc -tracelevel** définit la valeur du paramètre bci_dc.diagnose.level dans le fichier dotNetDcConfig.properties.
2. Activez les changements de configuration.

   Pour plus d'informations sur l'activation des modifications, voir «Activation des mises à jour de configuration», à la page 540.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données de diagnostic collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Activation du suivi des transactions dans l'environnement de coexistence d'agent

Dans un environnement de coexistence d'agent, vous pouvez configurer le collecteur de données pour collecter et transmettre les données de suivi des transactions à Tivoli Enterprise Portal, qui est un composant d'IBM Tivoli Monitoring.

Avant de commencer

Vous devez installer l'agent Microsoft .NET, qui est fourni dans Cloud APM et vous devez supprimer ou désenregistrer le composant .NET Data Collector, qui est fourni avec ITCAM for Microsoft Applications. Utilisez la commande **`configdc.exe unregisterdc`** pour désenregistrer tous les modules du collecteur de données.

Procédure

Pour configurer le collecteur de données dans le but de collecter et de transmettre les données de suivi des transactions à Tivoli Enterprise Portal, procédez comme suit :

1. Accédez au répertoire *rép_install*`\localconfig\qe`, où *rép_install* est le répertoire d'installation de l'agent Microsoft .NET. Le chemin par défaut est `C:\IBM\APM`.
2. Ouvrez le fichier `qe_default.properties` et définissez la valeur du paramètre **`transaction_tracking`** sur `ENABLED`.
3. Sauvegardez et fermez le fichier `qe_default.properties`.
4. Accédez au répertoire *rép_install*`\qe\config`.
5. Ouvrez le fichier `dotNetDcConfig.properties.inactive` dans un éditeur de texte.
6. Définissez les paramètres **`TTDC.enabled`** et **`TTAS.enabled`** comme suit :

```
TTDC.enabled=true
TTAS.enabled=true
```

7. Pour configurer la connexion au collecteur de transactions, affectez l'adresse IP et le numéro de port du collecteur de transactions aux paramètres **`TTAS.Host`** et **`TTAS.Port`**.
8. Exécutez la commande suivante pour activer les changements :

```
rép_install\qe\bin\configdc.exe activateconfig
```

9. Redémarrez l'application .NET pour appliquer les changements.

Résultats

Les données de suivi des transactions peuvent être collectées et affichées dans Tivoli Enterprise Portal.

Que faire ensuite

Pour désactiver l'opération de suivi pour un .NET Data Collector, répétez la procédure et utilisez les valeurs de configuration suivantes :

- Dans le fichier `qe_default.properties`, définissez `transaction_tracking=DISABLED`.
- Dans le fichier `dotNetDcConfig.properties.inactive`, définissez `TTDC.enabled=false` et `TTAS.enabled=false`.

Activation des mises à jour de configuration

Vous devez activer les mises à jour que vous effectuez dans les paramètres de configuration à l'aide de la commande `configdc`. Cette activation permet de sauvegarder vos mises à jour dans le fichier `dotNetConfig.properties`.

Pourquoi et quand exécuter cette tâche

Lorsque vous mettez à jour les paramètres de configuration à l'aide de la commande **`configdc`**, les valeurs des paramètres sont mises à jour dans le fichier `dotNetConfig.properties`. Toutefois, si ce fichier est déjà utilisé et qu'il ne peut pas être modifié, vos mises à jour des paramètres de configuration sont sauvegardées dans le fichier `dotNetDcConfig.properties.inactive`. Vous devez activer la

configuration de sorte que les mises à jour soient sauvegardées dans le fichier `dotNetConfig.properties`.

Procédure

1. Accédez au chemin suivant :
   rép_install\qe\bin
   Où *rép_install* correspond au répertoire d'installation de l'agent Microsoft .NET.
2. Exécutez la commande suivante :
   `configdc activateConfig`

Que faire ensuite

Si les transactions IIS (Internet Information Service) sont surveillées et que la configuration du collecteur de données est mise à jour, redémarrez IIS pour activer la configuration.

Si les services Web ASMX ou WCF sont surveillés et que la configuration du collecteur de données est mise à jour, redémarrez le processus hébergeant le service Web.

Optimisation des performances du collecteur de données

Lorsque vous configurez le collecteur de données pour qu'il collecte les données de suivi des transactions et de diagnostic, les performances du collecteur de données en sont affectées. Pour améliorer les performances, vous pouvez effectuer certaines tâches d'optimisation des performances.

Vous pourriez avoir besoin d'effectuer les tâches suivantes pour améliorer les performances du collecteur de données :

- Filtrer les interfaces ADO.NET que vous voulez surveiller.
- Echantillonner les données de suivi des transactions et de diagnostic.
- Configurer la consignation de trace.

Spécification d'interfaces ADO.NET pour la surveillance

Vous pouvez indiquer les interfaces client ADO.NET à activer pour le suivi des transaction.

Avant de commencer

Pour afficher les interfaces ADO.NET prises en charge par .NET Data Collector, voir Functions of namespaces supported by the data collector.

Pour afficher les valeurs de configuration de l'.NET Data Collector, consultez le fichier `dotNetDcConfig.properties` dans le répertoire *rép_install*\qe\config, où *rép_install* correspond au répertoire d'installation de l'agent Microsoft .NET.

Pourquoi et quand exécuter cette tâche

Par défaut, toutes les interfaces ADO.NET prises en charge sont activées pour le suivi des transactions lors de l'installation de l'agent. Pour spécifier les interfaces que doit surveiller le collecteur de données, activez ou désactivez la surveillance pour des interfaces spécifiques.

Si vous désactivez la surveillance d'une interface, les paramètres des filtres de domaine d'application associés sont conservés dans le fichier de configuration du collecteur de données. Le filtre est conservé lorsque l'interface est réactivée.

Procédure

- Pour activer la surveillance d'une interface ADO.NET, procédez comme suit :
  a) Depuis le répertoire *rép_install*\qe\bin, exécutez la commande suivante :

```
configdc enableMonitor all | adsi | db2 | ldap | odbc | oledb | oracle | sql
| http | web
[-appdomain liste filtres domaineapp]
```

b) Activez les changements de configuration.

Pour plus d'informations sur l'activation des modifications, voir «Activation des mises à jour de configuration», à la page 540.

- Pour désactiver la surveillance d'une interface ADO.NET, procédez comme suit :

a) Depuis le répertoire *rép_install*\qe\bin, exécutez la commande suivante :

```
configdc disableMonitor all | adsi | db2 | ldap | odbc | oledb | oracle | sql
| http | web
```

b) Activez les changements de configuration.

Pour plus d'informations sur l'activation des modifications, voir «Activation des mises à jour de configuration», à la page 540.

Echantillonnage de données de diagnostic et de suivi des transactions

Si les performances du système sont affectées en raison de la collecte des données de suivi des transactions ou de diagnostic, vous pouvez activer l'échantillonnage des données collectées afin d'améliorer les performances.

Pourquoi et quand exécuter cette tâche

Lorsque la performance du système pâtit du suivi des transactions et de la collecte des données de diagnostic, vous pouvez configurer le collecteur de données pour collecter périodiquement des données par échantillonnage. Lorsque l'échantillonnage est activé, le collecteur de données ne collecte pas les données pour chaque demande, mais à intervalles de plusieurs demandes. Vous pouvez modifier la fréquence d'échantillonnage de manière dynamique en fonction de l'utilisation de l'unité centrale par le processus DotNetProfilerService.

ATTENTION : L'échantillonnage permet d'épargner des ressources système, mais les données d'échantillon risquent de ne pas suffire pour diagnostiquer des problèmes. Une fois l'échantillonnage de données activé, la topologie de suivi des transactions peut être détériorée ou perdue. Par conséquent, n'activez l'échantillonnage de données que si les performances sont sérieusement affectées.

Procédure

Pour activer l'échantillonnage sur la collecte des données de diagnostic et de suivi des transactions, procédez comme suit :

1. Accédez au répertoire suivant :
   rép_install\qe\config
   Où *rép_install* correspond au répertoire d'installation de l'agent Microsoft .NET.
2. Dans un éditeur de texte, ouvrez le fichier `dotNetDcConfig.properties.inactive`.
3. Définissez les paramètres suivants dans le fichier :

bci_dc.sampling.Enabled
Indique si le collecteur de données collecte régulièrement des données de diagnostic et de suivi des transactions. Les valeurs admises sont `true` et `false`.

bci_dc.sampling.base
Indique la base de l'échantillonnage de données. Les valeurs admises sont les nombres positifs. Par exemple, si vous définissez la valeur du paramètre **`bci_dc.sampling.base`** sur 10, le collecteur de données recueille les données de diagnostic et de suivi des transactions toutes les 10 demandes. La fréquence d'échantillonnage est de 1 sur 10 demandes. Le collecteur de données collecte des données pour les 1re, 11e, 21e, 31e demandes et suivantes.

bci_dc.dynamic.sampling
Indique si la fréquence d'échantillonnage est constante ou dynamique. Les valeurs admises sont on et `off`. Lorsque vous définissez la valeur du paramètre **`bci_dc.dynamic.sampling`** sur on, le taux d'échantillonnage est ajusté de manière dynamique en fonction de la valeur du paramètre **`bci_dc.dynamic.max_cpu_usage`**.

bci_dc.dynamic.max_cpu_usage
Indique le seuil d'utilisation de l'unité centrale pour le processus DotNetProfilerService. Si l'utilisation de l'unité centrale par le processus DotNetProfilerService est supérieure à 110 % de la valeur indiquée, la fréquence d'échantillonnage est réduite. Si l'utilisation de l'unité centrale est inférieure à 90 % de la valeur indiquée, la fréquence d'échantillonnage est augmentée. Les valeurs admises sont comprises entre 1 et 100.

4. Sauvegardez et fermez le fichier `dotNetDcConfig.properties.inactive`.
5. Exécutez la commande suivante pour activer les modifications :

```
rép_install\qe\bin\configdc.exe activateconfig
```

6. Redémarrez l'application .NET pour appliquer la modification.

Activation de la consignation de trace pour le collecteur de données
Vous pouvez activer la génération de journaux de trace pour le collecteur de données. Vous pouvez utilisez ces journaux de trace pour traiter les incidents qui pourraient se produire avec la collecte des données de suivi des transactions et de diagnostic.

Pourquoi et quand exécuter cette tâche

Pour collecter les journaux des transactions ASP.NET, ADO.NET et des données de diagnostic, activez les journaux de trace pour httpmodule, le profileur et les composants isapi du collecteur de données. Pour collecter les journaux des transactions ASMX et WCF, activez les journaux de trace du composant soap du collecteur de données.

Important : Les performances du collecteur de données peuvent être affectées lorsque la consignation de trace est activée. Par conséquent, désactivez la consignation de trace une fois le journaux de trace collectés.

Procédure

1. Sur le serveur où l'agent est installé, accédez au répertoire suivant :
   rép_install\qe\bin
   où *rép_install* est le répertoire d'installation de l'agent Microsoft .NET.
2. Effectuez les deux procédures suivantes ou l'une d'entre elles en fonction des journaux de trace que vous voulez activer :
   - Pour activer les journaux de trace pour httpmodule, le profileur, les composants SOAP et le module de temps de réponse, procédez comme suit :
     a. Exécutez la commande suivante :
        configdc logging -tracing on
     b. Redémarrez les applications IIS et .NET.
   - Pour activer les journaux de trace pour le moteur BCI, procédez comme suit :
     a. Accédez au chemin suivant :
        <APM_HOME>\qe\config
     b. Dans un éditeur de texte, ouvrez le fichier `dotNetDcConfig.properties.inactive`.
     c. Pour le propriété **bci_dc.trace.logging**, spécifiez la valeur on.
     d. Exécutez la commande suivante :
        configdc activateconfig
     e. Redémarrez IIS.

Que faire ensuite
Pour désactiver les journaux de trace, procédez comme suit :

- Pour désactiver les journaux de trace pour httpmodule, le profileur, les composants SOAP et le module de temps de réponse, procédez comme suit :

  - Exécutez la commande suivante :
    `configdc logging -tracing off`
  - Redémarrez les applications IIS et .NET.
- Pour désactiver les journaux de trace pour le moteur BCI :
  - Accédez au chemin suivant :
    `<APM_HOME>\qe\config`
  - Dans un éditeur de texte, ouvrez le fichier `dotNetDcConfig.properties.inactive`.
  - Pour la propriété **`bci_dc.trace.logging`**, spécifiez la valeur `off`.
  - Exécutez la commande suivante :
    `configdc activateconfig`
  - Redémarrez les applications IIS et .NET.

Configuration de la surveillance de Microsoft Office 365

Vous devez configurer agent Microsoft Office 365 pour surveiller la disponibilité et les performances des abonnements Microsoft Office 365 de l'organisation.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel.
- Pour collecter des données pour les utilisateurs Office 365, il faut que les modules suivants soient installés sur le client Windows où l'agent est installé :
  - PowerShell 3.0 ou version ultérieure
  - Microsoft Online Services Sign-In Assistant PowerShell
  - SharePoint Online Management Shell
  - DotNetFrameworkVersion 4.5.2 ou version ultérieure

  Un utilisateur qui configure l'agent doit disposer des privilèges d'administration avec des privilèges pour activer la règle d'exécution à distance de PowerShell.
- Pour surveiller les transactions synthétiques Skype, effectuez les tâches suivantes :
  - Installez le client Skype 2013 sur le client Windows sur lequel l'utilisateur veut exécuter des transactions synthétiques pour Skype.
  - Définissez le périphérique vidéo par défaut pour Lync et Skype comme filtre audio/vidéo virtuel.
- Vérifiez que l'utilisateur qui démarre Microsoft Office 365 dispose des privilèges d'administrateur. Utilisez un utilisateur existant disposant des privilèges d'administrateur ou créez-en un nouveau. Ajoutez le nouvel utilisateur au groupe Administrateurs pour qu'il bénéficie des privilèges d'administrateur.

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Microsoft Office 365.

Pourquoi et quand exécuter cette tâche

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir agent Microsoft Office 365. Pour accéder à la documentation de la version 1.0.0, reportez-vous à l'IBM Knowledge Center d'IBM Cloud Application Performance Management.

Vous pouvez démarrer l'agent Microsoft Office 365 une fois installé. Une configuration manuelle est toutefois requise pour afficher les données pour tous les attributs d'agent.

Pour configurer l'agent, vous pouvez utiliser la fenêtre IBM Cloud Application Performance Management ou le fichier de réponses silencieux.

Vérification de l'accessibilité des utilisateurs configurés

Pour vérifier l'accessibilité, l'agent Microsoft Office 365 envoie un message électronique aux utilisateurs configurés et mesure le temps nécessaire pour recevoir une réponse automatique. Avant de démarrer l'agent, vous devez configurer tous les utilisateurs, qui sont configurés dans les paramètres d'accessibilité de la boîte aux lettres de l'agent Office 365,pour répondre automatiquement aux messages électroniques.

Avant de commencer

Avant de configurer les utilisateurs Exchange Online pour l'accessibilité, vérifiez que les tâches suivantes ont été effectuées :

- Une boîte aux lettres est créée pour chaque utilisateur sur l'instance Exchange Online que vous souhaitez surveiller.
- L'utilisateur que vous avez créé pour l'agent est un utilisateur Office 365 global.

Procédure

Effectuez les étapes suivantes pour chaque compte utilisateur Exchange Online pour lequel vous souhaitez vérifier l'accessibilité :

1. Connectez-vous à Microsoft Outlook en indiquant les données d'identification de l'utilisateur que vous avez créé.
2. Cliquez sur **Outils > Règles et alertes > Nouvelle règle**.
3. Dans l'**assistant de règles**, sous **Commencer à partir d'une règle vide**, cliquez sur **Apply rule on messages I receive**, puis sur **Suivant**.
4. Sélectionnez les options suivantes :
   - **From people or public group**
   - **Qui contiennent des mots spécifiques dans l'objet**
5. Sous **Etape 2** dans cette fenêtre, cliquez sur **people or public group**.
6. Dans la fenêtre **Rule address**, sélectionnez l'utilisateur (administrateur global) à partir duquel les messages doivent être reçus et cliquez sur **Next**.
7. Sous **Etape 2** dans cette fenêtre, cliquez sur **Mots spécifiques**.
8. Dans la zone **Spécifier un mot/une expression à rechercher dans l'objet/le corps du texte**, entrez `Tester l'accessibilté`.
9. Cliquez sur **Ajouter**.
10. Cliquez sur **OK**, puis sur **Suivant**.
11. Sélectionnez **Faire répondre le serveur avec un message spécifique** et cliquez sur **un message spécifique**.
12. Dans l'éditeur de message électronique, entrez le texte suivant dans la zone d'objet du message : `Tester l'accessibilité`.
13. Dans la liste **To**, ajoutez l'administrateur global.
14. Fermez l'éditeur de message électronique et cliquez sur **Oui** pour sauvegarder ces modifications.
15. Cliquez sur **Terminer**.
16. Cliquez sur **Appliquer**, puis sur **OK**.

Que faire ensuite

Configurez l'agent Microsoft Office 365.

Pour obtenir de l'aide sur le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent Microsoft Office 365 sur les systèmes d'exploitation Windows dans la fenêtre IBM Cloud Application Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'agent lorsqu'il est arrêté ou en cours d'exécution. L'agent reste au même état après la configuration. Par exemple, si l'agent est en cours d'exécution, il reste à l'état en cours d'exécution après la configuration.

L'agent Microsoft Office 365 fournit les valeurs par défaut de certains paramètres. Vous pouvez spécifier différentes valeurs pour ces paramètres.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez à l'aide du bouton droit de la souris sur **Monitoring Agent for Microsoft Office 365**, puis cliquez sur **Configuration de l'agent**.
3. Dans la fenêtre **Monitoring Agent for Microsoft Office 365**, procédez comme suit :
   a) Dans l'onglet **Détails de l'abonnement Office365**, entrez le nom d'utilisateur et le mot de passe de l'administrateur global Office 365, puis cliquez sur **Suivant**.
   b) Dans l'onglet **Transaction synthétique**, entrez la liste des adresses e-mail délimitées par des points-virgules dans la zone **Reachability Email Addresses**.
   c) Pour activer la collecte des mesures de qualité de service Skype, cochez la case **Skype QoS** et cliquez sur **Suivant**.
   d) A partir de l'onglet **Mailbox and OneDrive Usage Monitoring**, sélectionnez la durée (en heures) pour l'intervalle de collecte dans la liste **Collection Interval**, puis cliquez sur **Suivant**.
4. Dans la fenêtre **Monitoring Agent for Microsoft Office 365**, cliquez sur **Yes**.

Que faire ensuite

- Configurez les fonctionnalités de transaction synthétique Skype pour surveiller les transactions synthétiques de qualité de service Skype. Pour plus d'informations sur la surveillance de la qualité de service Skype, voir «Surveillance de la qualité de service Skype», à la page 548.
- Modifiez le compte utilisateur d'utilisateur local à utilisateur de domaine. Pour plus de détails, voir «Modification du compte utilisateur», à la page 547.
- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.
- Pour obtenir de l'aide sur le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Lorsque vous installez l'agent Microsoft Office 365, il doit être configuré et démarré manuellement après avoir défini les paramètres de configuration. Utilisez le fichier de réponses silencieux pour configurer les paramètres personnalisés.

Avant de commencer

Editez le fichier de réponses pour modifier les paramètres de configuration par défaut suivants :

KMO_USER_NAME
Nom d'utilisateur de l'administrateur global Office 365.

KMO_PASSWORD
Mot de passe de l'administrateur global Office 365.

KMO_MAIL_ADDRESSES1
Liste des adresses e-mail à cibler pour vérifier l'accessibilité de la boîte aux lettres. La liste d'adresses e-mail doit être délimitée à l'aide de point-virgules.

KMO_SKYPE
Ce paramètre permet d'activer la collecte des transactions synthétiques de qualité de service Skype.

KMO_DATA_COLLECTION_DURATION
Durée (en heures) pendant laquelle l'agent attend d'extraire les données d'utilisation de la boîte aux lettres et de OneDrive.

Le fichier de réponses se trouve à l'emplacement suivant :
`<CANDLEHOME>\samples`

Pourquoi et quand exécuter cette tâche
Vous pouvez configurer l'agent lorsqu'il est arrêté ou en cours d'exécution. L'agent reste au même état après la configuration. Par exemple, si l'agent est en cours d'exécution, il reste à l'état en cours d'exécution après la configuration.

Procédure

Pour configurer l'agent Microsoft Office 365, procédez comme suit :

1. A l'invite de commande, accédez au répertoire qui contient le fichier `microsoft_office365-agent.bat`.
2. Entrez la commande `microsoft_office365-agent.bat` *chemin d'accès absolu au fichier de réponses*.

   Le fichier de réponses contient les paramètres suivants :
3. Si l'agent est arrêté, démarrez-le.

Que faire ensuite

- Configurez les fonctionnalités de transaction synthétique Skype pour surveiller les transactions synthétiques de qualité de service Skype. Pour plus d'informations sur la surveillance de la qualité de service Skype, voir «Surveillance de la qualité de service Skype», à la page 548.
- Modifiez le compte utilisateur d'utilisateur local à utilisateur de domaine. Pour plus de détails, voir «Modification du compte utilisateur», à la page 547.
- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.
- Pour obtenir de l'aide sur le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Modification du compte utilisateur

Après avoir configuré l'agent Microsoft Office 365, modifiez le compte utilisateur d'utilisateur local en utilisateur de domaine.

Pourquoi et quand exécuter cette tâche
Par défaut, l'agent Microsoft Office 365 s'exécute sous le compte utilisateur local.

Procédure

1. Exécutez la commande suivante pour vérifier l'ID utilisateur qui est utilisé pour démarrer l'agent :

   rép_install\InstallITM\KinCinfo.exe -r
2. Si l'agent de surveillance a été démarré avec un ID utilisateur qui n'appartient pas au groupe Administrateur, arrêtez l'agent.
3. Ouvrez la fenêtre **Manage Monitoring Services**.

4. Dans la fenêtre **Manage Monitoring Services**, cliquez avec le bouton droit sur l'instance de l'agent et cliquez sur **Modifier le démarrage**.
5. Indiquez l'ID utilisateur complet sous la forme <Domaine\ID_utilisateur>, puis indiquez le mot de passe.
6. Lancez la agent Microsoft Office 365.

Surveillance de la qualité de service Skype

Pour surveiller la qualité de service Skype, un utilisateur doit configurer les utilitaires de gestion des transactions synthétiques Skype, `kmoskypecaller.exe` et `Kmoskypereceiver.exe`, sur le client Windows où l'agent est installé ou dans un environnement distribué où le client Skype for Business est configuré.

Avant de commencer

Pour exécuter des transactions synthétiques, vous devez mettre à jour le nom d'appelant et le nom de destinataire Skype dans le fichier <CANDLEHOME>
`\tmaitm6_x64\kmoskypecallerlist.properties` au format suivant :
`appelant skype = destinataire skype`
Par exemple, john@xyz.com = alan@xyz.com
Vous pouvez ajouter plusieurs destinataires d'appel Skype pour un seul appelant Skype au format suivant :
`appelant skype = liste de destinataires skype`
Par exemple, john@xyz.com = alam@xyz.com;bill@xyz.com;chuk@xyz.com

A faire : Si vous ne souhaitez pas exécuter de transactions synthétiques, mais que vous voulez surveiller la qualité de service Skype pour les utilisateurs en temps réel, la mise à jour du fichier <CANDLEHOME>
`\TMAITM6_x64 \kmoskypecallerlist.properties` n'est pas nécessaire.

Pourquoi et quand exécuter cette tâche

Lorsque l'agent Microsoft Office 365 est configuré et démarré, les fichiers et dossiers suivants sont créés dans le répertoire <CANDLEHOME>`\TMAITM6_x64\` :

- `kmoskypecaller.properties`
- `kmoskypecallerlist.properties`
- `KMOSynthTransSkype.zip`
- `KMOSkypeTransReceiver.zip`

En outre, le fichier `kmoskypecaller.properties` est mis à jour avec l'IP et le port de serveur qui sont utilisés pour la communication entre l'agent et l'utilitaire kmoskypecaller.

Procédure

Pour configurer l'appelant Skype et les destinataires Skype et lancer des transactions synthétiques, telles que la messagerie instantanée, les appels audio et vidéo, et les sessions de partage d'application, effectuez les étapes suivantes :

1. Démarrez l'agent Office 365.
2. Copiez le fichier `KMOSynthTransSkype.zip` du client d'agent vers le client Windows à partir duquel l'appel Skype doit être initié.
3. Procédez à l'extraction du fichier `KMOSynthTransSkype.zip`.
4. Copiez le fichier `kmoskypecaller.properties` du client d'agent vers le dossier `KMOSynthTransSkype` extrait sur le client Windows à partir duquel l'appel Skype doit être initié.
5. Copiez le fichier `KMOSkypeTransReceiver.zip` à partir du client d'agent sur tous les clients Windows sur lesquels les appels Skype doivent être reçus.

6. Extrayez le fichier `KM0SkypeTransReceiver.zip` sur tous les clients Windows sur lesquels les appels Skype doivent être reçus, et exécutez `KM0SkypeTransReceiver.exe` pour lancer la réception de messages.
7. Pour initier les transactions synthétiques, exécutez le fichier `KM0SynthTransSkype.exe`, qui est disponible dans le dossier d'extraction `KM0SynthTransSkype` sur le client Windows. L'agent Office 365 doit commencer à recevoir les données de surveillance Skype du client appelant.

Résultats
L'agent démarre la surveillance de la qualité de service Skype.

Définition des variables d'environnement local

Vous pouvez configurer les variables d'environnement local pour modifier le comportement de agent Microsoft Office 365.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **Agents IBM Monitoring** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, dans le menu **Actions**, cliquez sur **Advanced > Edit ENV File**.
3. Dans le fichier des variables d'environnement, entrez les valeurs pour les variables d'environnement.

   Pour plus d'informations sur les variables d'environnement que vous pouvez configurer, voir «Variables d'environnement local», à la page 549.

Variables d'environnement local
Vous pouvez changer le comportement de agent Microsoft Office 365 en définissant les variables d'environnement local.

Variables permettant de définir la méthode de collecte des données pour l'agent

Pour définir la méthode de collecte de données pour l'agent, utilisez les variables d'environnement suivantes :

- **CDP_DP_INITIAL_COLLECTION_DELAY** : cette variable permet de définir l'intervalle (en secondes) après lequel le pool d'unités d'exécution commence sa collecte de données.
- **KMO_MAILBOX_REACHABILITY_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en minutes) pour le groupe d'attributs d'accessibilité de la boîte aux lettres.
- **KMO_SKYPE_REPORT_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en heures) pour la fonction de statistiques d'utilisation de Skype for Business.
- **KMO_SERVICE_API_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en minutes) pour la fonction de santé du service Office 365.
- **KMO_NETWORK_CONNECTION_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en minutes) pour la fonction de connectivité Internet.
- **KMO_NETWORK_PERFORMANCE_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en minutes) pour la fonction de performances réseau des services Office 365.
- **KMO_SITE_CONNECTION_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en minutes) pour la fonction de connectivité Office 365.
- **KMO_SPSITE_COLLECTION_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en minutes) pour la fonction de détails SharePoint Sites.
- **KMO_UASGE_STATS_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en heures) pour la fonction de statistiques sur l'utilisateur et l'utilisation des services Office 365.
- **KMO_TENANT_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en minutes) pour la fonction de détails du titulaire Office 365.

- **KMO_ONEDRIVE_CONNECTIVITY_INTERVAL** : cette variable permet de définir l'intervalle de collecte de données (en minutes) pour la fonction de connectivité Office 365 OneDrive.
- **KMO_TENANT_DOMAIN** : cette variable permet de définir le nom de domaine du titulaire.

Configuration de la surveillance de Microsoft SharePoint Server

Lorsque vous installez Monitoring Agent for Microsoft SharePoint Server, il est configuré automatiquement avec les paramètres de configuration par défaut. Utilisez le fichier de réponses silencieux pour modifier les paramètres de configuration par défaut.

Avant de commencer

Veillez à exécuter les tâches suivantes :

- Vérifiez que l'utilisateur, qui se connecte à l'environnement ou à l'application Microsoft SharePoint Server, dispose des privilèges d'administrateur. Utilisez un utilisateur existant disposant des privilèges d'administrateur ou créez-en un nouveau. Ajoutez le nouvel utilisateur au groupe Administrateurs pour qu'il bénéficie des privilèges d'administrateur.

  A faire : Pour configurer l'agent MicrosoftSharePoint Server, vous pouvez utiliser un utilisateur local ou un utilisateur de domaine à condition que celui-ci dispose des privilèges d'administrateur.
- Editez le fichier de réponses et modifiez les paramètres de configuration par défaut.

  Le fichier de réponses contient les paramètres suivants :

  KQP_DB_User
  ID utilisateur de la base de données.

  KQP_DB_Password
  Mot de passe de la base de données.

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent MicrosoftSharePoint Server.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent. Pour accéder à la documentation des versions d'agent antérieures, reportez-vous au tableau ci-après.

Tableau 180. Versions d'agent et documentation

Version de l'agent MicrosoftSharePoint Server	Documentation
06.31.09.00, 06.31.10.00	IBM Cloud Application Performance Management
06.31.09.00	IBM Performance Management 8.1.3 **Remarque :** Le lien ouvre une rubrique Knowledge Center sur site.
06.31.07.00	IBM Performance Management 8.1.2 **Remarque :** Le lien ouvre une rubrique Knowledge Center sur site.

Procédure

Pour configurer l'agent MicrosoftSharePoint Server, procédez comme suit :

1. Ouvrez l'invite de commande.
2. Modifiez le chemin d'accès au répertoire qui contient le fichier `ms_sharepoint_server-agent.bat`.

3. Entrez la commande **ms_sharepoint_server-agent.bat config** *chemin d'accès absolu au fichier de réponses*
4. Si l'agent est arrêté, démarrez-le.

Que faire ensuite
Après avoir configuré l'agent, vous pouvez modifier le compte utilisateur d'utilisateur local à utilisateur de domaine. Pour connaître les étapes de modification du compte utilisateur, voir «Modification du compte utilisateur», à la page 551.

Modification du compte utilisateur

Après avoir configuré l'agent MicrosoftSharePoint Server, vous pouvez modifier le compte utilisateur d'utilisateur local à utilisateur de domaine.

Pourquoi et quand exécuter cette tâche
Lorsque l'agent s'exécute sous l'utilisateur de domaine, il peut surveiller tous les composants du agent MicrosoftSharePoint Server.

Procédure

Pour modifier le compte utilisateur, procédez comme suit :

1. Exécutez la commande suivante pour vérifier l'ID utilisateur qui est utilisé pour démarrer l'agent.
   rép_install\InstallITM\KinCinfo.exe -r
2. Si l'agent de surveillance a été démarré avec un ID utilisateur qui n'appartient pas au groupe Administrateur, arrêtez l'agent.
3. Ouvrez la fenêtre **Manage Monitoring Services**.
4. Cliquez avec le bouton droit de la souris sur l'instance de l'agent, puis cliquez sur **Modifier le démarrage**.
5. Indiquez l'ID utilisateur complet sous la forme `<Domaine\ID_utilisateur>`, puis indiquez le mot de passe.
6. Démarrez l'agent de surveillance.

Que faire ensuite
Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Exécution de Monitoring Agent for Microsoft SharePoint Server en tant qu'utilisateur non-administrateur

Des stratégies de sécurité locales sont disponibles pour permettre à un utilisateur non-administrateur d'exécuter un Monitoring Agent for Microsoft SharePoint Server.

Pourquoi et quand exécuter cette tâche

La combinaison des deux stratégies de sécurité locales suivantes permet à un utilisateur non-administrateur d'exécuter l'agent MicrosoftSharePoint Server :

1. Déboguer les programmes.
2. Ouvrir une session en tant que service.

Suivez la procédure fournie pour accorder des droits de sécurité locaux à un utilisateur non-administrateur.

Procédure

1. Accédez à TEMA et définissez les paramètres de démarrage de l'agent MicrosoftSharePoint Server pour un utilisateur non-administrateur.
2. Ajoutez l'utilisateur non-administrateur dans le répertoire HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office Server sous la clé de Registre et accordez des droits en lecture au répertoire.
3. Ajoutez l'utilisateur non-administrateur dans le répertoire HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server Extensions sous la clé de Registre et accordez des droits en lecture à ce répertoire.
4. Ajoutez manuellement l'utilisateur non-administrateur dans le répertoire HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server Extensions\16.0\Secure\ sous la clé de Registre et accordez des droits en lecture à ce répertoire.
5. Ajoutez l'utilisateur non-administrateur dans le répertoire HKEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring sous la clé de Registre et accordez des droits d'accès complets à ce répertoire.
6. Ajoutez l'utilisateur non-administrateur dans le répertoire HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib sous la clé de Registre et accordez des droits en lecture à ce répertoire.
7. Ajoutez l'utilisateur non-administrateur dans le dossier d'installation de l'agent SharePoint (le dossier Candle, par exemple, C:\IBM\APM) et accordez des droits d'accès complets à ce dossier.
8. Exécutez la commande **secpol.msc** dans le **menu Démarrer** pour ouvrir la **Stratégie de sécurité locale**.
9. Pour ajouter l'utilisateur non-administrateur à la stratégie de sécurité locale, voir «Droits de la stratégie de sécurité locale», à la page 552.
10. Ajoutez l'utilisateur non-administrateur au groupe d'utilisateurs Connexion à SQL Server. L'utilisateur doit disposer des droits du rôle sysadmin SQL Server sur le serveur SQL Server.
11. Redémarrez l'agent MicrosoftSharePoint Server.
12. Vérifiez le statut de l'agent MicrosoftSharePoint Server et les données sur le portail APM.
13. Les groupes d'attributs suivants affichent les données relatives aux utilisateurs qui sont membres du groupe Administrateurs.
    a) Disponibilité
    b) Service Web

Droits de la stratégie de sécurité locale

Des stratégies de sécurité locales sont disponibles pour qu'un utilisateur non-administrateur puisse exécuter un agent MicrosoftSharePoint Server. Ces stratégies permettent de démarrer, d'arrêter, de configurer l'agent ou d'en vérifier les données. Vous trouverez ci-dessous deux stratégies de sécurité locales grâce auxquelles un utilisateur non-administrateur peut exécuter l'agent MicrosoftSharePoint Server :

Octroi du droit Ouvrir une session en tant que service
Vous pouvez accorder le droit Ouvrir une session en tant que service.

Pourquoi et quand exécuter cette tâche
Pour accorder le droit Ouvrir une session en tant que service, suivez la procédure relative à l'agent MicrosoftSharePoint Server décrite ci-dessous :

Procédure

1. Cliquez sur **Démarrer** > **Outils d'administration** > **Stratégie de sécurité locale**. La fenêtre **Stratégie de sécurité locale** s'affiche.
2. Dans la sous-fenêtre de navigation, développez **Stratégie locale**, puis cliquez sur **Attribution des droits utilisateur**. La liste des droits utilisateur s'affiche.

3. Cliquez deux fois sur la stratégie **Ouvrir une session en tant que service**. La fenêtre **Propriétés de Ouvrir une session en tant que service** apparaît.
4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre **Sélectionner des utilisateurs ou des groupes** apparaît.
5. Dans la zone **Entrer les noms d'objet à sélectionner**, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **OK**.

Octroi du droit Déboguer les programmes
Vous pouvez accorder le droit Déboguer les programmes.

Pourquoi et quand exécuter cette tâche
Pour accorder le droit Déboguer les programmes, suivez la procédure relative à l'agent MicrosoftSharePoint Server décrite ci-dessous :

Procédure

1. Cliquez sur **Démarrer** > **Outils d'administration** > **Stratégie de sécurité locale**. La fenêtre **Stratégie de sécurité locale** s'affiche.
2. Développez **Stratégie locale**, puis cliquez sur **Attribution des droits utilisateur**. La liste des droits utilisateur s'affiche.
3. Cliquez deux fois sur la stratégie **Déboguer les programmes**. La fenêtre **Propriétés de Déboguer les programmes** apparaît.
4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre **Sélectionner des utilisateurs ou des groupes** apparaît.
5. Dans la zone Entrer les noms d'objet à sélectionner, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **OK**.

Configuration de la surveillance de Microsoft SQL Server

Vous devez configurer Monitoring Agent for Microsoft SQL Server pour qu'il puisse collecter des données de l'application surveillée.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Microsoft SQL Server.

Vous pouvez installer et configurer l'agent Microsoft SQL Server en local à l'aide de l'interface d'invite de commande. Vérifiez que l'agent est installé sur le serveur surveillé.

Pourquoi et quand exécuter cette tâche

Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

L'agent Microsoft SQL Server est un agent multi-instance ; vous devez configurer et démarrer chaque instance d'agent manuellement.

- Pour configurer l'agent, procédez comme suit :
  - Créez un utilisateur et accordez-lui les droits requis
  - Sélectionnez les bases de données à surveiller

  - Configurez les variables d'environnement local
- Pour exécuter l'agent dans un environnement cluster, procédez comme décrit dans la rubrique "Exécution de l'agent dans un environnement cluster".

Création d'un utilisateur et attribution des droits d'accès

Sur Microsoft SQL Server, vous devez créer un utilisateur sous lequel l'agent sera exécuté, puis octroyer des droits d'accès à l'utilisateur pour la surveillance de Microsoft SQL Server. Le processus d'attribution de droits est identique pour Microsoft SQL Server 2005 et les versions ultérieures.

Avant de commencer

Installez l'agent Microsoft SQL Server. Pour créer un utilisateur et lui octroyer des droits d'accès, vous devez être un administrateur de base de données avec le rôle d'autorisation sysdamin.

Pourquoi et quand exécuter cette tâche

Utilisez la procédure suivante pour déterminer si un utilisateur SQL Server existant dispose de droits suffisants pour surveiller Microsoft SQL Server :

- Windows «Vérification des droits d'un utilisateur SQL Server existant», à la page 554

Utilisez l'une des procédures suivantes pour créer un utilisateur :

- Windows «Création d'un ID utilisateur SQL Server avec l'authentification Windows», à la page 555
- Linux Windows «Création d'un ID utilisateur SQL Server avec l'authentification SQL Server», à la page 556

Utilisez la procédure suivante pour octroyer des droits :

- Windows «Octroi de droits d'accès minimum pour la collecte de données», à la page 556
- Windows «Octroi d'un droit à la clé de registre Perflib lui permettant de collecter les données de quelques ensembles de données», à la page 558

Vérification des droits d'un utilisateur SQL Server existant

Windows Vous pouvez exécuter l'utilitaire **koqVerifyPerminssions.exe** pour vérifier si un utilisateur SQL Server existant dispose de droits suffisants pour les bases de données SQL Server.

Pourquoi et quand exécuter cette tâche

L'utilitaire **koqVerifyPerminssions.exe** renvoie le message PASS si l'utilisateur possède le rôle **sysadmin** ou les droits minimaux requis. Le résultat détaillé de la vérification est consigné dans `koqVerifyPermissions_log`.

Les droits minimaux sont répertoriés ci-dessous :

- Les droits du serveur doivent inclure **Afficher l'état du serveur**, **Afficher une base de données** et **Afficher une définition**.

  Ces droits de niveau serveur sont obligatoires.
- Pour toutes les bases de données système et les bases de données définies par l'utilisateur pour la surveillance, l'appartenance au rôle de base de données doit inclure **public** et **db_owner**.

  Les droits **db_owner** sont requis pour collecter des données des ensembles de données suivants :
  - Ensemble de données des détails du serveur
  - Ensemble de données des détails de la base de données
  - Ensemble de données de la fonction miroir de la base de données
  - Ensemble de données du récapitulatif du serveur
  - Ensemble de données du récapitulatif du journal

- Pour la base de données **msdb**, l'appartenance au rôle de base de données doit inclure **db_datareader**, **SQLAgentReaderRole** et **SQLAgentUserRole**. Ces droits sont requis pour l'ensemble de données Détails du travail.

Procédure

1. Lancez l'invite de commande et accédez au répertoire de l'utilitaire ci-après.
   - Pour les agents 64 bits, *rép_base_agent*\TMAITM6_x64
   - Pour les agents 32 bits, *rép_base_agent* \TMAITM6

   , *rép_base_agent* représentant le répertoire d'installation de l'agent.
2. Exécutez la commande **koqVerifyPerminssions.exe** en spécifiant les paramètres suivants :

   ```
   koqVerifyPermissions.exe -S nom_instance -U nom_utilisateur -P mot_passe
   ```

   Où :
   - *nom_instance* représente le nom de l'instance SQL Server.
   - *nom_utilisateur* représente le nom d'utilisateur vérifié par l'utilitaire.
   - *mot_passe* représente le mot de passe de l'utilisateur. Ce paramètre est requis si *nom_utilisateur* est spécifié.

   Remarque : Si *nom_utilisateur* et *mot_passe* ne sont pas spécifiés, l'utilisateur par défaut connecté au système est utilisé. Exemple : `NT AUTHORITY\SYSTEM`.

Résultats

Le résultat détaillé de la vérification est disponible dans `koqVerifyPermissions_log`, dans le répertoire suivant :

- Pour les agents 64 bits, *rép_base_agent*\TMAITM6_x64\logs
- Pour les agents 32 bits, *rép_base_agent* \TMAITM6\logs

, *rép_base_agent* représentant le répertoire d'installation de l'agent.

Création d'un ID utilisateur SQL Server avec l'authentification Windows

Windows Créez un utilisateur avec l'authentification Windows et affectez-lui les rôles et droits d'accès requis.

Procédure

Pour créer un utilisateur, procédez comme suit :

1. Dans **SQL Server Management Studio**, ouvrez **Object Explorer**.
2. Cliquez sur ***nom_instance_serveur*** > **Sécurité Connexions**.
3. Cliquez avec le bouton droit de la souris sur **Connexions** et sélectionnez **Nouvelle connexion**.
4. Dans la zone **Nom de connexion** de la page **Général**, entrez le nom d'un utilisateur Windows.
5. Sélectionnez **Authentification Windows**.
6. En fonction du rôle et des droits d'accès que vous souhaitez affecter à cet utilisateur, effectuez l'une des tâches suivantes :
   - Dans la page Rôles du serveur, affectez le rôle *sysadmin* au nouvel ID de connexion.
   - Si vous ne souhaitez pas affecter le rôle *sysadmin* à l'utilisateur, octroyez-lui des droits d'accès minimum en effectuant les étapes mentionnées dans la rubrique «Octroi de droits d'accès minimum pour la collecte de données», à la page 556.

   Important : Par défaut, le rôle *public* est affecté au nouvel ID de connexion.
7. Cliquez sur **OK**.

Résultats
Un utilisateur est créé avec le rôle *public* par défaut et les droits d'accès que vous lui avez affectés ; il est affiché dans la liste **Connexions**.

Création d'un ID utilisateur SQL Server avec l'authentification SQL Server

Linux Windows Créez un utilisateur avec l'authentification SQL Server et affectez-lui les rôles et droits d'accès requis.

Procédure

Pour créer un utilisateur, procédez comme suit :

1. Dans **SQL Server Management Studio**, ouvrez **Object Explorer**.
2. Cliquez sur ***nom_instance_serveur*** > **Sécurité Connexions**.
3. Cliquez avec le bouton droit de la souris sur **Connexions** et sélectionnez **Nouvelle connexion**.
4. Dans la zone **Nom de connexion** de la page **Général**, entrez le nom d'un nouvel utilisateur.
5. Sélectionnez **Authentification SQL Server**.
6. Dans la zone **Mot de passe**, entrez un mot de passe pour l'utilisateur.
7. Dans la zone **Confirmer le mot de passe**, entrez le mot de passe que vous avez saisi dans la zone **Mot de passe** une seconde fois.
8. En fonction du rôle et des droits d'accès que vous souhaitez affecter à cet utilisateur, effectuez l'une des tâches suivantes :
   - Dans la page Rôles du serveur, affectez le rôle *sysadmin* au nouvel ID de connexion.
   - Si vous ne souhaitez pas affecter le rôle *sysadmin* à l'utilisateur, octroyez-lui des droits d'accès minimum en effectuant les étapes mentionnées dans la rubrique «Octroi de droits d'accès minimum pour la collecte de données», à la page 556.

   Important : Par défaut, le rôle *public* est affecté au nouvel ID de connexion.
9. Cliquez sur **OK**.

Résultats
Un utilisateur est créé avec le rôle *public* par défaut et les droits d'accès que vous lui avez affectés ; il est affiché dans la liste **Connexions**.

Octroi de droits d'accès minimum pour la collecte de données

Windows En dehors du rôle **public** par défaut, vous pouvez affecter le rôle **sysadmin** à un utilisateur ou lui octroyer les droits minimaux pour que l'agent puisse collecter des données pour les ensembles de données.

Pourquoi et quand exécuter cette tâche
Vous pouvez octroyer les droits via l'interface utilisateur ou l'utilitaire **`permissions.cmd`**.

Procédure

- Pour octroyer les droits d'accès minimaux à l'utilisateur via l'interface utilisateur, procédez comme suit :
  a) Ouvrez la page **Rôles du serveur** et vérifiez que la case **public** est cochée.
  b) Ouvrez la page **Mappage de l'utilisateur**, puis cochez les cases suivantes pour toutes les bases de données système et les bases de données définies par l'utilisateur que vous souhaitez surveiller :
     – **public**
     – **db_owner**

     Pour la base de données **msdb**, cochez les cases supplémentaires suivantes :
     – **db_datareader**

- **SQLAgentReaderRole**
- **SQLAgentUserRole**

c) Ouvrez la page **Securables**, puis cochez les cases suivantes pour l'instance de serveur que vous surveillez :

- view database
- view definition
- view server state

- Pour octroyer les droits d'accès minimaux à l'utilisateur à l'aide de l'utilitaire **permissions.cmd**, procédez comme suit :

a) Lancez Windows Explorer et accédez au répertoire *rép_octroi_droits_agent* de l'utilitaire :

- Pour l'agent 64 bits, *rép_octroi_droits_agent* correspond à *rép_base_agent* \TMAITM6_x64\scripts\KOQ\GrantPermission.
- Pour l'agent 32 bits, *rép_octroi_droits_agent* correspond à *rép_base_agent* \TMAITM6\scripts\KOQ\GrantPermission.
- *rép_base_agent* représente le répertoire d'installation de l'agent.

Avertissement : L'utilitaire **permissions.cmd** octroie les droits **db_owner** sur toutes les bases de données par défaut. Pour exclure certaines bases de données, vous devez ajouter les noms de base de données dans le fichier *rép_octroi_droits_agent* \exclude_database.txt. Les noms de base de données doivent être séparés par le symbole alias **@**.

Conseil : Par exemple, si vous souhaitez exclure les bases de données **MyDatabase1** et **MyDatabase2**, ajoutez l'entrée suivante dans le fichier exclude_database.txt :

```
MyDatabase1@MyDatabase2
```

b) Cliquez deux fois sur **permissions.cmd** pour lancer l'utilitaire.

c) Entrez les valeurs de paramètre prévues lorsque vous y êtes invité :

Tableau 181. Paramètres

Paramètres	**Description**
Nom SQL Server ou nom d'instance SQL Server	Entrez le nom SQL Server cible ou le nom d'instance SQL Server cible qui doit octroyer les droits à l'utilisateur.
Nom de connexion de l'utilisateur SQL Server existant	Entrez le nom d'utilisateur dont les droits seront modifiés.
Options de droits : **1** Octroie les droits **db_owner** **2** Octroie les droits **db_datareader**, **SQLAgentReaderRole** et **SQLAgentUserRole** **3** Octroie tous les droits requis	Entrez **1**, **2** ou **3** selon vos besoins.
Utilisateur auquel les droits doivent être octroyés : **1** Utilisateur actuellement connecté au système **2** Autre utilisateur	Entrez **1** ou **2**. Si **2** est sélectionné, entrez le nom d'utilisateur cible lorsque vous y êtes invité. **Remarque :** Les utilisateurs doivent avoir accès pour octroyer des droits à d'autres utilisateurs.

Que faire ensuite
Configurez l'agent.

Octroi d'un droit à la clé de registre Perflib lui permettant de collecter les données de quelques ensembles de données

Windows Pour collecter les données de quelques ensembles de données, vous devez accorder aux utilisateurs un accès en lecture à la clé de registre Perflib.

Pourquoi et quand exécuter cette tâche

Vous devez accorder ce droit à l'utilisateur Windows avec lequel les services d'agent sont configurés. Un grand nombre d'ensembles de données sont affectés en l'absence de droits Perflib, tels que MS SQL Database Detail, MS SQL Memory Manager, MS SQL Lock Resource Type Summary, MS SQL Job Summary, MS SQL Server Transactions Summary, MS SQL Server Summary, etc.

Procédure

Pour accorder ce droit à la clé de registre Perflib, procédez comme suit :

1. Pour ouvrir l'éditeur de registre, cliquez sur **Démarrer** > **Exécuter** > **Regedit.exe**, et appuyez sur **Entrée**.
2. Accédez à la clé de registre `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT \CurrentVersion\Perflib`.
3. Cliquez avec le bouton droit de la souris sur la clé **Perflib**, puis cliquez sur **Droits**.
4. Cliquez sur **Ajouter**, entrez le nom de l'utilisateur Windows avec lequel l'agent est installé et configuré, puis cliquez sur **OK**.
5. Cliquez sur l'utilisateur que vous avez ajouté.
6. Accordez à l'utilisateur un accès en lecture en cochant la case correspondante.
7. Cliquez sur **Appliquer**, puis sur **OK**.

Variables d'environnement local

Vous pouvez changer le comportement de agent Microsoft SQL Server en définissant les variables d'environnement local.

Variables de vérification de disponibilité du service SQL Server

Pour vérifier la disponibilité du service SQL Server, ajoutez les variables d'environnement suivantes :

- **COLL_MSSQL_RETRY_INTERVAL** : cette variable définit l'intervalle entre deux tentatives (en minutes) de vérification du statut du service SQL Server. Si la valeur est inférieure ou égale à zéro, la variable utilise la valeur par défaut 1 minute.
- **COLL_MSSQL_RETRY_CNT** : cette variable définit le nombre de tentatives de l'agent SQL pour vérifier que le service SQL Server est démarré. Si le service SQL Server n'est pas démarré après le nombre de tentatives spécifié dans cette variable, le collecteur s'arrête. Si la valeur de la variable est inférieure ou égale à zéro, la variable utilise la valeur par défaut 3.

Variables de surveillance du fichier journal des événements SQL Server

Pour surveiller l'ensemble de données MS SQL Error Event Details, utilisez les variables d'environnement suivantes :

- **COLL_ERRORLOG_STARTUP_MAX_TIME** : cette variable définit l'intervalle de temps (T) de la collecte des erreurs avant le démarrage de l'agent. La valeur par défaut est `0` minutes. Cette variable peut avoir les valeurs suivantes :

  T = 0
  L'agent démarre la surveillance du fichier journal des erreurs lorsqu'il démarre ou redémarre. L'agent ne lit pas les erreurs consignées dans le fichier journal des erreurs avant son démarrage.

T = 1
L'agent surveille le fichier journal des erreurs en fonction des valeurs suivantes définies pour la variable **COLL_ERRORLOG_STARTUP_MAX_EVENT_ROW** représentée par R :

- Si R < 0, l'agent démarre la surveillance du fichier journal des erreurs lorsqu'il démarre ou redémarre.
- Si R = 1, l'agent surveille toutes les erreurs consignées dans le fichier journal des erreurs.
- Si R > 1 et que l'agent est installé pour la première fois, l'agent surveille le fichier journal jusqu'à ce que R erreurs soient surveillées. Si R > 1 et que l'agent est redémarré, l'agent surveille les R erreurs précédemment non prises en compte.

T > 1
L'agent surveille toutes les erreurs précédentes consignées jusqu'au nombre de minutes T à partir de son démarrage ou redémarrage. L'agent qui surveille dépend également des valeurs suivantes que vous définissez pour la variable **COLL_ERRORLOG_STARTUP_MAX_EVENT_ROW** :

- Si R ≤ 0, l'agent démarre la surveillance du fichier journal des erreurs lorsqu'il démarre ou redémarre.
- Si R = 1, l'agent surveille toutes les erreurs consignées dans le fichier journal jusqu'à T minutes.
- Si R > 1, l'agent ne surveille pas plus de R erreurs consignées au cours des T dernières minutes.

- **COLL_ERRORLOG_STARTUP_MAX_EVENT_ROW** : cette variable définit le nombre maximum d'erreurs devant être traitées au démarrage de l'agent. La valeur par défaut est 0. Vous pouvez affecter les valeurs suivantes à la variable :

  R = 0
  L'agent démarre la surveillance du fichier journal des erreurs, dès qu'il démarre ou qu'il redémarre. Il ne lit pas les erreurs qui ont été créées dans le fichier journal des erreurs avant son démarrage.

  R = 1
  L'agent surveille les erreurs consignées au cours des T dernières minutes depuis son démarrage ou redémarrage.

  R > 1
  L'agent surveille les erreurs R consignée au cours des T dernières minutes.

- **COLL_ERRORLOG_MAX_EVENT_ROW** : cette variable fournit le nombre de lignes d'erreur. La valeur par défaut est 50. Vous pouvez affecter les valeurs suivantes à la variable :

  X = 0
  L'agent n'affiche pas les journaux d'erreur.

  X > 0
  L'agent affiche x lignes d'erreur.

- **COLL_ERRORLOG_RECYCLE_WAIT** : cette variable indique l'intervalle de temps (en secondes) pendant lequel l'agent Microsoft SQL Server attend de collecter les données du groupe d'attributs MS SQL Error Event Detail lorsque la situation de ce groupe d'attributs est déclenchée. Attribuez une valeur comprise entre 1 et 30 à cette variable. Si sa valeur est inférieure à 0, la variable utilise la valeur par défaut 0 (seconde). Si sa valeur est supérieure à 30, la variable utilise la valeur par défaut 30 (secondes).

Variable de définition du délai d'expiration de la requête

Pour définir l'intervalle du délai d'attente de requête pour l'agent SQL Server, utilisez les variables d'environnement suivantes :

- **QUERY_TIMEOUT** : cette variable d'environnement définit le délai maximum (en secondes) pendant lequel SQL Server attend une réponse pour une requête envoyée à SQL Server. La valeur par défaut de cette variable doit être inférieure à 45 secondes. Cependant, si vous définissez la valeur 0 pour cette variable, l'agent SQL Server attend indéfiniment une réponse de SQL Server. Si l'agent SQL Server accède à un grand nombre de bases de données verrouillées, vous devez affecter à cette variable une valeur comprise entre 10 et 20 secondes. Si la requête n'est pas traitée pendant le délai défini, l'agent SQL Server ignore la requête expiré et passe à la requête suivante dans la file d'attente. L'agent n'affiche pas de données pour la requête qui a expiré.

- **QUERY_THREAD_TIMEOUT** : cette variable d'environnement définit le délai maximum (en secondes) pendant lequel SQL Server attend une réponse pour une requête envoyée à SQL Server. Cette variable d'environnement est applicable à quelques groupes d'attributs qui utilisent la collecte basée sur les unités d'exécution. Par exemple, KOQDBD, KOQTBLD, KOQDEVD, etc. La valeur de cette variable n'a aucune limite, contrairement à la variable QUERY_TIMEOUT. Sinon, elle fonctionne de la même manière que la variable QUERY_TIMEOUT.

Variable d'affichage des informations sur les travaux activés

Pour afficher les informations relatives aux travaux activé dans l'ensemble de données MS SQL Job Detail, utilisez la variable d'environnement **COLL_JOB_DISABLED**. Si vous affectez à cette variable la valeur 1, agent Microsoft SQL Server n'affiche pas les informations relatives aux travaux activés. Si vous ne spécifiez pas cette variable, vous pouvez afficher les informations relatives aux travaux activés et désactivés.

Variable permettant de limiter le nombre de lignes dans l'ensemble de données Détail des groupes de fichiers MS SQL

Pour limiter le nombre de lignes extraites par le service de collecteur pour l'ensemble de données Détail des groupes de fichiers MS SQL, utilisez la variable d'environnement **COLL_KOQFGRPD_MAX_ROW**. Cette variable d'environnement définit le nombre maximal de lignes que le service de collecteur extrait pour l'ensemble de données Détail des groupes de fichiers. Si vous n'indiquez pas de valeur pour cette variable, le service de collecteur extrait 10000 lignes pour l'ensemble de données Détail des groupes de fichiers. Utilisez cette variable d'environnement pour modifier le nombre maximal de lignes par défaut dans le fichier `koqcoll.ctl`. Pour modifier le nombre maximal de lignes par défaut, procédez comme suit :

1. Indiquez le nombre maximal de lignes pour KOQFGRPD dans le fichier `koqcoll.ctl`.
2. Ajoutez la variable d'environnement **COLL_KOQFGRPD_MAX_ROW** et assurez-vous que la valeur de cette variable est identique à la valeur indiquée dans le fichier `koqcoll.ctl`.

Si la valeur du fichier `koqcoll.ctl` est inférieure à la valeur indiquée par la variable d'environnement **COLL_KOQFGRPD_MAX_ROW**, la valeur définie dans le fichier `koqcoll.ctl` est considérée comme la valeur représentant le nombre maximal de lignes.

Si la valeur du fichier `koqcoll.ctl` est supérieure à la valeur indiquée dans la variable d'environnement **COLL_KOQFGRPD_MAX_ROW**, la valeur de la variable d'environnement **COLL_KOQFGRPD_MAX_ROW** est considérée comme la valeur représentant le nombre maximal de lignes.

Variables d'optimisation de la collecte de l'ensemble de données Détail des groupes de fichiers MS SQL

Utilisez la variable **COLL_DBD_FRENAME_RETRY_CNT** pour indiquer le nombre de tentatives qui peuvent être effectuées pour déplacer le fichier `%COLL_HOME%_tmp_%COLL_VERSION%_%COLL_SERVERID%_%COLL_SERVERID%__FGRP_TEMP` vers le fichier `%COLL_HOME%_tmp_%COLL_VERSION%_%COLL_SERVERID%_%COLL_SERVERID%__FGRP_PREV`.

Si vous n'indiquez pas de valeur pour cette variable, l'agent Microsoft SQL Server fait trois tentatives de déplacement du fichier.

Variable permettant de limiter le nombre de lignes dans l'ensemble de données MS SQL Device Detail

Pour limiter le nombre de lignes extraites pour le service de collecteur de l'ensemble de données MS SQL Device Detail, utilisez la variable d'environnement **COLL_KOQDEVD_MAX_ROW**. Cette variable d'environnement définit le nombre maximal de lignes que le service de collecteur extrait pour l'ensemble de données Device Detail. Si vous n'indiquez pas de valeur pour cette variable, le service de collecteur extrait 10000 lignes pour l'ensemble de données Device Detail. Utilisez cette variable d'environnement pour modifier le nombre maximal de lignes par défaut dans le fichier `koqcoll.ctl`. Pour modifier le nombre maximal de lignes par défaut, procédez comme suit :

1. Indiquez le nombre maximal de lignes pour KOQDEVD dans le fichier `koqcoll.ctl`.
2. Ajoutez la variable d'environnement **COLL_KOQDEVD_MAX_ROW** et vérifiez que la valeur de cette variable est identique à celle indiquée dans le fichier `koqcoll.ctl`.

Si la valeur du fichier `koqcoll.ctl` est inférieure à la valeur indiquée par la variable d'environnement **COLL_KOQDEVD_MAX_ROW**, la valeur définie dans le fichier `koqcoll.ctl` est considérée comme la valeur représentant le nombre maximal de lignes.

Si la valeur du fichier `koqcoll.ctl` est supérieure à la valeur définie dans la variable d'environnement **COLL_KOQDEVD_MAX_ROW**, la valeur de la variable d'environnement **COLL_KOQDEVD_MAX_ROW** est considérée comme la valeur représentant le nombre maximal de lignes.

Variables d'optimisation de la collecte pour l'ensemble de données MS SQL Device Detail

Pour optimiser la collecte de l'ensemble de données MS SQL Device Detail, utilisez les variables d'environnement suivantes :

- **COLL_KOQDEVD_INTERVAL** : cette variable d'environnement permet d'indiquer un intervalle (en minutes) entre deux collectes consécutives de l'ensemble de données MS SQL Device Detail.

  Remarque : Par défaut, la collecte des données de l'ensemble de données Device Detail est lancée sur demande. Utilisez la variable **COLL_KOQDEVD_INTERVAL** pour démarrer une collecte basée sur des unités d'exécution pour l'ensemble de données Device Detail et définir l'intervalle entre deux collectes de ce type.
- **COLL_DBD_FRENAME_RETRY_CNT** : utilisez cette variable d'environnement pour indiquer le nombre de tentatives qui peuvent être effectuées pour déplacer le fichier `%COLL_HOME%_tmp_%COLL_VERSION%_%COLL_SERVERID%_%COLL_SERVERID%__DEVD_TEMP` vers le fichier `%COLL_HOME%_tmp_%COLL_VERSION%_%COLL_SERVERID%_%COLL_SERVERID%__DEVD_PREV`.

Si vous n'indiquez pas de valeur pour cette variable, l'agent Microsoft SQL Server fait une tentative de déplacement du fichier.

Variables d'optimisation de la collecte de l'ensemble de données MS SQL Database Detail

Pour optimiser la collecte de l'ensemble de données MS SQL Database Detail, utilisez les variables d'environnement suivantes :

- **COLL_KOQDBD_INTERVAL** : utilisez cette variable d'environnement pour indiquer un intervalle (en minutes) entre deux collectes basées sur une unité d'exécution consécutives de l'ensemble de données MS SQL Database Detail. Si vous n'indiquez pas de valeur pour cette variable ou si l'intervalle de temps spécifié est inférieur à 3 minutes, l'agent Microsoft SQL Server définit l'intervalle par défaut sur 3 minutes. Au cas où la collecte prend plus de temps, ou que les données sont fréquemment vues comme NOT_COLLECTED, vous pouvez vérifier la durée de la collecte en vous référant au journal `Database Detail Collection completed in %d seconds` et définir la valeur de la variable sur une valeur supérieure à la durée de collecte spécifiée dans le journal.
- **COLL_DBD_FRENAME_RETRY_CNT** : utilisez cette variable d'environnement pour indiquer le nombre de tentatives qui peuvent être effectuées pour déplacer le fichier `%COLL_HOME%_tmp_%COLL_VERSION%_%COLL_SERVERID%_%COLL_SERVERID%__DBD_TEMP` vers le fichier `%COLL_HOME%_tmp_%COLL_VERSION%_%COLL_SERVERID%_%COLL_SERVERID%__DBD_PREV`.

Si vous n'indiquez pas de valeur pour cette variable, l'agent Microsoft SQL Server fait une tentative de déplacement du fichier.

Variables d'optimisation de la collecte de l'ensemble de données MS SQL Database Details

Pour améliorer la collecte de l'ensemble de données MS SQL Database Details, utilisez les variables d'environnement suivantes :

- **COLL_AUDIT_TYPE** : utilisez cette variable pour activer ou désactiver la surveillance de journaux spécifiques. La valeur par défaut de la variable est [AL][FL][SL]. Par défaut, l'agent surveille les trois

types de journaux qui comprennent les journaux d'application, les fichiers de contrôle et les journaux de sécurité. La valeur de la variable inclut un code de deux caractères pour chaque type de journal :

- [AL] pour les journaux d'application
- [FL] pour les fichiers de contrôle
- [SL] pour les journaux de sécurité

Vous pouvez modifier la valeur de la variable afin de désactiver la surveillance du type de journal spécifique. Par exemple, si vous indiquez [AL][SL] comme valeur de la variable, les fichiers de contrôle ne sont pas surveillés. Si aucune valeur n'est associée à la variable, les détails de l'audit ne sont pas surveillés.

- **COLL_AUDIT_DURATION** : utilisez cette variable pour signaler les événements d'audit qui se sont produits lors de l'intervalle indiqué dans cette variable. Par exemple, si vous attribuez la valeur 7 à cette variable, les événements d'audit qui se sont produits au cours des sept dernières heures sont signalés par l'ensemble de données Détails de l'audit. La valeur par défaut de la variable **COLL_AUDIT_DURATION** est `24 heures`.
- **COLL_AUDIT_COLLECTION_INTERVAL** : la collecte basée sur les unités d'exécution de l'ensemble de données Détails de l'audit fournit les spécifications de toutes les bases de données incluses dans l'instance SQL Server. Utilisez cette variable pour définir l'intervalle de cette collecte basée sur des unités d'exécution. Par exemple, si vous attribuez la valeur 7 à cette variable, un nouvel ensemble de spécifications de base de données est extrait de l'instance SQL Server toutes les 7 heures. La valeur par défaut de la variable **COLL_AUDIT_COLLECTION_INTERVAL** est 24.

Variable d'optimisation de la collecte pour l'ensemble de données MS SQL Process Detail

Pour améliorer la collecte de l'ensemble de données MS SQL Process Detail, utilisez la variable **COLL_PROC_BLOCK_INTERVAL** avec les valeurs suivantes :

- Si **COLL_PROC_BLOCK_INTERVAL =** `0`, la collecte pour les attributs Durée du processus de blocage et Durée de ressource de blocage est désactivée.
- Si **COLL_PROC_BLOCK_INTERVAL =** *x*, l'intervalle entre les deux collectes de données consécutives pour les attributs Durée du processus de blocage et Durée de ressource de blocage est *x* minutes.

Si la variable **COLL_PROC_BLOCK_INTERVAL** n'est pas définie dans le répertoire `CANDLE_HOME`, l'intervalle entre les collectes de données consécutives est trois minutes.

Variable permettant l'exclusion d'objets verrouillés de la collecte de données

Si les requêtes envoyées pour les espaces de travail Détails de base de données, Détails des groupes de fichiers, Fonction miroir de la base de données et Détails des unités mettent du temps à s'exécuter, utilisez la variable **COLL_DBCC_NO_LOCK** pour exécuter une requête avec la valeur `WITH (NOLOCK)`. Cette variable permet à la requête de ne pas attendre dans la file d'attente lorsqu'un objet sur lequel elle s'exécute est verrouillé.

Variable permettant de définir les critères de recherche des lignes renvoyées par l'ensemble de données Détails de la table

Les lignes renvoyées par l'ensemble de données Détails de la table sont triées par ordre décroissant en fonction de la valeur définie pour la variable **COLL_TBLD_SORTBY**. La valeur par défaut de la variable **COLL_TBLD_SORTBY** est FRAG (pourcentage de fragmentation). Les valeurs admises sont ROWS (nombre de lignes dans une table), SPACE (espace utilisé par la table) et OPTSAGE (date des statistiques de l'optimiseur de la table).

Variable d'optimisation de la collecte pour les ensembles de données MS SQL Problem Detail et Problem Summary

- **COLL_ALERT_SEV** : utilisez cette variable pour définir le niveau de gravité des messages d'erreur affichés dans les ensembles de données Problem Detail et Problem Summary. Les messages d'erreur dont le niveau de gravité est supérieur ou égal à la valeur indiquée dans cette variable sont affichés

dans les ensembles de données Problem Detail et Problem Summary. Par exemple, si vous définissez la valeur 10 pour cette variable, les messages d'erreur dont le niveau de gravité est supérieur ou égal à 10 sont affichés dans les ensembles de données Problem Detail et Problem Summary. Si vous n'indiquez pas de valeur pour cette variable, les messages d'erreur dont le niveau de gravité est supérieur ou égal à 17 sont affichés dans les ensembles de données Problem Detail et Problem Summary.

- **COLL_SINCE_ERRORLOG_RECY** : utilisez cette variable pour surveiller uniquement les erreurs dont le niveau de gravité est élevé dans le fichier ERRORLOG. Si vous n'indiquez pas de valeur pour cette variable, la valeur de la variable est 0, ce qui signifie que pour la collecte des données, l'ensemble de données Problem Summary prend en compte les erreurs de gravité élevée qui sont lues dans le fichier ERRORLOG précédent. Pour surveiller uniquement les erreurs dont le niveau de gravité est élevé dans le fichier ERRORLOG en cours, définissez cette variable en indiquant la valeur 1.

Variables de définition de l'intervalle du délai d'attente

Pour définir l'intervalle du délai d'attente pour l'agent Microsoft SQL Server, vous pouvez utiliser les variables d'environnement suivantes :

- **WAIT_TIMEOUT** : utilisez cette variable pour définir le délai d'attente de l'agent Microsoft SQL Server. Si un ensemble de données prend plus de 45 secondes pour collecter des données, l'agent risque de se bloquer ou le déclenchement de situations risque d'être incorrect. Examinez le journal afin d'identifier les ensembles de données qui prennent plus de 45 secondes pour collecter les données et utilisez la variable **WAIT_TIMEOUT** pour augmenter le délai d'attente entre la procédure de l'agent et la procédure du collecteur.
- **COLL_DB_TIMEOUT** : utilisez cette variable pour définir le délai d'attente (en secondes) de n'importe quelle demande, comme l'exécution d'une requête sur une connexion de serveur SQL existante à effectuer avant de revenir à l'application. Si vous indiquez la valeur 0, il n'y a pas de délai d'attente. Si vous n'indiquez pas de valeur pour cette variable, l'agent attend 15 secondes avant de revenir à l'application.

Variables permettant de définir les propriétés des fichiers journaux du collecteur

Pour définir les propriétés des fichiers journaux du collecteur, vous pouvez utiliser les variables d'environnement suivantes :

- **COLL_WRAPLINES** : cette variable permet d'indiquer le nombre maximal de lignes dans le fichier `col.out`. La valeur par défaut de cette variable est 90000 lignes (2 Mo environ).
- **COLL_NUMOUTBAK** : cette variable permet d'indiquer le nombre de copies de sauvegarde des fichiers journaux du collecteur à créer. Par défaut, cinq copies de sauvegarde du fichier journal du collecteur sont créées. Le fichier de sauvegarde s'appelle `*.out`. Lorsque ce fichier de sauvegarde atteint sa taille maximale, il est renommé `*.ou1` et les derniers journaux sont placés dans le fichier `*.out`. Ainsi, pour cinq fichiers de sauvegarde, les journaux les plus anciens sont disponibles dans le fichier `*.ou5` et les journaux les plus récents sont disponibles dans le fichier `*.out`.

  Vous pouvez créer plus de cinq copies de sauvegarde des fichiers journaux du collecteur en indiquant l'une des valeurs suivantes dans la variable **COLL_NUMOUTBAK** :

  – Pour moins de dix fichiers de sauvegarde, indiquez le nombre de fichiers de sauvegarde que vous souhaitez créer dans la variable **COLL_NUMOUTBAK**. Par exemple, si vous indiquez 9 dans la variable **COLL_NUMOUTBAK**, neuf fichiers de sauvegarde sont créés.

  – Si le nombre de fichiers de sauvegarde est supérieur à 9 et inférieur à 1000, indiquez le nombre de fichiers de sauvegarde précédé par un tiret dans la variable **COLL_NUMOUTBAK**. Par exemple, si vous indiquez -352 dans la variable **COLL_NUMOUTBAK**, 352 fichiers de sauvegarde sont créés.
- **COLL_DEBUG** : utilisez cette variable pour activer le suivi complet du collecteur en attribuant cette variable à la valeur ddddddddd (10 fois "d").

Variable de suppression des fichiers temporaires

COLL_TMPFILE_DEL_INTERVAL : cette variable permet d'indiquer l'intervalle (en minutes) au-delà duquel les fichiers temporaires KOQ_<horodatage> doivent être supprimés. Si vous n'indiquez pas de

valeur pour cette variable, la valeur de la variable est 0, ce qui signifie que les fichiers temporaires doivent être supprimés immédiatement.

Variable pour le changement de pilote utilisée par l'agent MS SQL Server

Pour changer le pilote utilisé par l'agent Microsoft SQL Server, utilisez la variable d'environnement **KOQ_ODBC_DRIVER**. Cette variable spécifie le pilote utilisé par l'agent Microsoft SQL Server pour se connecter au serveur SQL. Si vous n'indiquez pas de valeur pour cette variable, l'agent utilise le pilote ODBC SQL Server comme pilote par défaut.

Remarque : Lorsque vous spécifiez le pilote Microsoft SQL Server, vérifiez que le nom du pilote est correct et que le pilote est répertorié sous l'option correspondante dans la source de données (ODBC).

Variable pour la connexion à une base de données SQL Server compatible AlwaysOn

KOQ_APPLICATION_INTENT : cette variable permet d'indiquer l'option de connexion lors de la connexion à SQL Server.
Détails de l'option **KOQ_APPLICATION_INTENT** :

- **Readonly** : la connexion est établie avec **ApplicationIntent** en tant que *readonly*.
- **Readwrite** : la connexion est établie avec **ApplicationIntent** en tant que *readwrite*.
  Lorsque l'option est définie sur Readwrite, l'agent Microsoft SQL Server n'effectue aucune opération d'écriture avec la connexion.

Si cette variable n'est pas définie, la connexion est établie sans propriété **ApplicationIntent**.

Remarque : Le pilote est spécifié par la variable d'environnement **KOQ_ODBC_DRIVER**. Si cette variable n'est pas définie, le pilote SQL Server par défaut est utilisé.
Si le pilote ne prend pas en charge **ApplicationIntent**, la connexion est établie sans propriété **ApplicationIntent**.

Paramètres de configuration de l'agent

Vous devez fournir les paramètres de configuration obligatoires de l'agent.

Pourquoi et quand exécuter cette tâche

Le tableau suivant contient les détails des paramètres de configuration. Passez ces derniers en revue et déterminez leur valeur.

Nom du paramètre	Description	Valeur par défaut	Zone obligatoire
User Name	Nom d'utilisateur ou login utilisé pour établir une connexion entre l'agent et le serveur SQL	N/A	Oui
Password	Mot de passe de l'utilisateur ou login	N/A	Oui
Database Version	Version de la base de données de serveur SQL à surveiller	N/A	Oui

Database Server Home Directory	Chemin de base de la base de données du serveur SQL	N/A	Oui
Error Log File Path	Emplacement du fichier journal des erreurs du serveur SQL	N/A	Oui

Configuration de l'agent sur des systèmes Windows

La fenêtre IBM Cloud Application Performance Management permet de configurer l'agent sur des systèmes Windows.

Avant de commencer

Pour pouvoir configurer l'agent, veillez à exécuter les tâches suivantes :

- Créez un utilisateur et accordez-lui les droits requis
- Passez en revue les variables d'environnement local

Pourquoi et quand exécuter cette tâche

L'agent Microsoft SQL Server est un agent multi-instance ; vous devez configurer et démarrer chaque instance d'agent manuellement.

- Pour configurer l'agent, procédez comme suit :
  - Sélectionnez les bases de données à surveiller
  - Configurez les variables d'environnement local

Sélection des bases de données à surveiller

Vous pouvez sélectionner la base de données à surveiller en utilisant la fenêtre **Configure Database Agents**.

Procédure

1. Ouvrez la fenêtre **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez sur la colonne **Tâche/sous-système**, puis cliquez avec le bouton droit de la souris sur **Modèle**, puis sur **Configurer avec les valeurs par défaut**.
3. Dans la fenêtre **Configure Database Agents**, sélectionnez le serveur de base de données à surveiller dans la liste **Database Servers Available**, puis cliquez sur la flèche gauche pour déplacer le serveur vers la liste **Server to Monitor**.
4. Dans la fenêtre **Propriétés du serveur de base de données**, les valeurs des zones suivantes sont automatiquement indiquées :
   - nom de serveur
   - Database Version
   - Home Directory
   - Error Log File

   Les zones suivantes de la fenêtre **Propriétés du serveur de base de données** sont facultatives :
   - Windows Authentication
   - Support Long Lived Database Connections
   - Extended Parms
   - Monitor all Databases

- Day(s) Frequency
- Weekly Frequency
- Monthly Frequency
- Collection Start Time
- Table Detail Continuous Collection

Pour plus d'informations sur les paramètres de configuration de la fenêtre **Propriétés du serveur de base de données**, voir «Paramètres de configuration des propriétés du serveur de base de données», à la page 566.

5. Si vous ne sélectionnez pas la zone **Authentification Windows**, entrez votre ID utilisateur et votre mot de passe dans les zones **Login** et **Password** en utilisant uniquement des caractères ASCII.
6. Dans la zone **Extended Parms**, entrez le nom du jeu de données pour désactiver la collecte des données, puis cliquez sur **OK**.

   Par exemple :

   - Entrez `koqtbld` pour désactiver la collecte de données de l'ensemble de données Détails des tables.
   - Entrez `koqdbd` pour désactiver la collecte de données de l'ensemble de données Détail des bases de données.
   - Entrez `koqtbld,koqdbd` pour désactiver la collecte de données des ensembles de données Détails des tables et Détails des bases de données.
7. Si vous ne cochez pas la case **Surveillance de toutes les bases de données**, indiquez la liste de bases de données pour lesquelles vous souhaitez activer ou désactiver la surveillance dans la zone de la zone de groupe **Bases de données**.

   A faire : Si vous cochez la case **Monitor All Databases** et spécifiez les bases de données dans la zone de groupe **Bases de données**, le réglage de la case à cocher **Monitor All Databases** est prioritaire.
8. Définissez la fréquence de la collecte pour l'ensemble de données Détails des tables MS SQL. Les valeurs possibles sont quotidienne, hebdomadaire ou mensuelle.
9. Cochez la case **Table Detail Continuous Collection** pour activer la collecte continue de l'ensemble de données MS SQL Table Detail. Si vous cochez la case **Table Detail Continuous Collection**, entrez une valeur dans la zone **Interval Between Two Continuous Collection (in minutes)**.
10. Dans la fenêtre **Configure Database Agents**, cliquez sur **OK**, puis démarrez l'agent.

Que faire ensuite
Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Paramètres de configuration des propriétés du serveur de base de données
Dans la fenêtre des **propriétés du serveur de base de données**, vous pouvez configurer des propriétés du serveur de base de données, telles que le nom du serveur, la version de base de données et le répertoire de base.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de la fenêtre des **propriétés du serveur de base de données**.

*Tableau 182. Noms et descriptions des paramètres de configuration de la fenêtre des **propriétés du serveur de base de données***

Nom du paramètre	Description	Zone obligatoire	Exemples
nom de serveur	Nom de l'instance Microsoft SQL Server à surveiller. Utilisez MSSQLSERVER comme nom d'instance de l'instance par défaut. Le nom doit être suffisamment court pour répondre aux exigences des noms de système géré qui admettent de 2 à 32 caractères.	Oui	Si l'instance Microsoft SQL Server surveillée est l'instance Microsoft SQL Server par défaut, entrez `MSSQLSERVER` dans cette zone. Si l'instance Microsoft SQL Server surveillée est une instance nommée (où le nom de l'instance est `mysqlserver` et le nom d'hôte est `popcorn`), entrez `mysqlserver` dans cette zone.
Connexion	ID utilisateur Microsoft SQL Server à utiliser pour se connecter à Microsoft SQL Server. L'ID utilisateur n'est obligatoire que si le paramètre **`Windows Authentication`** est défini sur `False`. Utilisez uniquement des caractères ASCII pour l'ID utilisateur. Lorsque vous configurez l'agent Microsoft SQL Server en indiquant un ID de connexion dans la zone **Connexion**, l'agent utilise cet ID pour se connecter à Microsoft SQL Server. **Important :** Si, lors de la configuration de l'agent, vous cochez la case **Authentification Windows** et que vous indiquez un ID de connexion dans la zone **Connexion**, l'agent donne la préférence à l'authentification Windows.	Non	
mot de passe	Mot de passe associé à l'ID utilisateur Microsoft SQL Server. Le mot de passe n'est obligatoire que si le paramètre **`Windows Authentication`** est défini sur `False`. Utilisez uniquement des caractères ASCII pour le mot de passe.	Non	

*Tableau 182. Noms et descriptions des paramètres de configuration de la fenêtre des **propriétés du serveur de base de données** (suite)*

Nom du paramètre	Description	Zone obligatoire	Exemples
Version de la base de données	Version de l'instance SQL Server.	Oui	Les versions de base de données de l'instance SQL Server sont les suivantes : • Microsoft SQL Server 2014 - 12.0.2000.8 • Microsoft SQL Server 2012 - 11.0.2100.60 • Microsoft SQL Server 2008 R2 - 10.50.1600.1 • Microsoft SQL Server 2008 - 10.0.1600.22 • Microsoft SQL Server 2005 - 9.0.1399.06
Répertoire de base	Répertoire d'installation de SQL Server.	Oui	Le chemin d'accès par défaut au répertoire de base pour l'instance Microsoft SQL Server 2005 est `C:\Program Files\Microsoft SQL Server\MSSQL`. Une instance Microsoft SQL Server 2005 nommée dispose d'un chemin d'accès par défaut au répertoire de base au format `C:\Program Files\Microsoft SQL Server\MSSQL$`*`nom_instance`*, où *nom_instance* est le nom de l'instance Microsoft SQL Server.

*Tableau 182. Noms et descriptions des paramètres de configuration de la fenêtre des **propriétés du serveur de base de données** (suite)*

Nom du paramètre	Description	Zone obligatoire	Exemples
Fichier journal des erreurs	Emplacement et nom qualifiés complets du journal des erreurs SQL Server.	Oui	Le chemin d'accès par défaut au journal des erreurs de l'instance Microsoft SQL Server 2005 par défaut est `C:\Program Files\Microsoft SQL Server\MSSQL\LOG\ERRORLOG`. Une instance Microsoft SQL Server 2005 nommée dispose d'un chemin d'accès par défaut au journal des erreurs au format `C:\Program Files\Microsoft SQL Server\MSSQL$`*`nom_instance`*`\LOG\ERRORLOG`, où *nom_instance* est le nom de l'instance Microsoft SQL Server.

*Tableau 182. Noms et descriptions des paramètres de configuration de la fenêtre des **propriétés du serveur de base de données** (suite)*

Nom du paramètre	Description	Zone obligatoire	Exemples
Authentification Windows	L'authentification Windows est un compte Windows sous lequel les services d'agent sont configurés. Il s'agit de l'option de configuration par défaut. Si vous cochez la case **Windows**, les informations d'identification Windows sont utilisées pour l'authentification. Lorsque l'agent Microsoft SQL Server est configuré avec l'authentification Windows, le **Compte système local** ou **Ce compte** est utilisé par les services d'agent pour la connexion à Microsoft SQL Server. • Si les services d'agent sont configurés pour utiliser le **Compte système local** pour se connecter, alors l'agent utilise l'ID utilisateur NT AUTHORITY\SYSTEM pour accéder à Microsoft SQL Server. • Si les services d'agent sont configurés pour utiliser **Ce compte** pour se connecter, alors l'agent utilise l'ID utilisateur respectif pour accéder à Microsoft SQL Server. **A faire :** Si vous ne sélectionnez pas la case à cocher **Authentification Windows**, vous devez indiquer des valeurs pour les paramètres **Connexion** et **Mot de passe**. Si vous n'indiquez pas ces paramètres et que vous cliquez sur **OK** dans la fenêtre **Propriétés du serveur de base de données**, un message d'erreur s'affiche dans une fenêtre en incrustation et la configuration d'agent n'aboutit pas. **Important :** Si, lors de la configuration de l'agent, vous cochez la case **Authentification Windows** et que vous indiquez un ID de connexion dans la zone **Connexion**, l'agent donne la préférence à l'authentification Windows.	Non	
Prise en charge des connexions de base de données de longue durée	Active ou désactive les connexions de base de données de longue durée. Les connexions de base de données de longue durée ne sont pas utilisées dans les ensembles de données suivants : • Texte MS SQL • Détail des groupes de fichiers MS SQL • Récapitulatif Microsoft SQL Server	Non	

*Tableau 182. Noms et descriptions des paramètres de configuration de la fenêtre des **propriétés du serveur de base de données** (suite)*

Nom du paramètre	Description	Zone obligatoire	Exemples
Paramètres étendus	Désactive la collecte de données de n'importe quel groupe d'attributs.	Non	Par exemple : Pour désactiver la collecte de données pour l'ensemble de données Détail des tables, entrez `koqtbld` dans la zone **Extended Parms**. Pour désactiver la collecte de données pour l'ensemble de données Détail des bases de données, entrez `koqdbd` dans la zone **Extended Parms**. Pour désactiver la collecte de données pour les ensembles de données Table Details et Database Details, entrez `koqtbld,koqdbd` dans la zone **Extended Parms**.

*Tableau 182. Noms et descriptions des paramètres de configuration de la fenêtre des **propriétés du serveur de base de données** (suite)*

Nom du paramètre	Description	Zone obligatoire	Exemples

Base de données	Pour sélectionner les bases de données à surveiller, indiquez une valeur pour ce paramètre. Pour activer la surveillance de toutes les bases de données disponibles dans l'instance de serveur SQL, cochez la case **Surveillance de toutes les bases de données** dans le groupe **Bases de données**. La case **Surveillance de toutes les bases de données** est sélectionnée par défaut.
	
	Pour activer ou désactiver la surveillance de bases de données spécifiques, désélectionnez la case **Surveillance de toutes les bases de données**.
	• Pour surveiller des bases de données spécifiques, sélectionnez **Include** dans la liste, puis indiquez les noms des bases de données dans la zone de texte en regard de la liste.
	• Pour exclure des bases de données spécifiques de la surveillance, sélectionnez **Exclude** dans la liste, puis indiquez les noms des bases de données dans la zone de texte en regard de la liste.
	
	Utilisez cette zone de texte pour filtrer les bases de données que vous voulez surveiller.
	
	Pour indiquer le filtre de bases de données, vous devez d'abord sélectionner un séparateur. Un séparateur est un caractère qui distingue un nom de base de données ou une expression de base de données d'un autre nom de base de données ou d'une autre expression de base de données.
	
	Lorsque vous sélectionnez un séparateur, vérifiez que les noms de base de données et l'expression de base de données ne contiennent pas le caractère que vous choisissez comme séparateur. Vous ne devez pas utiliser les caractères génériques généralement utilisés dans la requête T-SQL (par exemple : %, _, [ ], ^, -) s'ils sont utilisés dans les noms de base de données ou dans l'expression de base de données.
	
	Lorsque vous spécifiez un filtre de base de données :
	• Les noms de base de données doivent commencer par un séparateur.
	• L'expression de base de données doit commencer par deux séparateurs.
	
	L'expression de base de données est une expression valide qui peut être utilisée dans la section LIKE de la requête T-SQL. Toutefois, la clause T-SQL ESCAPE n'est pas autorisée lorsque vous spécifiez l'expression de base de données. Les jeux de données suivants sont affectés par le filtre de base de données :
		Non	Exemples de filtres :
			
			Cas 1 : % d'utilisation
			
			Exemple :
			
			`@@%m%`
			
			Résultat : toutes les bases de données ayant le caractère m dans leur nom sont filtrées.
			
			Cas 2 : utilisation de _
			
			Exemple :
			
			`@@____`
			
			Résultat : toutes les bases de données d'une longueur de quatre caractères sont filtrées.
			
			Cas 3 : utilisation de []
			
			Exemple :
			
			`@@[m]___`
			
			Résultat : toutes les bases de données d'une longueur de quatre caractères et dont le nom commence par le caractère m sont filtrées.
			
			Cas 4 : utilisation de [^]
			
			Exemple :
			
			`@@[^m]%`
			
			Résultat : toutes les bases de données (quelle que soit leur longueur) exceptées celles dont le nom commence par le caractère *m* sont filtrées.

*Tableau 182. Noms et descriptions des paramètres de configuration de la fenêtre des **propriétés du serveur de base de données** (suite)*

Nom du paramètre	Description	Zone obligatoire	Exemples

Database (suite)	**A faire :**
	• Si vous ne cochez pas la case **Surveillance de toutes les bases de données**, vous devez indiquer la liste de bases de données pour lesquelles vous souhaitez activer ou désactiver la surveillance dans la zone de texte figurant dans le groupe **Bases de données**. Si vous cliquez sur **OK** dans la fenêtre **Propriétés du serveur de base de données** sans cocher la case **Surveillance de toutes les bases de données** et indiquer la liste de bases de données, un message d'erreur s'affiche dans une fenêtre en incrustation et la configuration d'agent n'aboutit pas.
	• Si vous cochez la case **Surveillance de toutes les bases de données** et indiquez les bases de données à surveiller dans la zone de texte située dans le groupe **Bases de données**, la priorité est donnée à la valeur de la case **Surveillance de toutes les bases de données**. La liste de bases de données indiquée dans la zone de texte est ignorée.
			Cas 5 : entrée erronée
			Exemple :
			`@%m%`
			Résultat : aucune des bases de données n'est filtrée.
			Cas 6 : option par défaut
			Exemple : zone laissée vide (aucune requête n'est saisie)
			Résultat : toutes les bases de données sont filtrées.
			Cas 7 : modèles mixtes
			Exemple :
			`@@[m-t]_d%`
			Résultat : toutes les bases de données (quelle que soit leur longueur) dont le noms commence par le caractères m, n, o, p, q, r, s, t, suivi d'un caractère quelconque, avec le caractère d en troisième position, sont filtrées.

Day(s) Frequency	Utilisez cette fonction pour définir la fréquence de collecte des données des attributs Détail des tables. Les valeurs sont comprises entre zéro et 31.	Non	
Weekly Frequency	Utilisez cette fonction pour définir un jour particulier pour la collecte des données des attributs Détail des tables. Les valeurs sont comprises entre zéro et sept.	Non	
Monthly Frequency	Utilisez cette fonction pour définir la fréquence de collecte des données des attributs Détail des tables sur un jour donné du mois. Les valeurs possibles sont 1, 2, 3, etc.	Non	

*Tableau 182. Noms et descriptions des paramètres de configuration de la fenêtre des **propriétés du serveur de base de données** (suite)*

Nom du paramètre	Description	Zone obligatoire	Exemples
Collection Start Time	Heure de début de la collecte au format HH:MM. Les valeurs possibles pour les heures vont de zéro à 23. La valeur par défaut est zéro. Les valeurs possibles pour les minutes vont de zéro à 59. La valeur par défaut est zéro.	Non	
Table Detail Continuous Collection	Utilisez cette fonction pour collecter en arrière-plan de manière continue les données de détail des tables. La case **Table Detail Continuous Collection** est cochée par défaut.	Non	
Interval Between Two Continuous Collection (in min.)	Durée de l'intervalle entre deux collectes en minutes. L'intervalle minimum est de 3 minutes. Vous pouvez cocher la case **Interval Between Two Continuous Collection (in min.)** ou utiliser la planification pour spécifier la collecte continue de l'ensemble de données Détail des tables. Si vous cochez la case **Interval Between Two Continuous Collection (in min.)**, vous devez spécifiez l'intervalle de temps pour la collection. Si vous utilisez la planification pour spécifier la collecte de l'ensemble de données Détail des tables, l'intervalle de temps minimal est de 1 jour. L'intervalle par défaut entre deux collectes continues est de 3 minutes.	Non	

L'agent collecte les données à l'intervalle de temps où la collecte de données se produit fréquemment. Par exemple, si vous spécifiez toutes les fréquences (quotidienne, hebdomadaire et mensuelle) pour la collecte des données, l'agent démarre la collecte des données en tenant compte des critères suivants :

- Si la fréquence quotidienne est ≤ 7, les paramètres de fréquence quotidienne sont sélectionnés et les paramètres de fréquence hebdomadaire et mensuelle sont ignorés.
- Si la fréquence quotidienne est > 7, les paramètres de fréquence hebdomadaire sont sélectionnés et les paramètres de fréquence quotidienne et mensuelle sont ignorés.

A faire : Si la case **Table Detail Continuous Collection** est cochée, l'agent collecte les données à l'intervalle défini par la zone **Interval Between Two Continuous Collection (in min.)** et non selon les fréquences quotidienne, hebdomadaire ou mensuelle.

Configuration des variables d'environnement local sur les systèmes Windows
Vous pouvez configurer les variables d'environnement local pour modifier le comportement de agent Microsoft SQL Server.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **Agents IBM Monitoring** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, dans le menu **Actions**, cliquez sur **Avancé > Editer les variables**.

3. Dans la fenêtre Monitoring Agent for Microsoft SQL Server: **Override Local Variable Settings**, cliquez sur **Ajouter**.
4. Dans la fenêtre **Ajouter la substitution des paramètres d'environnement**, entrez la variable et la valeur correspondante.

   Remarque : Pour la liste complète des variables d'environnement configurables, voir «Variables d'environnement local», à la page 558.

Exécution en tant qu'utilisateur non-administrateur
Vous pouvez exécuter Monitoring Agent for Microsoft SQL Server en tant qu'utilisateur non-administrateur.

Pourquoi et quand exécuter cette tâche
L'agent Microsoft SQL Server peut être exécuté en tant qu'utilisateur non administrateur à partir du groupe Utilisateurs du domaine.

Procédure

1. Démarrez l'application Windows Utilisateurs et ordinateurs Active Directory et créez un utilisateur de domaine.
   - Vérifiez que le nouvel utilisateur fait bien partie du groupe *Utilisateurs du domaine*.
   - Vérifiez que le serveur SQL Server fait bien partie du groupe *Ordinateurs du domaine*.
2. Ajoutez l'utilisateur de domaine que vous venez de créer au groupe d'utilisateurs *Connexion à SQL Server*. L'utilisateur de domaine doit disposer soit des droits du rôle SQL Server **sysadmin** sur le serveur SQL Server, soit des droits indiqués dans https://www.ibm.com/support/knowledgecenter/SSMKFH/com.ibm.apmaas.doc/install/sql_config_agent_grant_permission_sqlserver.htm.
3. Connectez-vous au serveur SQL Server en tant qu'administrateur de domaine.
4. Accordez le droit de **modification** sur chaque unité à laquelle l'agent Microsoft SQL Server à accès. Pour propager les droits à tous les sous-répertoires, procédez comme suit :
   a) Allez dans **Poste de travail**.
   b) Cliquez avec le bouton droit de la souris sur l'**unité**.
   c) Cliquez sur l'onglet **Sécurité**.
   d) Ajoutez le nouvel utilisateur.
   e) Accordez-lui le droit de **modification**.
   f) Cliquez sur **OK**. L'application des droits sur tous les sous-répertoires prend quelques minutes.
5. A partir du registre Windows, accordez un accès en lecture à `HKEY_LOCAL_MACHINE` et propagez les paramètres. Pour propager les paramètres, procédez comme suit :
   a) Cliquez avec le bouton droit de la souris sur le répertoire `HKEY_LOCAL_MACHINE` et sélectionnez **Droits**.
   b) Ajoutez le nouvel utilisateur.
   c) Sélectionnez le nouvel utilisateur.
   d) Cochez la case **Autoriser la lecture**.
   e) Cliquez sur **OK**. La propagation des paramètres à toute l'arborescence de `HKEY_LOCAL_MACHINE` prend quelques minutes.
6. A partir du Registre Windows, accordez des droits sur le Registre spécifiques à l'agent en fonction de la liste suivante.
   - Si vous avez installé un agent 32 bits sur un système d'exploitation 32 bits, accordez un accès complet au répertoire `KEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring` et propagez les paramètres.

- Si vous avez installé un agent 32 bits sur un système d'exploitation 64 bits, accordez un accès complet au répertoire HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Candle et propagez les paramètres.
- Si vous avez installé un agent 64 bits sur un système d'exploitation 64 bits, accordez un accès complet au répertoire KEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring et propagez les paramètres.

Procédez comme suit pour propager les paramètres :

a) Cliquez avec le bouton droit de la souris sur le répertoire pour lequel vous disposez d'un accès complet et sélectionnez **Droits**.

b) Ajoutez le nouvel utilisateur.

c) Sélectionnez l'utilisateur qui vient d'être créé.

d) Cochez la case **Autoriser le plein contrôle**.

e) Cliquez sur **OK**. La propagation des paramètres à toute l'arborescence de KEY_LOCAL_MACHINE \SOFTWARE\IBMMonitoring prend quelques minutes.

7. Ajoutez un nouvel utilisateur de domaine au groupe **Utilisateurs de l'Analyseur de performances**.
8. Vérifiez que le groupe Utilisateurs de domaine fait partie du groupe *Utilisateurs*.
9. Accordez les droits suivants sur le répertoire Windows pour une exécution en tant qu'utilisateur non-administrateur :
   - Si un agent 32 bits est installé sur un système d'exploitation 32 bits, accordez un accès en lecture et en écriture au répertoire unité_installation_SE:\Windows\system32
   - Si un agent 32 bits est installé sur un système d'exploitation 64 bits, accordez un accès en lecture et en écriture au répertoire unité_installation_SE:\Windows\SysWOW64

   Remarque : Des droits sur le répertoire Windows ne sont pas nécessaires pour Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 et Windows Server 2016.
10. Accordez le droit de **modification** sur le fichier de données SQL Server et sur le fichier journal :
    - Le chemin par défaut du fichier de données SQL Server est *rép_principal_SQLServer*\DATA, où *rép_principal_SQLServer* représente le répertoire principal de l'instance SQL Server. Par exemple, si le répertoire principal de l'instance SQL Server est C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL, le chemin du fichier de données sera C:\Program Files \Microsoft SQL Server\MSSQL.1\MSSQL\DATA.
    - Le chemin par défaut du fichier journal SQL Server est *rép_principal_SQLServer*\LOG, où *rép_principal_SQLServer* représente le répertoire principal de l'instance SQL Server. Par exemple, si le répertoire principal de l'instance SQL Server est C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL, le chemin du fichier journal sera C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG.
11. Accordez un accès complet au répertoire rép_principal_candle. Le chemin par défaut est C:\IBM\ITM.
12. Appliquez les droits de sécurité locaux (voir «Droits de la stratégie de sécurité locale», à la page 577).
13. Redémarrez SQL Server pour vous assurer que les droits de sécurité locaux sont bien appliqués.
14. Modifiez les paramètres de connexion de l'utilisateur non-administrateur pour les services d'agent SQL Server. Pour ce faire, procédez comme suit :

    a) Cliquez sur **Démarrer > Outils d'administration > Services**.

    b) Cliquez avec le bouton droit de la souris sur le service **Monitoring Agent for SQL Server *nom_instance***, puis cliquez sur **Propriétés**. La fenêtre **Propriétés de Service SQL** s'affiche.

    c) Cliquez sur l'onglet **Connexion**.

    d) Cliquez sur **Ce compte** et entrez le nom de l'utilisateur.

e) Dans les zones **Mot de passe** et **Confirmer le mot de passe**, entrez le mot de passe et cliquez sur **OK**.

f) Répétez les étapes b à e pour l'**Agent de surveillance du collecteur SQL Server *nom_instance***, où *nom_instance* représente le nom d'instance de Microsoft SQL Server.

Droits de la stratégie de sécurité locale

La stratégie de sécurité locale administre le système et ses règles de sécurité. Elle joue un rôle important dans le maintien de la sécurité de l'agent et du système sur lequel l'agent est installé. Cette stratégie fonctionne en donnant des droits et des droits aux utilisateurs. Dans le cas de l'agent Microsoft SQL Server, assurez-vous que l'utilisateur dispose les droits suivants afin de respecter les règles de la stratégie de sécurité locale.

Droit Ouvrir une session en tant que service

Pourquoi et quand exécuter cette tâche

Pour accorder le droit Ouvrir une session en tant que service, procédez comme suit.

Procédure

1. Cliquez sur **Démarrer > Outils d'administration > Stratégie de sécurité locale**. La fenêtre **Stratégie de sécurité locale** s'affiche.
2. Cliquez sur **Stratégies locales** pour développer la liste.
3. Cliquez sur **Attribution des droits utilisateur**. La liste des droits utilisateur s'affiche.
4. Cliquez deux fois sur la stratégie **Ouvrir une session en tant que service**. La fenêtre **Propriétés de Ouvrir une session en tant que service** apparaît.
5. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre **Sélectionner des utilisateurs ou des groupes** apparaît.
6. Dans la zone **Entrer les noms d'objet à sélectionner**, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
7. Cliquez sur **OK**.

Droit Déboguer les programmes

Pourquoi et quand exécuter cette tâche

Pour accorder le droit Déboguer les programmes, procédez comme suit sur l'agent Microsoft SQL Server.

Procédure

1. Cliquez sur **Démarrer > Outils d'administration > Stratégie de sécurité locale**. La fenêtre **Stratégie de sécurité locale** s'affiche.
2. Cliquez sur **Stratégies locales** pour développer la liste.
3. Cliquez sur **Attribution des droits utilisateur**. La liste des droits utilisateur s'affiche.
4. Cliquez deux fois sur la stratégie **Déboguer les programmes**. La fenêtre **Propriétés de Déboguer les programmes** apparaît.
5. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre **Sélectionner des utilisateurs ou des groupes** apparaît.
6. Dans la zone **Entrez les noms des objets à sélectionner**, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
7. Cliquez sur **OK**.

Simuler les droits d'un client après l'authentification

Pourquoi et quand exécuter cette tâche

Pour accorder le droit Simuler les droits d'un client après l'authentification, suivez la procédure ci-dessous dans l'agent Microsoft SQL Server.

Procédure

1. Cliquez sur **Démarrer > Outils d'administration > Stratégie de sécurité locale**. La fenêtre **Stratégie de sécurité locale** s'affiche.
2. Cliquez sur **Stratégies locales** pour développer la liste.
3. Cliquez sur **Attribution des droits utilisateur**. La liste des droits utilisateur s'affiche.
4. Cliquez deux fois sur la stratégie **Simuler les droits d'un client après l'authentification**. La fenêtre **Propriétés de Simuler les droits d'un client après l'authentification** apparaît.
5. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre **Sélectionner des utilisateurs ou des groupes** apparaît.
6. Dans la zone **Entrer les noms d'objet à sélectionner**, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
7. Cliquez sur **OK**.

Configuration de l'agent sur des systèmes Linux

Pour configurer l'agent sur des systèmes d'exploitation Linux, vous pouvez exécuter le script ou répondre à des invites.

Avant de commencer

Pour pouvoir configurer l'agent, veillez à exécuter les tâches suivantes :

- Passez en revue les variables d'environnement local

Pourquoi et quand exécuter cette tâche

L'agent Microsoft SQL Server est un agent multi-instance ; vous devez configurer et démarrer chaque instance d'agent manuellement.

Procédure

1. Dans la ligne de commande, modifiez le chemin d'accès au répertoire d'installation de l'agent.
   Exemple :
   ```
   cd /opt/ibm/apm/agent/bin
   ```
2. Exécutez la commande suivante, où *nom_instance* correspond au nom que vous souhaitez attribuer à l'instance :
   ```
   ./mssql-agent.sh config nom_instance
   ```
3. Lorsque l'invite de commande affiche le message suivant, tapez 1 et entrez :
   `Edit ‘Monitoring Agent for MSSQL setting? [1=Yes, 2=No]`
4. A l'invite, indiquez les valeurs des paramètres de configuration.
   Pour plus d'informations sur les paramètres de configuration, voir Paramètres de configuration de l'agent.
5. Exécutez la commande suivante pour démarrer l'agent :
   ```
   ./mssql-agent.sh start nom_instance
   ```
6. Exécutez la commande suivante pour arrêter l'agent :

```
./mssql-agent.sh stop nom_instance
```

Configuration des variables d'environnement local sur les systèmes Linux
Vous pouvez configurer les variables d'environnement local pour modifier le comportement de l'agent Microsoft SQL Server sur les systèmes Linux.

Procédure

1. Lancez un terminal ou le gestionnaire de fichiers système et accédez au répertoire d'installation de l'agent :
   Exemple :
   ```
   /opt/ibm/apm/agent
   ```
2. Exécutez la commande suivante pour arrêter l'agent :
   ```
   ./mssql-agent.sh stop nom_instance
   ```
   Où *nom_instance* est le nom d'instance de l'agent.
3. Ouvrez le fichier `.oq.environment` qui figure dans le répertoire config suivant :
   Exemple :
   ```
   rép_install/config
   ```
   Où *rép_install* représente le répertoire d'installation de l'agent.
4. Ajoutez les variables d'environnement requises à la fin du fichier `.oq.environment` au format paire nom-valeur.
   `export VARIABLE_NAME=VARIABLE_VALUE`
   Exemple :
   ```
   export KOQ_ODBC_DRIVER=ODBC Driver 17 for SQL Server
   ```
   Remarque :
   - Pour la liste complète des variables d'environnement configurables, voir «Variables d'environnement local», à la page 558.
   - Les variables personnalisées ajoutées ne sont pas conservées après la mise à niveau de l'agent.
5. Sauvegardez le fichier.
6. Démarrez l'agent à partir du répertoire d'installation de l'agent :
   ```
   cd /opt/ibm/apm/agent/bin
   ```
   ```
   ./mssql-agent.sh start nom_instance
   ```

Configuration de l'agent à l'aide du fichier de réponses silencieux

Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'agent ou plusieurs instances de l'agent.

Avant de commencer

Pour configurer plusieurs instances de l'agent, vérifiez que les détails de configuration de toutes les instances de l'agent sont spécifiés dans le fichier de réponses silencieux.

Pourquoi et quand exécuter cette tâche
Exécutez le script de configuration pour modifier les paramètres de configuration. Vous pouvez modifier le fichier de réponses silencieux avant d'exécuter le script de configuration.

Procédure

Pour configurer l'agent, procédez comme suit :

1. Lancez un éditeur de texte et ouvrez le fichier de réponses silencieux qui est disponible à l'emplacement suivant :
   - Windows *rép_install*\samples/mssql_silent_config.txt
   - Linux *rép_install*/samples/mssql_silent_config.txt

   Où *rép_install* représente le répertoire d'installation de l'agent.

   Exemple :
   - Windows C:\IBM\APM\samples\mssql_silent_config.txt
   - Linux /opt/ibm/apm/agent/samples/mssql_silent_config.txt

   Remarque : Pour plus d'informations sur les paramètres de configuration de l'agent, voir «Paramètres de configuration de l'agent », à la page 564.
2. Lancez une invite de commande et accédez au répertoire suivant :
   - Windows
     ```
     cd rép_install\bin
     ```
   - Linux
     ```
     cd rép_install/bin
     ```
3. Exécutez la commande suivante :
   - Windows
     ```
     mssql-agent.bat config rép_install\samples\mssql_silent_config.txt
     ```
   - Linux
     ```
     mssql-agent.sh config  nom_instance rép_install/samples/mssql_silent_config.txt
     ```
4. Démarrez l'agent.
   - Windows Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur l'instance d'agent que vous avez créée et cliquez sur Démarrer.
   - Linux Exécutez la commande suivante :
     ```
     cd /opt/ibm/apm/agent/bin
     ```
     ```
     ./mssql-agent.sh start nom_instance
     ```

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Exécution de l'agent dans un environnement cluster

Windows Vous pouvez configurer l'agent Microsoft SQL Server dans un environnement cluster. Plusieurs instances de Microsoft SQL Server et d'agent Microsoft SQL Server peuvent s'exécuter sur un noeud unique.

Après avoir installé et configuré l'agent Microsoft SQL Server, procédez comme suit pour exécuter l'agent dans un environnement cluster :

- Ajoutez des variables d'environnement
- Modifiez le type de démarrage du service d'agent et du service de collecteur
- Ajoutez l'agent et le collecteur à l'environnement cluster

Vous pouvez configurer un environnement en cluster pour les versions suivantes de Microsoft SQL Server :

- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016

Important : Sur les systèmes Windows, l'agent doit être installé dans le même répertoire que l'agent de système d'exploitation. Installez l'agent sur le disque système de noeuds de chaque noeud de cluster.

Ajout de variables d'environnement

Vous devez configurer les variables d'environnement qui sont utilisées par les agents qui sont installés sur chaque noeud de cluster.

Pourquoi et quand exécuter cette tâche

Vous devez définir les variables d'environnement suivantes :

- *CTIRA_HOSTNAME* : Cette variable est utilisée pour configurer chaque instance de l'agent Microsoft SQL Server. La valeur de cette variable est limitée à 31 caractères et est commune à tous les agents de surveillance. Définissez la valeur de cette variable sur le nom de cluster pour accéder à tous les agents de surveillance de ce cluster dans Tableau de bord d'Application Performance.
- *CTIRA_NODETYPE* : Cette variable est utilisée pour identifier l'agent. Par défaut, la valeur de cette variable est définie sur **MSS** pour l'agent Microsoft SQL Server.
- *CTIRA_SUBSYSTEMID* : La variable est utilisée pour distinguer plusieurs instances de l'agent Microsoft SQL Server. Par défaut, la valeur de cette variable est définie sur **Microsoft SQL Virtual Server** pour l'agent Microsoft SQL Server.
- *COLL_HOME* : Cette variable est utilisée pour collecter des données et pour stocker des fichiers journaux pour les groupes d'attributs qui utilisent des fichiers de configuration à un emplacement partagé. Définissez la valeur de la variable sur *X*:\shared-location, où *X* est une unité partagée accessible aux noeuds de cluster. Par exemple, définissez la valeur pour la variable *COLL_HOME* quand vous définissez les paramètres de configuration pour le groupe d'attributs Détails des tables MS SQL ou le groupe d'attributs Détails des événements d'erreur MS SQL.
- *CTIRA_HIST_DIR* : Cette variable est utilisée pour spécifier le chemin vers le répertoire de disque partagé. Si l'historique de l'agent Microsoft SQL Server est configuré pour être stocké sur l'agent de surveillance, chaque instance de l'agent doit être configurée avec une variable *CTIRA_HIST_DIR* commune qui fait référence au répertoire de disque partagé.

  A faire : Si l'historique est stocké sur le serveur Cloud APM, vous n'avez pas besoin d'indiquer une valeur pour la variable *CTIRA_HIST_DIR*. Le fait de stocker l'historique sur le serveur Cloud APM augmente la charge sur ce serveur.

Pour ajouter ces variables, consultez les étapes décrites dans «Configuration des variables d'environnement local sur les systèmes Windows», à la page 574.

Que faire ensuite
Changez le type de démarrage du service d'agent et du service de collecteur sur **Manuel** en suivant les étapes décrites dans «Modification du type de démarrage du service d'agent et du service de collecteur», à la page 582.

Modification du type de démarrage du service d'agent et du service de collecteur
Par défaut, le type de démarrage du service d'agent et du service de collecteur est **Automatique**. Changez le type de démarrage du service d'agent et du service de collecteur sur **Manuel** de sorte que la ressource de cluster puisse contrôler le démarrage et l'arrêt de l'agent de surveillance

Procédure

Pour modifier le type de démarrage du service d'agent, effectuez les étapes suivantes :

1. Cliquez sur **Démarrer** > **Exécuter**, puis entrez la commande `services.msc` et cliquez sur **OK**.
2. Cliquez avec le bouton droit de la souris sur l'agent, puis cliquez sur **Propriétés**.
3. Dans la liste **Type de démarrage** de la fenêtre de **propriétés de Monitoring Agent for Microsoft SQL Server**, sélectionnez **Manuel**, cliquez sur **Appliquer** puis sur **OK**.

Que faire ensuite

- Employez la même procédure pour changer le type de démarrage du service de collecteur en **Manuel**.
- Ajoutez l'agent et le collecteur à l'environnement cluster en suivant les étapes décrites dans «Ajout de l'agent et du collecteur à l'environnement cluster », à la page 582.

Ajout de l'agent et du collecteur à l'environnement cluster
Vous devez ajouter l'agent et le collecteur à l'environnement cluster.

Procédure

1. Cliquez sur **Démarrer > Panneau de configuration > Outils d'administration > Gestion du cluster de basculement**.
2. Développez **Gestion du cluster de basculement**.
3. Développez **Services et applications** et cliquez avec le bouton droit de la souris sur l'instance SQL à configurer.
4. Cliquez sur **Ajouter une ressource > Service générique**. L'assistant Nouvelle ressource s'affiche.
5. Sur la page de sélection du service, sélectionnez le nom du service, puis cliquez sur **Suivant**.

   Exemple de noms de services Windows :

   - `Monitoring Agent for Microsoft SQL Server : SQLTEST#INSTANCE1`
   - `Monitoring Agent for Microsoft SQL Server : Collector SQLTEST#INSTANCE1`
   - `Monitoring Agent for Microsoft SQL Server : SQLTEST2#INSTANCE2`
   - `Monitoring Agent for Microsoft SQL Server : Collector SQLTEST2#INSTANCE2`
6. Sur la page de confirmation, contrôlez les détails, puis cliquez sur **Suivant**.
7. Dans la page Récapitulatif, cliquez sur **Terminer**. Le agent Microsoft SQL Server est maintenant ajouté.

   A faire : Utilisez les mêmes étapes pour ajouter le collecteur à l'environnement cluster.
8. Pour remettre l'agent en ligne, cliquez avec le bouton droit de la souris sur l'agent, puis cliquez sur l'option permettant de **mettre cette ressource en ligne**.
9. Pour remettre le collecteur en ligne, cliquez avec le bouton droit de la souris sur le collecteur, puis cliquez sur l'option permettant de **mettre cette ressource en ligne**.

Résultats
L'agent Microsoft SQL Server est dorénavant en cours d'exécution dans un environnement cluster.

A faire : Si vous voulez configurer l'agent de nouveau, vous devez d'abord mettre l'agent et le collecteur hors ligne, ou éditer les variables d'agent sur le noeud sur lequel ils s'exécutent. Une fois que vous avez terminé la configuration d'agent, remettez l'agent et le collecteur en ligne.

Configuration de l'agent à l'aide de l'utilitaire Cluster

Windows L'utilitaire cluster vous permet d'ajouter plusieurs instances d'agent Microsoft SQL Server à un groupe de clusters dans un environnement cluster.

L'utilitaire Cluster ajoute automatiquement le service d'agent et le service de collecteur de chaque instance d'agent Microsoft SQL Server en tant que ressource de service générique au groupe de clusters. L'utilitaire cluster vous permet de réaliser les tâches suivantes :

- Ajout d'une instance d'agent SQL Server au cluster
- Mise à jour d'une instance existante d'agent SQL Server dans un cluster
- Suppression d'une instance d'agent SQL Server à partir d'un cluster

Prérequis pour l'utilisation de l'utilitaire Cluster
Vous devez vous assurer que votre environnement système satisfait aux prérequis pour l'exécution de l'utilitaire Cluster.

Assurez-vous que les prérequis suivants sont respectés :

- Exécutez l'utilitaire Cluster sur un ordinateur disposant d'au moins un groupe dans l'environnement cluster.
- Démarrez le service de registre distant pour tous les noeuds dans la grappe.
- Vous devez avoir l'autorisation de gestionnaire de grappes pour accéder à l'utilitaire Cluster.
- Le nom de service de l'agent et du collecteur doit être identique sur tous les noeuds de cluster.

  Par exemple, si le nom de service de l'agent est Monitoring Agent for Microsoft SQL Server : SQLTEST#INSTANCE1 et que le nom du collecteur est Monitoring Agent for Microsoft SQL Server : Collecteur SQLTEST#INSTANCE1, le même nom de service doit figurer sur tous les noeuds du cluster.

Ajout d'une instance d'agent Microsoft SQL Server au cluster
L'utilitaire cluster vous permet d'ajouter une instance d'agent Microsoft SQL Server à un groupe de clusters dans un environnement cluster.

Procédure

1. Pour exécuter l'utilitaire, exécutez l'une des étapes suivantes :
   - Dans le cas d'un agent 64 bits, accédez au répertoire *rép_base_candle*\TMAITM6_x64.
   - Dans le cas d'un agent 32 bits, accédez au répertoire *rép_base_candle*\TMAITM6.
2. Cliquez deux fois sur KoqClusterUtility.exe pour lancer l'utilitaire Cluster.
3. Dans la zone SQL **Server Agent Instances Available**, sélectionnez une instance d'agent Microsoft SQL Server, puis cliquez sur **Add**.
4. Dans la fenêtre **Select cluster group name**, sélectionnez un groupe de clusters.

   Le groupe de clusters que vous sélectionnez doit être l'instance de SQL Server surveillée par l'agent Microsoft SQL Server.
5. Dans la fenêtre **Select Path for Shared Location**, naviguez jusqu'à l'emplacement de stockage des journaux de l'agent et du collecteur.

   Si vous n'avez pas sélectionné de chemin d'accès, l'emplacement CANDLEHOME/TMAITM6(_x64)/logs est sélectionné par défaut pour stocker les journaux d'agent et de collecteur.
6. Pour ajouter l'instance d'agent Microsoft SQL Server à l'environnement cluster, cliquez sur **OK**.

   Les journaux d'activité de l'utilitaire Cluster s'affichent dans le panneau **Historique**.

Mise à jour d'une instance d'agent Microsoft SQL Server existante dans un cluster
L'utilitaire cluster vous permet de mettre à jour l'emplacement de stockage des journaux de l'agent et du collecteur pour une instance de SQL Server dans un cluster.

Procédure

1. Pour mettre à jour une instance d'agent Microsoft SQL Server existante, accédez à la fenêtre **Cluster Utility**.
2. Dans la zone **SQL Server Agent Instances Configured**, sélectionnez une instance d'agent Microsoft SQL Server, puis cliquez sur **Update**.
3. Dans la fenêtre **Set Path for Shared Location**, naviguez jusqu'à l'emplacement de stockage des journaux de l'agent et du collecteur.

   Si vous ne sélectionnez pas le chemin d'accès, les journaux de l'agent et du collecteur sont stockés à l'emplacement qui a été défini lors de l'ajout de l'instance d'agent Microsoft SQL Server dans un cluster.
4. Cliquez sur **OK**.

   Les journaux d'activité de l'utilitaire Cluster s'affichent dans le panneau **Historique**.

Suppression d'une instance d'agent Microsoft SQL Server à partir d'un cluster
L'utilitaire cluster vous permet de supprimer une instance d'agent Microsoft SQL Server d'un groupe de clusters.

Procédure

1. Accédez à la fenêtre **Cluster Utility**.
2. Dans la zone **SQL Server Agent Instances Configured**, sélectionnez une instance d'agent Microsoft SQL Server, puis cliquez sur **Remove**.
3. Dans la boîte de dialogue **Please Confirm Action**, cliquez sur **Yes** pour supprimer l'instance d'agent Microsoft SQL Server du cluster.

   Les journaux d'activité de l'utilitaire Cluster s'affichent dans le panneau **Historique**.

Configuration de plusieurs classements pour le fichier ERRORLOG

L'agent Microsoft SQL Server version 06.31.17.00 (ou version ultérieure) pour Application Performance Management version 8.1.4.0.4 prend en charge les classements multiples dans le fichier ERRORLOG. Vous pouvez désormais configurer l'agent pour qu'il analyse plusieurs classements dans le fichier ERRORLOG pour le groupe d'attributs **Problem Detail**. Notez que les classements multiples dans le fichier ERRORLOG ne sont pas applicables pour le groupe d'attributs **Détails des événements d'erreur**.

Avant de commencer

Pour configurer plusieurs classements de l'agent, vérifiez que l'agent est installé.

Pourquoi et quand exécuter cette tâche
Le classement par défaut est Anglais. Pour les autres langues de SQL Server, l'agent analyse le fichier ERRORLOG en fonction des classements du fichier de configuration `koqErrConfig.ini`. Vous devez donc ajouter les classements utilisés dans le fichier `koqErrConfig.ini`.

Procédure

Pour configurer plusieurs classements pour l'agent, procédez comme suit :

1. Accédez au répertoire *répertoire_agent* de l'agent.

   Windows

   - Pour l'agent 64 bits, *répertoire_agent* correspond à *rép_base_agent*\TMAITM6_x64.
   - Pour l'agent 32 bits, *répertoire_agent* correspond à *rép_base_agent*\TMAITM6.

Linux

- Pour l'agent 64 bits, *répertoire_agent* correspond à *rép_base_agent*/TMAITM6_x64.

, *rép_base_agent* représentant le répertoire d'installation de l'agent.

2. Ouvrez le fichier koqErrConfig.ini de la configuration :
3. Accédez à la fin du fichier pour ajouter les nouveaux classements.

   Par exemple, pour activer le classement pour Français, ajoutez les paramètres de classement ci-après dans le format des paires **name-value** à la fin du fichier koqErrConfig.ini.

```
[French]
Error = Erreur :
Severity = Gravité :
State = Etat :
```

   Remarque : L'exemple de liste de classements est disponible dans *répertoire_agent* \koqErrConfigSample.ini.

   Où Windows

   - Pour l'agent 64 bits, *répertoire_agent* correspond à *rép_base_agent*\TMAITM6_x64.
   - Pour l'agent 32 bits, *répertoire_agent* correspond à *rép_base_agent*\TMAITM6.

   Linux

   - Pour l'agent 64 bits, *répertoire_agent* correspond à *rép_base_agent*/TMAITM6_x64.

   , *rép_base_agent* représentant le répertoire d'installation de l'agent.

   Si le classement cible n'est pas disponible dans le fichier koqErrConfigSample.ini, vous pouvez déterminer les valeurs des mots clés de classement dans le fichier ERRORLOG.
   Respectez le format de classement suivant lorsque vous configurez les paramètres de classement dans koqErrConfig.ini.

```
[nom_section]
Error = valeur_erreur
Severity = valeur_gravité
State = valeur_état
```

   Où

   - *nom_section* représente le nom du classement SQL Server. Vérifiez que le nom de classement est placé entre un crochet ouvrant "**[**" et un crochet fermant "**]**".
   - *valeur_erreur* représente le mot clé de l'erreur correspondante qui se trouve dans le fichier ERRORLOG de votre classement cible.
   - *valeur_gravité* représente le mot clé de la gravité correspondante qui se trouve dans le fichier ERRORLOG de votre classement cible.
   - *valeur_état* représente le mot clé de l'état correspondant qui se trouve dans le fichier ERRORLOG de votre classement cible.

   Important : Les valeurs de mot clé doivent être identiques à celles du fichier ERRORLOG, caractères spéciaux compris.
4. Sauvegardez le fichier koqErrConfig.ini de la configuration.

   Il n'est pas nécessaire de redémarrer l'agent.

   Si le fichier de configuration koqErrConfig.ini n'est pas disponible ou que le fichier de configuration koqErrConfig.ini est vide, le fichier ERRORLOG indique le classement par défaut sous forme de message d'erreur anglais dont le niveau de gravité est supérieur au niveau de gravité par défaut (s'il en existe un).

   Si le fichier de configuration koqErrConfig.ini est correctement configuré, le fichier ERRORLOG affiche les messages d'erreur correspondants dont le niveau de gravité est supérieur au niveau de gravité par défaut (s'il en existe un).

Le niveau de gravité par défaut est de 17.

Avertissement : Les modifications apportées au fichier `koqErrConfig.ini` ne sont pas conservées lors de la mise à niveau de l'agent ; vous devez effectuer une sauvegarde au préalable.

Que faire ensuite
Vérifiez le widget **Errorlog Alert** ou le groupe d'attributs **Problem Detail** sur le tableau de bord Application Performance Management qui résulte des paramètres de classement.

Configuration de la surveillance de MongoDB

Monitoring Agent for MongoDB a besoin d'un nom d'instance. Vous devez configurer et démarrer manuellement l'instance d'agent. L'Agent MongoDB prend en charge la surveillance locale et la surveillance à distance. Prenez connaissance des prérequis suivants pour configurer l'Agent MongoDB en vue de la surveillance locale et de la surveillance à distance.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent MongoDB.
- Assurez-vous que l'utilisateur qui configure l'Agent MongoDB dispose des rôles permettant de collecter les données pour l'ensemble des attributs.
  - Pour configurer l'agent sur la version 2.4 et la version 2.6 de la base de données MongoDB, les rôles clusterAdmin, readAnyDatabase et dbAdminAnyDatabase doivent être affectés à l'utilisateur
  - Pour configurer l'agent sur la version 3.x et 4.x de la base de données MongoDB, les rôles clusterMonitor, readAnyDatabase et dbAdminAnyDatabase doivent être attribués à l'utilisateur

  Pour en savoir plus sur les groupes d'attributs pour lesquels ces rôles utilisateur sont requis, voir Tableau 183, à la page 587.
- Utilisez un utilisateur existant ou créez-en un dans la base de données d'administration.

  Important : Avant de créer un utilisateur et de lui attribuer des rôles, vous devez vous connecter à la base de données MongoDB et changer la base de données en base de données d'administration. Si le processus mongod ou mongos s'exécute en mode d'authentification, entrez les données d'identification requises pour vous connecter à la base de données MongoDB.

  1. Exécutez la commande suivante pour vous connecter à la base de données MongoDB :

     `mongo IP:port`

     Où

     – *IP* est l'adresse IP du processus mongod ou mongos
     – *port* est le numéro de port du processus mongod ou mongos
  2. Changez la base de données en base de données d'administration :

     `use admin`
  3. Exécutez l'une des commandes suivantes pour ajouter un utilisateur dans la base de données d'administration MongoDB, puis affectez les rôles requis à l'utilisateur :
     – Pour la base de données MongoDB version 2.4, exécutez la commande suivante :

       ```
       db.addUser({ user: "nomutilisateur", pwd: "motdepasse", roles:
       [ 'clusterAdmin', 'readAnyDatabase', 'dbAdminAnyDatabase' ] })
       ```
     – Pour la base de données MongoDB version 2.6, exécutez la commande suivante :

```
db.createUser({user: "username", pwd: "password", roles:
[ 'clusterAdmin', 'readAnyDatabase', 'dbAdminAnyDatabase' ] })
```

– Pour la base de données MongoDB version 3.x et 4.x, exécutez la commande suivante :

```
db.createUser({user: "username", pwd: "password", roles:
[ 'clusterMonitor', 'readAnyDatabase', 'dbAdminAnyDatabase' ] })
```

4. Exécutez la commande suivante pour vérifier que l'utilisateur a été ajouté à la base de données d'administration :

   ```
   db.auth("nomutilisateur", "motdepasse")
   ```

   Le code retour **1** indique que l'utilisateur est ajouté, tandis que le code retour **0** indique que l'ajout de l'utilisateur a échoué.

Le tableau suivant contient des informations sur les rôles utilisateur et sur les attributs pour lesquels ils sont requis :

Tableau 183. Groupes d'attributs et leurs rôles utilisateur requis

Rôles	**Version de base de données MongoDB**	**Groupes d'attributs**
dbAdminAnyDatabase	2.x, 3.x et 4.x	Temps de réponse
readAnyDatabase	2.x, 3.x et 4.x	• Liste Mongod • Informations générales sur les fragments • Stockage des collectes • Noms de base de données • Détails du fragment • Détails du stockage des collections
clusterAdmin	2.x, 3.x et 4.x	• Informations d'instance Mongo • Infos d'E-S d'instance Mongo • MII Copy For APMUI One • MII Copy For APMUI Two • Verrou de BD d'instance Mongo • Verrous • Verrous MongoDB • Détails WiredTiger • Détails MMAPv1
clusterMonitor	2.x, 3.x et 4.x	• Informations d'instance Mongo • Infos d'E-S d'instance Mongo • MII Copy For APMUI One • MII Copy For APMUI Two • Verrou de BD d'instance Mongo • Verrous • Verrous MongoDB • Détails WiredTiger • Détails MMAPv1

- Pour la surveillance à distance du serveur MongoDB, prenez connaissance des deux prérequis suivants :
  1. Etant donné que l'Agent MongoDB exige l'interpréteur de commandes mongo pour collecter des informations à distance auprès du serveur MongoDB, le système sur lequel l'Agent MongoDB est installé et configuré doit posséder une instance du serveur MongoDB. L'interpréteur de commandes mongo du serveur MongoDB sur la machine agent permet de se connecter au serveur MongoDB distant à des fins de surveillance.
  2. Le fichier `/etc/hosts` du système hébergeant l'agent contient une entrée pour la machine distante.

Pourquoi et quand exécuter cette tâche

Le nom du système géré inclut le nom d'instance que vous indiquez. Par exemple, vous pouvez spécifier le nom d'instance sous la forme *nom_instance*`:`*nom_hôte*`:`*cp*, où *cp* est le code produit à deux caractères de votre agent. Le nom de système géré admet jusqu'à 32 caractères. Le nom d'instance admet jusqu'à 28 caractères, moins la longueur du nom d'hôte. Par exemple, si vous indiquez `Mongo2` comme nom d'instance, le nom du système géré est `Mongo2:hostname:KJ`.

Important : Si vous indiquez un nom d'instance long, le nom du système géré est tronqué et le code d'agent ne s'affiche pas entièrement.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

A faire :

- Pour que l'agent collecte correctement les données, démarrez-le en tant que superutilisateur (root) ou utilisez le même ID utilisateur pour démarrer l'agent et le processus mongod.
- Dans un environnement où MongoDB fonctionne comme cluster, veillez à installer l'agent sur le même ordinateur que celui où s'exécute le processus de routeur. Configurez l'agent sur le même ordinateur avec l'adresse IP et le numéro de port de ce dernier et définissez **TYPE** à la valeur `1`.
- Dans un environnement où MongoDB fonctionne comme cluster en mode d'authentification, ajoutez bien le même ID utilisateur avec les droits requis sur tous les fragments du cluster.

Vous pouvez configurer l'agent en utilisant les paramètres par défaut, en éditant le fichier de réponses silencieux ou en répondant aux invites.

Configuration de l'agent avec les paramètres par défaut

Dans un environnement typique, utilisez les paramètres par défaut pour configurer l'agent. Lorsque les paramètres par défaut sont utilisés pour la configuration d'agent, ce dernier ne s'exécute pas en mode d'authentification.

Procédure

1. Exécutez la commande suivante :
   rép_install`/bin/mongodb-agent.sh config` *nom_instance rép_install*`/samples/mongodb_silent_config.txt`

   Où

   - *nom_instance* est le nom que vous spécifiez pour l'instance d'application unique.
   - *rép_install* correspond au répertoire d'installation de l'Agent MongoDB.

   Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.
2. Exécutez la commande suivante pour démarrer l'agent :
   rép_install`/bin/mongodb-agent.sh start` *nom_instance*

Que faire ensuite
Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour définir des valeurs différentes pour les paramètres de configuration, et configurer l'agent.

Avant de commencer
Pour exécuter la base de données MongoDB dans le mode d'authentification, veillez à configurer l'agent avec un identificateur disposant des rôles clusterAdmin, readAnyDatabase et dbAdminAnyDatabase sur la base de données MongoDB.

Procédure

1. Dans un éditeur de texte, ouvrez le fichier de réponses silencieux disponible à l'emplacement suivant : *rép_install*/samples/mongodb_silent_config.txt.
2. Pour le paramètre **TYPE**, entrez l'une des valeurs suivantes :
   - 1 pour un cluster
   - 2 pour un ensemble de réplication
   - 3 pour une instance autonome

   Par défaut, l'agent surveille un cluster.
3. Pour le paramètre **PORT**, indiquez le numéro de port du routeur d'un cluster MongoDB ou d'une instance mongod de l'ensemble de réplication MongoDB surveillé.

   A faire : Si vous n'indiquez pas de numéro de port, l'agent reconnaît automatiquement le numéro de port du processus MongoDB approprié qui est actif dans l'interface par défaut. S'il n'y a pas de processus MongoDB actif dans l'interface par défaut, l'agent sélectionne le numéro de port du processus MongoDB approprié qui est actif dans la seconde interface.
4. Pour le paramètre **HOST**, indiquez l'adresse IP du système hôte MongoDB.

   A faire : Si vous n'indiquez pas d'adresse IP, l'agent détecte automatiquement l'adresse IP du processus MongoDB approprié qui est actif dans l'interface par défaut. Si le processus MongoDB est actif dans l'interface par défaut, l'agent détecte l'adresse IP du processus MongoDB approprié qui est actif dans l'interface secondaire.
5. Pour le paramètre **AUTHENTICATION**, indiquez YES pour spécifier que MongoDB est exécuté dans le mode d'authentification. La valeur par défaut est NO, qui indique que l'agent ne s'exécute pas actuellement en mode d'authentification.

   A faire : Lorsque la base de données MongoDB s'exécute en mode d'authentification, l'Agent MongoDB ou un client MongoDB ne peut pas se connecter à celle-ci sans données d'identification. Pour vous connecter à la base de données qui s'exécute en mode d'authentification, spécifiez YES pour le paramètre **AUTHENTICATION**.

   Si vous indiquez YES, effectuez les opérations suivantes :

   a) Pour le paramètre **User Name**, indiquez le nom d'utilisateur du routeur ou l'instance mongod. Assurez-vous que les rôles minimaux sont affectés à l'utilisateur. Pour plus d'informations sur les rôles d'utilisateur, voir Tableau 183, à la page 587.

   b) Pour le paramètre **Password**, indiquez le mot de passe.
6. Sauvegardez et fermez le fichier mongodb_silent_config.txt, puis exécutez la commande suivante :

rép_install/bin/mongodb-agent.sh config *nom_instance rép_install*/samples/mongodb_silent_config.txt

Où

- *nom_instance* est le nom que vous donnez à l'instance.
- *rép_install* correspond au répertoire d'installation de l'Agent MongoDB.

7. Exécutez la commande suivante pour démarrer l'agent :
rép_install/bin/mongodb-agent.sh start *nom_instance*

Important : Si vous mettez à niveau l'agent vers la version V1.0.0.9 ou ultérieure, et que vous voulez exécuter l'agent en mode d'authentification, vous devez reconfigurer l'agent afin d'indiquer un nom d'utilisateur et un mot de passe. Pour effectuer la collecte des données, vous devez arrêter et redémarrer l'agent après l'avoir configuré.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration de l'agent en répondant à des invites

Pour configurer l'agent avec des paramètres personnalisés, vous pouvez indiquer des valeurs pour les paramètres de configuration lorsque le système vous y invite pendant que le script est en cours d'exécution.

Procédure

1. Exécutez la commande suivante :
rép_install/bin/mongodb-agent.sh config *nom_instance*

Où

- *nom_instance* est le nom que vous donnez à l'instance.
- *rép_install* correspond au répertoire d'installation de l'Agent MongoDB.

2. Lorsque vous êtes invité à indiquer une valeur pour le paramètre **TYPE**, appuyez sur Entrée pour accepter la valeur par défaut ou spécifiez l'une des valeurs suivantes et appuyez ensuite sur la touche Entrée:

- 1 pour un cluster
- 2 pour un ensemble de réplication
- 3 pour une instance autonome

Par défaut, l'agent surveille un cluster.

3. Lorsque vous êtes invité à indiquer une valeur pour le paramètre **PORT**, appuyez sur Entrée pour accepter la valeur par défaut ou spécifiez le numéro de port du routeur pour un cluster MongoDB ou une instance mongod de l'ensemble de réplication MongoDB qui est surveillé, puis appuyez sur Entrée.

A faire : Si vous n'indiquez pas de numéro de port, l'agent reconnaît automatiquement le numéro de port du processus MongoDB approprié qui est actif dans l'interface par défaut. S'il n'y a pas de processus MongoDB actif dans l'interface par défaut, l'agent sélectionne le numéro de port du processus MongoDB approprié qui est actif dans la seconde interface.

4. Lorsque vous êtes invité à indiquer une valeur pour le paramètre **HOST**, appuyez sur Entrée pour accepter la valeur par défaut ou spécifiez l'adresse IP du système hôte MongoDB et appuyez ensuite sur la touche Entrée.

A faire : Si vous n'indiquez pas d'adresse IP, l'agent détecte automatiquement l'adresse IP du processus MongoDB approprié qui est actif dans l'interface par défaut. Si le processus MongoDB est actif dans l'interface par défaut, l'agent détecte l'adresse IP du processus MongoDB approprié qui est actif dans l'interface secondaire.

5. Lorsque vous êtes invité à indiquer une valeur pour le paramètre **AUTHENTICATION**, appuyez sur Entrée pour accepter la valeur par défaut ou indiquez si l'agent s'exécute en mode d'authentification.

   La valeur par défaut est NO, qui indique que l'agent ne s'exécute pas actuellement en mode d'authentification. Spécifiez YES pour indiquer que mongoDB s'exécute en mode d'authentification.

   A faire : Lorsque la base de données MongoDB s'exécute en mode d'authentification, l'Agent MongoDB ou un client MongoDB ne peut pas se connecter à celle-ci sans données d'identification. Pour vous connecter à la base de données qui s'exécute en mode d'authentification, spécifiez YES pour le paramètre **AUTHENTICATION**.

   Si vous indiquez YES, effectuez les opérations suivantes :

   a) Pour le paramètre **User Name**, indiquez le nom d'utilisateur du routeur ou l'instance mongod. Assurez-vous que les rôles minimaux sont affectés à l'utilisateur. Pour plus d'informations sur les rôles d'utilisateur, voir Tableau 183, à la page 587.

   b) Pour le paramètre **Password**, indiquez le mot de passe.

6. Exécutez la commande suivante pour démarrer l'agent :
   rép_install/bin/mongodb-agent.sh start *nom_instance*

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration de la surveillance de MySQL

Monitoring Agent for MySQL requiert un nom d'instance et les données d'identification utilisateur pour le serveur MySQL. Vous pouvez modifier les paramètres de configuration après avoir créé la première instance d'agent.

Avant de commencer

- Assurez-vous qu'un utilisateur est créé dans la base de données MySQL pour exécuter l'agent. L'utilisateur n'a pas besoin de privilèges particuliers sur la base de données MySQL surveillée.
- Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent MySQL.

Pourquoi et quand exécuter cette tâche

Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Le nom de système géré inclut le nom d'instance que vous spécifiez, *nom_instance*:*nom_hôte*:*cp* par exemple, où *cp* est le code produit à deux caractères. Le nom de système géré admet jusqu'à 32 caractères. Le nom d'instance que vous entrez admet jusqu'à 28 caractères, moins la longueur de votre nom d'hôte. Par exemple, si vous indiquez MySQL2 comme nom d'instance, le nom du système géré est MySQL2:hostname:SE.

Important : Si vous indiquez un nom d'instance long, le nom du système géré est tronqué et le code d'agent ne s'affiche pas entièrement.

Configuration de l'agent sur des systèmes Windows

Vous pouvez utiliser la fenêtre IBM Cloud Application Performance Management pour configurer l'agent sur des systèmes Windows.

Procédure

1. Cliquez sur **Démarrer > Tous les programmes > IBM Monitoring agents > IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, procédez comme suit :
   a) Cliquez deux fois sur le modèle **Monitoring Agent for MySQL**.
   b) Dans la fenêtre **Monitoring Agent for MySQL** indiquez un nom d'instance et cliquez sur **OK**.
3. Dans la fenêtre **Monitoring Agent for MySQL**, procédez comme suit :
   a) Dans la zone **Adresse IP**, entrez l'adresse IP d'un serveur MySQL à surveiller à distance. Si l'agent est installé sur le serveur à surveiller, conservez la valeur par défaut.
   b) Dans la zone **Nom d'utilisateur JDBC**, entrez le nom d'un utilisateur du serveur MySQL. La valeur par défaut est root.
   c) Dans la zone **Mot de passe JDBC**, entrez le mot de passe d'un utilisateur JDBC.
   d) Dans la zone **Confirmer le mot de passe JDBC**, entrez de nouveau le mot de passe.
   e) Dans la zone **Fichier Jar JDBC**, cliquez sur **Parcourir** et localisez le répertoire qui contient le fichier Java de connecteur MySQL, et sélectionnez-le.
   f) Cliquez sur **Suivant**.
   g) Dans la zone **Numéro de port JDBC**, indiquez le numéro de port du serveur JDBC.
   Le numéro de port par défaut est 3306.
   h) Dans la liste **Niveau de trace Java**, sélectionnez un niveau de trace pour Java.
   La valeur par défaut est `Error`.
   i) Cliquez sur **OK**.
   L'instance est affichée dans la fenêtre **IBM Performance Management**.
4. Cliquez avec le bouton droit de la souris sur l'instance **Monitoring Agent for MySQL** et cliquez sur **Démarrer**.

   A faire : Pour configurer de nouveau l'agent, effectuez ces étapes dans la fenêtre **IBM Performance Management** :

   a. Arrêtez l'instance d'agent que vous voulez configurer.
   b. Cliquez avec le bouton droit de la souris sur l'instance **Monitoring Agent for MySQL** et cliquez sur **Reconfigurer**.
   c. Répétez les étapes 3 et 4.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de l'agent sur des systèmes Linux

Exécutez le script de configuration pour configurer l'agent sur les systèmes Linux.

Procédure

1. Exécutez la commande suivante :

```
rép_install/bin/mysql-agent.sh config nom_instance
```

Où *nom_instance* est le nom à attribuer à l'instance, et *rép_install* est le répertoire d'installation de l'Agent MySQL.

2. A l'invite d'entrée d'une valeur pour les paramètres suivants, appuyez sur Entrée pour accepter la valeur par défaut ou indiquez une autre valeur et appuyez sur Entrée.
   - Adresse IP
   - Nom d'utilisateur JDBC
   - Mot de passe JDBC
   - Ressaisir le mot de passe JDBC
   - Fichier Jar JDBC
   - Numéro du port JDBC (le numéro du port par défaut est 3306.)
   - Niveau de trace Java (la valeur par défaut est `Error`.)

   Pour plus d'informations sur les paramètres de configuration, voir «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 593.
3. Exécutez la commande suivante pour démarrer l'agent.

```
rép_install/bin/mysql-agent.sh start nom_instance
```

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Utilisez le fichier de réponses silencieux pour configurer l'agent sans répondre aux invites quand vous exécutez le script de configuration. Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'agent sur les systèmes Windows et Linux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration. Vous éditez les valeurs de paramètre dans le fichier de réponses, et exécutez le script de configuration pour créer une instance d'agent et mettre à jour les valeurs de configuration.

Procédure

1. Dans un éditeur de texte, ouvrez le fichier de réponses disponible à l'emplacement suivant :

   Linux *rép_install*`/samples/mysql_silent_config.txt`

   Windows *rép_install*`\samples\mysql_silent_config.txt`

   Où *rép_install* correspond au répertoire d'installation de l'Agent MySQL.
2. Dans le fichier de réponses, indiquez une valeur pour les paramètres suivants :
   - Pour le paramètre **`Nom de serveur`**, spécifiez l'adresse IP d'un serveur MySQL à surveiller à distance. Sinon, conservez la valeur par défaut `localhost`.
   - Pour le paramètre **`Nom d'utilisateur JDBC`**, conservez la valeur de nom d'utilisateur par défaut `root` ou indiquez le nom d'un utilisateur qui dispose des droits permettant d'afficher les tables INFORMATION_SCHEMA.
   - Pour le paramètre **`Mot de passe JDBC`**, entrez le mot de passe de l'utilisateur JDBC.

- Pour le paramètre **Fichier JAR JDBC**, conservez le chemin par défaut si ce chemin d'accès au connecteur MySQL pour le fichier JAR Java est correct. Sinon, indiquez le chemin approprié. Le connecteur est disponible à l'emplacement par défaut suivant :

  Linux `/usr/share/java/mysql-connector-java.jar`

  Windows `C:\Program Files (x86)\MySQL\Connector J 5.1.26\mysql-connector-java-5.1.26-bin.jar`
- Pour le paramètre **Numéro de port JDBC**, conservez le numéro de port par défaut 3306 ou indiquez un autre numéro de port.
- Pour le paramètre **Niveau de trace Java**, conservez la valeur par défaut Erreur ou indiquez un autre niveau de trace selon les instructions du support IBM.

3. Sauvegardez et fermez le fichier de réponses, puis entrez la commande suivante pour mettre à jour les paramètres de configuration de l'agent :

   Linux `rép_install/bin/mysql-agent.sh config nom_instance rép_install/samples/mysql_silent_config.txt`

   Windows `rép_install\BIN\mysql-agent.bat config nom_instance rép_install\samples\mysql_silent_config.txt`

   Où *nom_instance* est le nom à attribuer à l'instance, et *rép_install* est le répertoire d'installation de l'Agent MySQL.

   Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, aucune donnée d'agent ne s'affiche dans les tableaux de bord.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de la surveillance de NetApp Storage

Monitoring Agent for NetApp Storage surveille les systèmes de stockage NetApp à l'aide de NetApp OnCommand Unified Manager, d'OnCommand API Services et d'OnCommand Performance Manager.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent NetApp Storage.
- Assurez-vous que les composants suivants sont installés sur votre machine :
  - OnCommand Unified Manager
  - OnCommand Performance Manager
  - OnCommand API Services

  Pour plus d'informations sur l'installation de ces composants, voir la documentation NetApp.
- Assurez-vous que les versions d'OnCommand API Services, d'OnCommand Unified Manager et d'OnCommand Performance Manager sont compatibles. Par exemple, pour configurer OnCommand API Services V1.0, associez OnCommand Unified Manager V6.2, V6.1 ou V6.0 à OnCommand Performance Manager V1.1. Pour connaître les versions de produit compatibles, voir Interoperability Matrix Tool.
- Assurez-vous que l'utilisateur qui se connecte à OnCommand Unified Manager dispose du privilège GlobalRead pour le système de stockage NetApp en cours de surveillance. Utilisez un ID utilisateur existant disposant de ce privilège ou créez un nouvel ID utilisateur. Pour plus d'informations sur la création de l'ID utilisateur dans votre système de stockage NetApp, voir la documentation NetApp.

- Assurez-vous que l'utilisateur que vous utilisez pour la configuration d'OnCommand API Services est un administrateur ou un contrôleur. Ces types d'utilisateur disposent par défaut des droits d'exécution de l'API REST.
- Téléchargez le fichier JAR de NetApp Manageability SDK (`manageontap.jar`) à partir du site Web de NetApp et installez le fichier dans le répertoire `lib` de l'agent de surveillance en procédant comme décrit à la rubrique «Téléchargement et installation du fichier JAR de NetApp Manageability SDK», à la page 595.

Pourquoi et quand exécuter cette tâche

L'agent NetApp Storage est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

- Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser la fenêtre **IBM Performance Management** ou le fichier de réponses silencieux.
- Pour configurer l'agent sur les systèmes Linux, vous pouvez exécuter le script et répondre aux invites, ou utiliser le fichier de réponses silencieux.

Téléchargement et installation du fichier JAR de NetApp Manageability SDK

L'agent NetApp Storage nécessite que le fichier JAR de NetApp Manageability SDK communique avec un serveur NetApp OCUM.

Pourquoi et quand exécuter cette tâche

Après avoir installé l'agent NetApp Storage, téléchargez le fichier JAR de NetApp Manageability SDK (`manageontap.jar`) à partir du site Web de NetApp et installez le fichier dans le répertoire `lib` de l'agent de surveillance.

Procédure

1. Téléchargez le fichier compressé contenant le fichier JAR à partir du site Web suivant : http://communities.netapp.com/docs/DOC-1152.
2. Extrayez ce fichier compressé et copiez le fichier `manageontap.jar` aux emplacements suivants :
   - Pour les systèmes Windows 32 bits, copiez le fichier dans *rép_install*`/tmaitm6`
   - Pour les systèmes Windows 64 bits, copiez le fichier dans *rép_install*`/tmaitm6_x64`
   - Pour les systèmes Linux 32 bits, copiez le fichier dans *rép_install*`/li6263/nu/lib`
   - Pour les systèmes Linux x86-64 64 bits, copiez le fichier dans *rép_install*`/lx8266/nu/lib`
   - Pour les systèmes zLinux 64 bits, copiez le fichier dans *rép_install*`/ls3266/nu/lib`

Que faire ensuite

Terminez la configuration de l'agent.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent sur les systèmes d'exploitation Windows à l'aide de la fenêtre **IBM Performance Management**. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Pourquoi et quand exécuter cette tâche

L'agent NetApp Storage fournit les valeurs par défaut de certains paramètres. Vous pouvez spécifier différentes valeurs pour ces paramètres.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Monitoring Agent for NetApp Storage**, puis sur **Configuration de l'agent**.

   A faire : La première fois que vous configurez l'agent, l'option **Configuration de l'agent** est désactivée. Pour reconfigurer l'agent, cliquez sur **Reconfigurer**.
3. Dans la fenêtre Monitoring Agent for NetApp Storage, procédez comme suit :
   a) Entrez un nom unique pour l'instance d'agent NetApp Storage et cliquez sur **OK**.
   b) Dans l'onglet **Fournisseur de données**, indiquez les valeurs des paramètres de configuration, puis cliquez sur **Suivant**.
   c) Dans l'onglet **OnCommand Unified Manager**, indiquez les valeurs des paramètres de configuration, puis cliquez sur **Suivant**.
   d) Dans l'onglet **OnCommand API Service**, indiquez les valeurs des paramètres de configuration, puis cliquez sur **OK**.

   Pour plus d'informations sur les paramètres de configuration dans chaque onglet de la fenêtre Monitoring Agent for NetApp Storage, consultez les rubriques suivantes :
   - «Paramètres de configuration du fournisseur de données», à la page 598
   - «Paramètres de configuration d'OnCommand Unified Manager», à la page 600
   - «Paramètres de configuration d'OnCommand API Service», à la page 600
4. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Monitoring Agent for NetApp Storage**, puis sur **Démarrer**.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

- Pour configurer l'agent NetApp Storage en mode silencieux, procédez comme suit :
  a) Dans un éditeur de texte, ouvrez le fichier `netapp_storage_silent_config.txt` disponible à l'emplacement suivant :
     – Linux *rép_install*`/samples/netapp_storage_silent_config.txt`

       Exemple : `/opt/ibm/apm/agent/samples/netapp_storage_silent_config.txt`
     – Windows *rép_install*`\samples\netapp_storage_silent_config.txt`

       Exemple : `C:\IBM\APM\samples\netapp_storage_silent_config.txt`
  b) Dans le fichier `netapp_storage_silent_config.txt`, spécifiez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.

     Pour plus d'informations sur les paramètres de configuration, voir les rubriques suivantes :
     – «Paramètres de configuration du fournisseur de données», à la page 598
     – «Paramètres de configuration d'OnCommand Unified Manager», à la page 600
     – «Paramètres de configuration d'OnCommand API Service», à la page 600
  c) Sauvegardez et fermez le fichier `netapp_storage_silent_config.txt` et exécutez la commande suivante :
     – Linux *rép_install*`/bin/netapp_storage-agent.sh config` *nom_instance* *rép_install*`/samples/netapp_storage_silent_config.txt`

       Exemple : **`/opt/ibm/apm/agent/bin/netapp_storage-agent.sh config nom_instance /opt/ibm/apm/agent/samples/netapp_storage_silent_config.txt`**
     – Windows *rép_install*`\bin\netapp_storage-agent.bat config` *rép_install_nom_instance*`\samples\netapp_storage_silent_config.txt`

       Exemple : **`C:\IBM\APM\bin\netapp_storage-agent.bat config nom_instance C:\IBM\APM\samples\netapp_storage_silent_config.txt`**

       Où

       nom_instance
       Nom à attribuer à l'instance.

       rép_install
       Chemin d'installation de l'agent.

     Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.
  d) Exécutez la commande suivante pour démarrer l'agent :
     – Linux *rép_install*`/bin/netapp_storage-agent.sh start` *nom_instance*

       Exemple : **`/opt/ibm/apm/agent/bin/netapp_storage-agent.sh start nom_instance`**
     – Windows *rép_install*`\bin\netapp_storage-agent.bat start` *nom_instance*

       Exemple : **`C:\IBM\APM\bin\netapp_storage-agent.bat start nom_instance`**

Que faire ensuite
Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration de l'agent en répondant à des invites

Pour configurer l'agent sur des systèmes Linux, vous pouvez exécuter le script ou répondre à des invites.

Procédure

1. Sur la ligne de commande, entrez la commande suivante :

   rép_install/bin/netapp_storage-agent.sh config *nom_instance*

   Exemple : **/opt/ibm/apm/agent/bin/netapp_storage-agent.sh config nom_instance**

   Où

   nom_instance
   Nom à attribuer à l'instance.

   rép_install
   Chemin d'installation de l'agent.
2. Répondez aux invites en vous référant aux rubriques suivantes :
   - «Paramètres de configuration du fournisseur de données», à la page 598
   - «Paramètres de configuration d'OnCommand Unified Manager», à la page 600
   - «Paramètres de configuration d'OnCommand API Service», à la page 600
3. Exécutez la commande suivante pour démarrer l'agent :

   rép_install/bin/netapp_storage-agent.sh start *nom_instance*

   Exemple : **/opt/ibm/apm/agent/bin/netapp_storage-agent.sh start nom_instance**

Que faire ensuite
Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Paramètres de configuration du fournisseur de données

Lorsque vous configurez l'agent NetApp Storage, vous pouvez modifier les valeurs par défaut des paramètres pour le fournisseur de données, comme le nombre maximal de fichiers journaux du fournisseur de données, la taille maximale du fichier journal et le niveau de détail inclus dans le fichier journal.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration du fournisseur de données.

Tableau 184. Noms et descriptions des paramètres de configuration du fournisseur de données

Nom du paramètre	Description	Zone obligatoire
Nom d'instance (**KNU_INSTANCE_NAME**)	Nom de l'instance. **Restriction :** La zone Nom d'instance contient le nom de l'instance que vous spécifiez lorsque vous configurez l'agent pour la première fois. Lorsque vous reconfigurez l'agent, vous ne pouvez pas modifier le nom d'instance de l'agent.	Oui
Maximum number of Data Provider Log Files (**KNU_LOG_FILE_MAX_COUNT**)	Nombre maximal de fichiers journaux créés par le fournisseur de données avant qu'il remplace les anciens fichiers journaux. La valeur par défaut est 10.	Oui
Maximum Size in KB of Each Data Provider Log (**KNU_LOG_FILE_MAX_SIZE**)	Taille maximale en ko qu'un fichier journal de fournisseur de données doit atteindre avant que le fournisseur de données ne crée un autre fichier journal. La valeur par défaut est 5190 ko.	Oui
Level of Detail in Data Provider Log (**KNU_LOG_LEVEL**)	Niveau de détail qui peut être inclus dans le fichier journal que le fournisseur de données crée. La valeur par défaut est 4 (Info). Les valeurs suivantes sont valides : • 1 (Off) : aucun message n'est consigné. • 2 (Severe) : seules les erreurs sont consignées. • 3 (Warning) : toutes les erreurs et tous les messages consignés au niveau Severe et les erreurs potentielles qui peuvent entraîner un comportement non souhaité. • 4 (Info) : toutes les erreurs et tous les messages consignés au niveau Warning et les messages d'information de niveau supérieur qui décrivent l'état du fournisseur de données pendant son traitement. • 5 (Fine) : toutes les erreurs et tous les messages consignés au niveau Info et les messages d'information de niveau inférieur qui décrivent l'état du fournisseur de données pendant son traitement. • 6 (Finer) : toutes les erreurs et tous les messages consignés au niveau Fine plus les messages d'information très détaillés, tels que les informations sur le profil de performance et les données de débogage. Si vous sélectionnez cette option, cela peut affecter les performances de l'agent de surveillance. Ce paramètre n'est destiné qu'à être utilisé comme un outil pour l'identification des problèmes, en collaboration avec l'équipe de support IBM. • 7 (Finest) : toutes les erreurs et tous les messages consignés au niveau Fine et les messages d'information les plus détaillés qui incluent les messages et les données de programmation de niveau inférieur. Cette option risque d'affecter les performances de l'agent de surveillance de manière négative. Ce paramètre n'est destiné qu'à être utilisé comme un outil pour l'identification des problèmes, en collaboration avec l'équipe de support IBM. • 8 (All) : toutes les erreurs et tous les messages sont consignés.	Oui

Paramètres de configuration d'OnCommand Unified Manager

Lorsque vous configurez l'agent NetApp Storage, vous pouvez modifier les valeurs par défaut des paramètres d'OnCommand Unified Manager (OCUM), tels que l'adresse IP du serveur OCUM, le nom d'utilisateur et le mot de passe.

Le tableau ci-après contient une description détaillée des paramètres de configuration de la source de données.

Tableau 185. Noms et descriptions des paramètres de configuration d'OnCommand Unified Manager

Nom du paramètre	Description	Zone obligatoire
Serveur (**KNU_DATASOURCE_HOST_ADDRESS**)	Nom d'hôte ou adresse IP du serveur NetApp OCUM à surveiller.	Oui
Utilisateur (**KNU_DATASOURCE_USERNAME**)	Nom d'utilisateur sur le serveur NetApp OCUM dotés de privilèges lui permettant de collecter des données. La valeur par défaut est admin.	Oui
Mot de passe (**KNU_DATASOURCE_PASSWORD**)	Mot de passe de l'utilisateur que vous spécifiez dans le paramètre **Utilisateur**.	Oui
Confirmer le mot de passe	Mot de passe que vous avez indiqué dans le paramètre **Mot de passe**.	Oui
Protocole (**KNU_DATASOURCE_PROTOCOL**)	Protocole utilisé pour communiquer avec le serveur NetApp OCUM. La valeur par défaut est HTTPS.	Oui

Paramètres de configuration d'OnCommand API Service

Lorsque vous configurez l'agent NetApp Storage, vous pouvez modifier les valeurs par défaut des paramètres d'OnCommand API Service, tels que l'adresse hôte, le nom d'utilisateur et le mot de passe.

Le tableau ci-après contient une description détaillée des paramètres de configuration de la source de données.

Tableau 186. Noms et descriptions des paramètres de configuration d'OnCommand API Service

Nom du paramètre	Description	Zone obligatoire
Adresse hôte (**KNU_API_SERVICES_HOST_ADDRESS**)	Nom d'hôte ou adresse IP d'OnCommand API service.	Oui
Utilisateur (**KNU_API_SERVICES_USERNAME**)	Nom d'utilisateur disposant des privilèges lui permettant de se connecter à OnCommand API Service. La valeur par défaut est admin.	Oui
Mot de passe (**KNU_API_SERVICES_PASSWORD**)	Mot de passe de l'utilisateur que vous spécifiez dans le paramètre **Utilisateur**.	
Confirmer le mot de passe	Mot de passe que vous avez indiqué dans le paramètre **Mot de passe**.	Oui

Configuration de la surveillance de Node.js

Vous pouvez utiliser l'agent Node.js ou le collecteur de données Node.js autonome pour surveiller vos applications Node.js. Le collecteur de noeuds Node.js offre un processus d'installation et une fonction de suivi des transactions plus simples.

Avant de commencer

- Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent et du collecteur de données. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.
- Assurez-vous que votre environnement possède la configuration système requise pour l'Agent Node.js ou le collecteur de données Node.js.
  - Pour les toutes dernières informations sur la configuration système requise de l'Agent Node.js, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent Node.js.
  - Pour les toutes dernières informations sur la configuration système requise de l'collecteur de données Node.js, voir les rapports de compatibilité des produits logiciels (SPCR) de l'collecteur de données Node.js.

Pourquoi et quand exécuter cette tâche

La procédure suivante, qui inclut des étapes obligatoires et facultatives, permet de configurer Monitoring Agent for Node.js et le collecteur de données Node.js autonome.

- Pour surveiller les applications sur site, vous pouvez configurer le collecteur de données Node.js autonome ou l'Agent Node.js. Si vous souhaitez activer le suivi des transactions pour vos applications Node.js, configurez le collecteur de données autonome.
- Pour surveiller IBM Cloud(anciennement Bluemix) ou les applications Kubernetes, configurez le collecteur de données Node.js autonome.

Effectuez les étapes ci-après en fonction de vos besoins.

Procédure

- Configurez l'Agent Node.js pour surveiller vos applications sur site.
  a) Ajoutez un collecteur de données d'agent à vos applications Node.js pour que l'agent fonctionne correctement. Voir «Configuration de l'Agent Node.js», à la page 602.
  b) Facultatif : Pour modifier le comportement de surveillance de votre agent, voir Configuration du collecteur de données de l'Agent Node.js.
  c) Facultatif : Pour configurer la collecte et l'affichage des données de diagnostic, voir Configuration du collecteur de données de diagnostic.
- Configurez le collecteur de données Node.js autonome pour surveiller les applications IBM Cloud.
  a) Pour configurer le collecteur de données Node.js autonome, voir «Configuration du collecteur de données Node.js autonome pour les applications IBM Cloud(anciennement Bluemix)», à la page 608.
  b) Pour modifier le comportement du collecteur de données Node.js autonome, voir «Personnalisation du collecteur de données Node.js autonome pour les applications IBM Cloud», à la page 610.
- Configurez le collecteur de données Node.js autonome pour surveiller les applications sur site.
  a) Pour configurer le collecteur de données Node.js autonome, voir «Configuration du collecteur de données Node.js autonome pour les applications sur site», à la page 615.
  b) Pour modifier le comportement du collecteur de données Node.js autonome, voir «Personnalisation du collecteur de données Node.js pour les applications sur site», à la page 616.

- Configurez le collecteur de données Node.js autonome pour surveiller les applications dans Kubernetes.
  a) Pour configurer le collecteur de données Node.js autonome, voir «Configuration du collecteur de données Node.js autonome pour les applications Kubernetes», à la page 621.
  b) Pour modifier le comportement du collecteur de données Node.js autonome, voir «Personnalisation du collecteur de données Node.js autonome pour les applications Kubernetes», à la page 621.

Configuration de l'Agent Node.js

Vous devez ajouter un collecteur de données d'agent à votre application Node.js et la redémarrer pour que l'agent puisse commencer à la surveiller.

Avant de commencer

Avant de reconfigurer les paramètres de l'agent dans la même version, nettoyez les fichiers du collecteur de données qui ont été créés par la configuration précédente de la manière suivante :

1. Accédez au répertoire *rép_install*/lx8266/nj/bin.
2. Exécutez la commande ./uninstall.sh pour supprimer les fichiers du collecteur de données existants.

Pourquoi et quand exécuter cette tâche

L'agent Node.js est un agent à instance unique. Il enregistre des sous-noeuds pour chaque application Node.js surveillée. Le sous-noeud possède la structure suivante :

NJ:hostname_port:NJA

Conseil : Si une application Node.js est en mode écoute sur plusieurs numéros de port, le numéro de port le plus bas est utilisé.

Vous devez ajouter un collecteur de données d'agent à votre application Node.js et la redémarrer pour que l'agent puisse commencer à la surveiller. Les collecteurs de données d'agent collectent des données qui sont transmises à l'agent Node.js. Actuellement, les collecteurs de données d'agent suivants sont fournis :

- Le collecteur de données de ressources collecte les données de surveillance des ressources à partir de vos applications Node.js.
- Le collecteur de données de diagnostic collecte les données de diagnostic et de surveillance des ressources à partir de vos applications Node.js.
- Le collecteur de données de trace de méthode collecte les traces de méthode, les données de diagnostic et les données de surveillance des ressources à partir de vos applications Node.js.

Procédure

1. Assurez-vous que l'ID utilisateur utilisé pour exécuter le serveur d'applications a des droits complets sur le répertoire rép_install de l'agent.
2. Accédez au répertoire *rép_install*/bin et exécutez la commande suivante :

   ```
   ./nodejs-agent.sh config
   ```

3. Suivez les instructions des invites pour spécifier les valeurs des options de configuration suivantes :

   KNJ_NODEJS_RUNTIME_BIN_LOCATION
   Répertoire contenant le dossier bin de votre exécution Node.js. Le répertoire par défaut est /usr/local/bin.

   KNJ_NPM_RUNTIME_BIN_LOCATION
   Répertoire contenant le dossier bin de votre commande **npm**. Le répertoire par défaut est /usr/local/bin.

KNJ_NPM_LIB_LOCATION
Répertoire contenant le dossier `lib` de votre répertoire d'installation global du package npm. Le répertoire par défaut est `/usr/local/lib`. Par exemple, si vous installez le package npm en exécutant la commande `npm install -g`, le package est installé dans `/rép_base_nodejs/lib/node_modules` et **KNJ_NPM_LIB_LOCATION** correspond à `/rép_base_nodejs/lib`.

CP_PORT
Port sur lequel l'agent écoute les données provenant des clients du socket. La valeur `0` indique qu'un port éphémère sera utilisé. La valeur par défaut est `63336`.

Remarque : N'utilisez pas le numéro de port déjà utilisé sur votre système. Pour vérifier si le port est déjà utilisé, exécutez la commande `netstat -apn | grep numéro_port`.

4. Démarrez l'agent en exécutant la commande suivante :

```
./nodejs-agent.sh start
```

5. Vérifiez que l'Agent Node.js est démarré avec succès. Le dossier *KNJ_NPM_LIB_LOCATION*`/node_modules/ibmapm` est généré si l'agent démarre correctement.
6. En fonction de l'offre dont vous disposez et des exigences, insérez l'une des entrées suivantes dans le fichier `.js` de votre application Node.js pour configurer les collecteurs de données d'agent :

   Remarque : Une seule entrée peut être ajoutée à votre application Node.js afin d'activer les fonctionnalités du collecteur de données de l'agent. De même, si vous activez les fonctionnalités qui ne sont pas incluses dans l'offre, le système peut être inutilement surchargé, ce qui peut réduire l'efficacité de l'exécution de l'application.

   - Si vous n'avez que des fonctionnalités de surveillance de ressources, vous pouvez ajouter le collecteur de données de ressource. Pour ce faire, insérez la ligne suivante au début du fichier d'application Node.js :

     ```
     require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm');
     ```

     Si la valeur de **KNJ_NPM_LIB_LOCATION** est `/usr/local/lib` dans votre environnement, la ligne apparaît comme suit :

     ```
     require('/usr/local/lib/node_modules/ibmapm');
     ```

   - Si vous avez des fonctionnalités de diagnostic en plus de la surveillance au niveau de la ressource, vous pouvez choisir d'ajouter l'un des collecteurs de données d'agent suivants :
     – Pour ajouter le collecteur de données de trace de méthode, insérez la ligne suivante au début du fichier d'application Node.js :

       ```
       require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm/methodtrace.js');
       ```

     – Pour ajouter le collecteur de données de diagnostic, insérez la ligne suivante au début du fichier d'application Node.js :

       ```
       require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm/deepdive.js');
       ```

     – Pour ajouter le collecteur de données de surveillance des ressources, insérez la ligne suivante au début du fichier d'application Node.js :

       ```
       require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm');
       ```

     Pour améliorer les performances, ajoutez le collecteur de données de trace de méthode à des fins de débogage uniquement.

   Remarque : le code des plug-in change à partir de Cloud APM mars 2017. Si vous mettez à niveau votre agent à partir de versions antérieures, vous devez mettre à jour le code des collecteurs de données existants dans vos applications pour que la fonctionnalité de surveillance fonctionne correctement.

7. Redémarrez l'application Node.js pour activer le collecteur de données de l'agent.

Résultats
Vous avez correctement configuré l'Agent Node.js.

Que faire ensuite

- Vous pouvez à présent vérifier que les données de l'Agent Node.js s'affichent dans la console Cloud APM. Pour obtenir des instructions de démarrage de la console Cloud APM, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.

  Important : pour ajouter votre application à la console Cloud APM, choisissez **Node.js** dans l'éditeur d'application.
- Vous pouvez modifier le comportement d'exécution des collecteurs de données d'agent Node.js. Pour plus d'informations, voir Configuration du collecteur de données de l'agent Node.js.
- Vous pouvez activer la collecte et l'affichage des données de diagnostic en configurant le collecteur de données de diagnostic. Pour plus d'informations, voir Configuration du collecteur de données de diagnostic.

Configuration du collecteur de données de l'Agent Node.js
Vous pouvez modifier le comportement du collecteur de données de chaque agent Node.js en changeant la configuration d'environnement d'exécution qui lui est associée dans son fichier de configuration.

Fichier de configuration de l'environnement d'exécution

Le code du collecteur de données Node.js se trouve dans le répertoire suivant :

KNJ_NPM_LIB_LOCATION/node_modules/ibmapm

où *KNJ_NPM_LIB_LOCATION* correspond au répertoire du dossier lib de votre répertoire d'installation global du package npm. Le répertoire par défaut est /usr/local/lib.

Il existe également un fichier de configuration d'environnement d'exécution pour le collecteur de données de chaque agent dans le même dossier. Le collecteur de données de l'agent lit le fichier de configuration toutes les minutes.

Conseil : Le fichier de configuration d'environnement d'exécution est nommé comme suit :

plugin_*numéro de port d'application*_conf.json

Lorsque vous modifiez le contenu du fichier de configuration, le comportement du collecteur de données de l'agent associé change. Le fichier de configuration contient deux types d'information que vous pouvez modifier :

- Règles de filtrage d'URL
- Paramètres de consignation du collecteur de données de l'agent

Règles de filtrage d'URL

Vous pouvez modifier les règles de filtrage d'URL dans le fichier de configuration d'exécution. Des expressions régulières sont utilisées pour mapper le nom de chemin d'URL à un nom de chemin personnalisé par l'utilisateur. Vous pouvez mapper l'URL à un nom de chemin personnalisé pour répondre aux exigences suivantes :

- Agrégation d'URL avec des chemins similaires. Prenons l'exemple des chemins d'URL suivants :

```
/demo/poll/1
/demo/poll/2
/demo/poll/3
...
```

Sur le serveur Web, les demandes associées à ces chemins sont probablement exécutées par une routine commune ; vous pouvez donc agréger les chemins en un type d'URL unique en utilisant le filtre de l'exemple ci-dessous.

```
"filters":
[
    {
        "pattern": "/demo/poll/.+",
        "to": "/demo/poll/"
    }
```

Avec ce filtre, toutes les demandes vers des chemins d'URL semblables à "`/demo/poll/xxx`" sont mappées au type de chemin d'URL "`/demo/poll`". La moyenne des temps de réponse pour toutes les demandes vers les chemins d'URL de ce type est alors calculée pour générer une valeur unique. Une telle agrégation permet d'utiliser plus efficacement les ressources disponibles.

- Omission des chemins d'URL pointant vers des fichiers statiques ou filtrage de certains types de demande. Par exemple, si une page Web inclut des images qui génèrent des demandes de téléchargement sur des serveurs distincts, l'affichage des temps de réponse pour ces types de demandes peut ne pas présenter d'intérêt.

  Pour filtrer un type de demande, ne définissez pas la valeur "`to`", conformément au format de l'exemple suivant :

  ```
  "filters":
  [
      {
          "pattern": "GET /css/.+\\.css$",
          "to": ""
      }
  ```

  Lors de l'exécution de ce filtre, le fichier `.css` concerné par la demande est ignoré. Par conséquent, vous pouvez utiliser les ressources disponibles de manière plus efficace sur les demandes que vous devez surveiller.

Dans le fichier de configuration, les règles de filtrage d'URL sont répertoriées dans un tableau JSON nommé `filters` :

```
"filters":
[
    {
        "pattern": ".+\\.png$",
        "to": ""
    },
    {
        "pattern": ".+\\.jpg$",
        "to": ""
    },
    {
        "pattern": "GET /js/.+\\.js$",
        "to": ""
    },
    {
        "pattern": "GET /css/.+\\.css$",
        "to": ""
    }
]
```

Chaque membre du tableau est une règle de filtrage. Lorsqu'une demande HTTP est reçue par le collecteur de données de l'agent, celui-ci extrait le nom de chemin d'URL de la demande et le compare à chaque "`pattern`". Si le nom de chemin ne correspond à aucun "`pattern`", le nom de chemin d'URL d'origine est conservé et utilisé pour les mesures.

Paramètre de consignation du collecteur de données de l'agent

Vous pouvez modifier les comportements de consignation en modifiant le paramètre dans le fichier de configuration `config.properties` du répertoire *KNJ_NPM_LIB_LOCATION*`/node_modules/ibmapm/etc`. Le paramètre de consignation suivant est fourni et peut être modifié :

Niveau de consignation

Dans le fichier de configuration, l'entrée correspondant au niveau de consignation est `KNJ_LOG_LEVEL=info`, ce qui signifie que les informations récapitulatives sur les actions sont enregistrées dans le journal. Vous pouvez définir le niveau de consignation en modifiant la valeur de `KNJ_LOG_LEVEL`. La valeur par défaut est `info` et le journal est imprimé dans la sortie standard.

Les cinq valeurs de niveau de consignation suivantes sont prises en charge :

off
Les journaux ne sont pas imprimés.

error
Les informations ne sont consignées qu'en cas d'erreur.

info
Les informations sont consignées lorsque le collecteur de données de l'Agent Node.js fonctionne normalement. Les données de surveillance brutes envoyées à l'agent sont également consignées.

debug
Les informations de niveau débogage, informations et erreur sont consignées dans le journal. Il peut s'agir notamment des données collectées, des données envoyées au serveur et de la réponse du serveur.

all
Toutes les informations sont consignées dans le journal.

Configuration du collecteur de données de diagnostic de l'Agent Node.js

La prise en charge de la collecte des données de diagnostic est désactivée par défaut. Si vous avez des fonctionnalités de diagnostic, vous devez définir et ajuster la collecte de données pour les applications Node.js.

Procédure

- Pour modifier les paramètres du collecteur de données pour une application spécifique en cours d'exécution :
  1. Accédez au répertoire *KNJ_NPM_LIB_LOCATION*`/node_modules/ibmapm` et ouvrez le fichier `plugin_`*port*`_conf.json` dans un éditeur de texte.

     Conseil : Pour plus d'informations sur *KNJ_NPM_LIB_LOCATION*, voir la description du paramètre «KNJ_NPM_LIB_LOCATION», à la page 603
  2. Utilisez le tableau suivant pour obtenir des informations sur la modification des paramètres du collecteur de données :

Tableau 187. Paramètres du collecteur de données

Catégorie de données de diagnostic	Description	Propriété	Action
Retardement minimum pour la génération d rapport de trace de pile	Indique le seuil de temps de réponse pour la collecte de la trace de pile d'une demande ou d'un appel de méthode. Si le temps de réponse d'une demande ou d'un appel de méthode dépasse cette valeur, le collecteur de données collecte sa trace de pile.	`minClockStack`	Valeur en millisecondes
Retardement minimum de signalement des demandes	Indique le seuil de temps de réponse pour la collecte de la trace de méthode d'une instance de demande. Si le temps de réponse d'une instance de demande dépasse ce seuil, le collecteur de données collecte sa trace de méthode.	`minClockTrace`	Valeur en millisecondes
Nombre maximum d'événements par fichier	Indique le nombre maximal d'événements à enregistrer dans un fichier `.jso`. Le fichier `.jso` enregistre les données de diagnostic de ces événements.	`eventsPerFile`	Nombre maximum d'événements
Délai de signalement maximum dans un fichier	Indique la durée maximale d'enregistrement des données de diagnostic par le fichier `.jso`	`fileCommitTime`	Délai maximum en secondes

Tableau 187. Paramètres du collecteur de données (suite)

Catégorie de données de diagnostic	Description	Propriété	Action
Nombre maximum de fichiers à conserver avant de supprimer les plus anciens	Indique le nombre maximal de fichiers `.jso` à conserver avant que les anciens fichiers soient supprimés.	`maxFiles`	Nombre maximum de fichiers
Période d'échantillonnage des demandes	Indique la période d'échantillonnage des demandes.	`sampling`	Période d'échantillonnage considérée. La valeur par défaut est `10`. La valeur `10` indique que l'agent collecte une demande sur 10.

- Facultatif : Définissez la variable d'environnement *SECURITY_OFF* si vous voulez que le collecteur de données de diagnostic collecte les informations sensibles de l'utilisateur, telles que les cookies, les contextes de demande HTTP et les contextes de requête de base de données. Ces informations ne sont pas collectées par défaut.

  Soyez prudent lorsque vous définissez cette variable, car le processus peut entraîner une fuite des informations.

  Linux Par exemple, pour définir cette variable d'environnement, exécutez la commande suivante :

  ```
  export SECURITY_OFF=true
  ```

Résultats

La configuration du collecteur de données de diagnostic est modifiée pour l'application en cours d'exécution que vous avez spécifiée ou pour toutes les applications.

Configuration du collecteur de données Node.js autonome pour les applications IBM Cloud(anciennement Bluemix)

Pour collecter des informations concernant les applications Node.js sur IBM Cloud, vous devez configurer le collecteur de données Node.js autonome.

Avant de commencer

1. Assurez-vous que votre application Node.js peut s'exécuter avec succès localement. Le collecteur de données Node.js autonome peut surveiller les versions de Node.js 8.0.0 et groupes de correctifs à venir, 10.0.0 et groupes de correctifs à venir, et 12.0.0 et groupes de correctifs à venir.
2. Téléchargez le package du collecteur de données à partir du site Web IBM Marketplace. Pour des instructions détaillées, voir «Téléchargement de vos agents et de vos collecteurs de données», à la page 105.

Procédure

1. Extrayez les fichiers du package du collecteur de données. Le module `nodejs_datacollector_8.1.4.0.6.tgz` est inclus dans le répertoire extrait.
2. Extrayez le fichier `nodejs_datacollector_8.1.4.0.6.tgz`, par exemple, en exécutant la commande suivante :

   ```
   tar -zxf nodejs_datacollector_8.1.4.0.6.tgz
   ```

3. Extrayez le fichier `ibmapm.tgz` dans le dossier `nodejs_dc` en exécutant la commande suivante :

   ```
   tar -zxf nodejs_dc/ibmapm.tgz
   ```

   Vous obtiendrez un dossier `ibmapm`.
4. Copiez le dossier `ibmapm` qui est extrait du module de collecteur de données dans le répertoire de base de votre application, par exemple, en exécutant la commande suivante :

   ```
   cp –r répertoire_accès_au_dossier_ibmapm  répertoire_base_de_votre_application_Node.js
   ```

   Conseil : Le répertoire de base de votre application Node.js est déterminé par la commande que vous utilisez pour démarrer l'application Node.js et par le répertoire qui contient votre fichier principal. Si vous utilisez la commande **node app.js** pour démarrer votre application Node.js et si le fichier principal `app.js` se trouve dans le répertoire `/root/nodejs_app`, `/root/nodejs_app` est le répertoire de base de votre application.
5. Dans le fichier `package.json` de votre application Node.js, ajoutez la ligne suivante dans la section Dépendances :

   ```
   “ibmapm": "./ibmapm"
   ```

   A faire : veillez à inclure la virgule à la fin de chaque ligne du fichier, à l'exception de la dernière, et conservez la syntaxe correcte du fichier `package.json`.

   Exemple :

   ```
   "dependencies": {
      "ibmapm": "./ibmapm",
      "cors": "^2.5.2",
      "helmet": "^1.3.0",
      "loopback": "^2.22.0",
      "loopback-boot": "^2.6.5",
      "loopback-datasource-juggler": "^2.39.0",
      "serve-favicon": "^2.0.1",
      "strong-error-handler": "^1.0.1"
    }
   ```
6. Ajoutez la ligne suivante au début du fichier principal de l'application Node.js :

   ```
   require('ibmapm');
   ```

   Si vous démarrez votre application en exécutant la commande **node app.js**, `app.js` est le fichier principal de votre application.
7. A partir du répertoire qui contient le fichier `manifest.yml` de votre application Node.js, connectez-vous à IBM Cloud puis exécutez la commande suivante :

   ```
   cf push
   ```

   Conseil : Pour un fichier `manifest.yml` exemple, voir «Exemple de fichier manifest.yml», à la page 193.

Résultats
Le collecteur de données est configuré et il est connecté au serveur Cloud APM.

Que faire ensuite

Vous pouvez vérifier que les données de surveillance de votre application IBM Cloud sont affichées dans la console Cloud APM. Pour obtenir des instructions de démarrage de la console Cloud APM, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.

A faire : Pour ajouter votre application à la console Cloud APM, choisissez **Node.js Runtime** dans l'éditeur d'application.

Personnalisation du collecteur de données Node.js autonome pour les applications IBM Cloud
Vous pouvez ajouter des variables d'environnement dans l'interface utilisateur IBM Cloud pour personnaliser la surveillance de votre application IBM Cloud.

Variables d'environnement définies par l'utilisateur pour le collecteur de données Node.js

Vous pouvez utiliser les informations du tableau suivant pour personnaliser la surveillance Node.js sur IBM Cloud.

Tableau 188. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance Node.js sur IBM Cloud

Nom de la variable	Importance	Valeur	Description
KNJ_SAMPLING	Facultative	Nombre des demandes par échantillonnage	Le nombre de demandes sur la base duquel un échantillon est prélevé. La valeur par défaut est 10, ce qui signifie qu'une demande sur 10 est surveillée. Si vous ne définissez pas cette variable, la valeur par défaut 10 est utilisée.
KNJ_MIN_CLOCK_TRACE	Facultative	Seuil de temps de réponse pour collecter la trace de méthode, en millisecondes	Si le temps de réponse d'une instance de demande dépasse la valeur de cette variable, le collecteur de données collecte sa trace de méthode. La valeur par défaut est 0. Si vous ne définissez pas cette variable, la valeur par défaut 0 est utilisée.
KNJ_MIN_CLOCK_STACK	Facultative	Seuil de temps de réponse pour collecter la trace de pile, en millisecondes	Si le temps de réponse d'une instance de demande dépasse la valeur de cette variable, le collecteur de données collecte sa trace de pile. La valeur par défaut est 0. Si vous ne définissez pas cette variable, la valeur par défaut 0 est utilisée.

Tableau 188. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance Node.js sur IBM Cloud (suite)

Nom de la variable	Importance	Valeur	Description
KNJ_ENABLE_METHODTRACE	Facultative	• `True` • `False`	Active ou désactive la trace de méthode. • Si vous définissez cette variable sur true, la trace de méthode pour les demandes est désactivée. • Si vous définissez cette valeur sur false, la trace de méthode pour les demandes est activée. Il s'agit de la valeur par défaut. Si vous ne définissez pas cette variable, la valeur par défaut `False` est utilisée et la trace de méthode pour les demandes est activée.
KNJ_ENABLE_DEEPDIVE	Facultative	• `True` • `False`	Si vous définissez cette variable sur true, les données de diagnostic sont envoyées au serveur. Par défaut, cette valeur est définie sur false, ce qui signifie que les données de diagnostic ne sont pas envoyées au serveur.
KNJ_ENABLE_TT	Facultative	• `true` • `false`	Active ou désactive le suivi des transactions d'AAR. • Si vous définissez cette variable sur true, le suivi des transactions d'AAR est activé. • Si vous définissez cette variable sur false, le suivi des transactions d'AAR est désactivé. Par défaut, cette valeur n'est pas définie, ce qui signifie que le suivi des transactions est désactivé.

Tableau 188. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance Node.js sur IBM Cloud (suite)

Nom de la variable	Importance	Valeur	Description
KNJ_AAR_BATCH_FREQ	Facultative	Intervalle d'envoi des données AAR, en secondes	Indique l'intervalle auquel les données AAR sont envoyées par lot au serveur, en secondes. La valeur par défaut est de 60, ce qui signifie que les données AAR sont envoyées par lot au serveur toutes les minutes. **Remarque :** cette variable fonctionne avec KNJ_AAR_BATCH_COUNT pour déterminer quand les données AAR sont envoyées par lot au serveur. Si la condition définie par l'une des deux variables est remplie, les données AAR sont envoyées par lot. Si les demandes contenues dans les données AAR atteignent leur nombre maximal, par exemple 100, dans un délai plus court que celui défini, les données sont tout de même envoyées immédiatement par lot.
KNJ_AAR_BATCH_COUNT	Facultative	Nombre maximal de demandes pouvant être contenues dans un lot de données AAR	Indique le nombre maximal de demandes pouvant être contenues dans un lot de données AAR avant que ce lot ne soit envoyé au serveur. La valeur par défaut est de 100, ce qui signifie que lorsque le nombre de demandes pouvant être contenues dans un lot de données AAR atteint 100, ce lot de données AAR est envoyé au serveur.

Tableau 188. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance Node.js sur IBM Cloud (suite)

Nom de la variable	Importance	Valeur	Description
KNJ_LOG_LEVEL	Facultative	Niveau d'information imprimé dans le journal	Contrôle le niveau d'information imprimé dans le journal. Les niveaux suivants sont fournis : **off** Les journaux ne sont pas imprimés. **error** Les informations ne sont consignées qu'en cas d'erreur. **info** Les informations sont consignées lorsque le collecteur de données d'agent Node.js s'exécute normalement. Les données de surveillance brutes envoyées à l'agent sont également consignées. **debug** Les informations de niveau débogage, informations et erreur sont consignées dans le journal. Il peut s'agir notamment des données collectées, des données envoyées au serveur et de la réponse du serveur. **all** Toutes les informations sont consignées dans le journal. Par défaut, le niveau de consignation est `info`, ce qui signifie que les informations récapitulatives sur les actions du collecteur de données sont imprimées dans le journal. Les journaux sont imprimés dans la sortie standard.

Tableau 188. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance Node.js sur IBM Cloud (suite)

Nom de la variable	Importance	Valeur	Description
SECURITY_OFF	Facultative	• `true` • `false`	Active ou désactive la collecte des informations sensibles de l'utilisateur, telles que les cookies, le contexte de demande HTTP et le contexte de requête de base de données. • Si vous définissez cette variable sur true, les informations sensibles de l'utilisateur sont collectées. • Si vous définissez cette variable sur false, les informations sensibles de l'utilisateur ne sont pas collectées. Il s'agit de la valeur par défaut. Si vous ne spécifiez pas cette variable, la valeur par défaut `false` est utilisée et les informations sensibles de l'utilisateur ne sont pas collectées.

Annulation de la configuration du collecteur de données Node.js autonome pour les applications IBM Cloud

Si vous n'avez pas besoin de surveiller votre environnement Node.js ou si vous souhaitez mettre à niveau le collecteur de données Node.js autonome, vous devez d'abord annuler la configuration des paramètres précédents pour le collecteur de données Node.js autonome.

Procédure

1. Supprimez la ligne `require('ibmapm');` du fichier principal de l'application.

   Conseil : Si vous démarrez votre application en exécutant la commande **node app.js**, `app.js` est le fichier principal de votre application.
2. Supprimez les dépendances suivantes du fichier `package.json`.

   ```
   “ibmapm": "./ibmapm"
   ```

   A faire : Ne supprimez pas les dépendances dont votre application a besoin.
3. Supprimez le dossier `ibmapm` du répertoire de base de votre application.

Résultats

Vous avez correctement annulé la configuration du collecteur de données Node.js autonome.

Que faire ensuite

Une fois que vous avez configuré le collecteur de données, la console Cloud APM continue d'afficher le collecteur de données dans les applications auxquelles vous l'avez ajouté. La console Cloud APM indique qu'aucune donnée n'est disponible pour l'application et n'indique pas que le collecteur de données est hors ligne. Pour plus d'informations sur la manière de supprimer le collecteur de données d'applications et de groupes de ressources, voir «Suppression de collecteurs de données de la console Cloud APM», à la page 193.

Configuration du collecteur de données Node.js autonome pour les applications sur site

Si vous avez installé l'application Node.js dans un environnement sur site, vous devez configurer le collecteur de données Node.js pour qu'il collecte les informations la concernant.

Avant de commencer

1. Assurez-vous que votre application Node.js peut s'exécuter avec succès localement. Le collecteur de données Node.js autonome peut surveiller les versions de Node.js 8.0.0 et groupes de correctifs à venir, 10.0.0 et groupes de correctifs à venir, et 12.0.0 et groupes de correctifs à venir.
2. Téléchargez le package du collecteur de données à partir du site Web IBM Marketplace. Pour des instructions détaillées, voir «Téléchargement de vos agents et de vos collecteurs de données», à la page 105.

Procédure

1. Extrayez les fichiers du package du collecteur de données. Le module `nodejs_datacollector_8.1.4.0.6.tgz` est inclus dans le répertoire extrait.
2. Déterminez le répertoire de base de votre application.
   - Pour les applications Node.js type, si vous utilisez la commande **`node app.js`** pour démarrer votre application Node.js et que le fichier principal `app.js` se trouve dans le répertoire `/root/nodejs_app`, `/root/nodejs_app` est le répertoire de base de votre application.
   - Pour les membres de collectivité dans l'environnement IBM API Connect, exécutez la commande **`wlpn-server list`** pour afficher la liste de tous les membres de collectivité sur la même machine. Le répertoire de base de votre membre de collectivité est au format suivant :

     ```
     répertoire_utilisateur/nom_membre-collectivité/package
     ```

     Par exemple, si vous obtenez `/root/wlpn/rock-8345a96-148538-1/package` comme sortie de commande, `/root/wlpn` est le répertoire utilisateur et `rock-8345a96-148538-1` est le nom de membre de collectivité.
   - Pour les applications Developer Portal dans l'environnement IBM API Connect, vous pouvez exécuter la commande **`ps -ef | grep node`** pour rechercher le répertoire de base. Si vous obtenez la sortie de commande suivante, par exemple, le répertoire de base est `/home/admin/bgsync` et le fichier principal de votre application est `rest_server.js` :

     ```
     admin 19085 1 0 Jun25 ?  00:06:53 /usr/local/bin/node /home/admin/bgsync/
     rest_server.js
     ```
3. A partir du répertoire de base de votre application, exécutez la commande suivante pour extraire les fichiers du module de collecteur de données :

   ```
   tar -zxf nodejs_datacollector_8.1.4.0.6.tgz
   ```
4. Extrayez le fichier `ibmapm.tgz` dans le dossier `nodejs_dc` en exécutant la commande suivante :

   ```
   tar -zxf nodejs_dc/ibmapm.tgz
   ```

   Vous obtiendrez un dossier `ibmapm`.
5. Exécutez la commande suivante pour installer le collecteur de données dans votre application :

   ```
   npm install ./ibmapm
   ```
6. Ajoutez la ligne suivante au début du fichier principal de l'application Node.js :

   ```
   require('ibmapm');
   ```
   - Si vous démarrez votre application en exécutant la commande **`node app.js`**, `app.js` est le fichier principal de votre application.

- Pour les membres de collectivité dans l'environnement IBM API Connect, le fichier principal est défini dans le fichier `package.json` dans le répertoire de base ou ses sous-dossiers. Par défaut, le fichier principal est *répertoire_base*`/server/server.js`, où *répertoire_base* est le répertoire de base de votre membre de collectivité.
- Pour les applications Developer Portal dans l'environnement IBM API Connect, vous pouvez exécuter la commande **`ps -ef | grep node`** pour rechercher le fichier principal. Si vous obtenez la sortie de commande suivante, par exemple, le fichier principal de votre application est `rest_server.js`.

```
admin 19085 1 0 Jun25 ?  00:06:53 /usr/local/bin/node /home/admin/bgsync/
rest_server.js
```

7. Redémarrez votre application.

   Conseil :

   - Pour redémarrer votre membre de collectivité, exécutez la commande `wlpn-server stop` *`nom_membre_collectivité`*. Le membre de collectivité redémarre automatiquement après l'exécution de cette commande. S'il ne démarre pas, exécutez la commande `wlpn-server start` *`nom_membre_collectivité`* pour le redémarrer manuellement.
   - Pour redémarrer vos applications Developer Portal, exécutez d'abord la commande `/etc/init.d/restservice stop` pour arrêter l'application, puis la commande `/etc/init.d/restservice start` pour la démarrer.

Résultats
Le collecteur de données est configuré et il est connecté au serveur Cloud APM.

Que faire ensuite

- Vous pouvez vérifier que les données de surveillance de votre application sont affichées dans la console Cloud APM. Pour obtenir des instructions de démarrage de la console Cloud APM, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.
- Pour afficher les informations de topologie pour votre environnement API Connect, activez le suivi des transactions. Pour plus d'instructions, consultez la description de la variable *KNJ_ENABLE_TT* dans «Personnalisation du collecteur de données Node.js pour les applications sur site», à la page 616.

A faire : Pour ajouter votre application à la console Cloud APM, choisissez **Node.js Runtime** dans l'éditeur d'application.

Personnalisation du collecteur de données Node.js pour les applications sur site
En modifiant des fichiers dans le module de collecteur de données, vous pouvez définir les variables d'environnement de façon à personnaliser la surveillance pour votre application Node.js.

Vous pouvez définir les variables en personnalisant les variables d'environnement ou en modifiant le fichier `config.properties`. Ce dernier se trouve dans le dossier `ibmapm/etc` où votre collecteur de données Node.js est installé.

Tableau 189. Variables prises en charge

Nom de la variable	Importance	Valeur	Description
KNJ_SAMPLING	Facultative	Nombre des demandes par échantillonnage	Le nombre de demandes sur la base duquel un échantillon est prélevé. La valeur par défaut est `10`, ce qui signifie qu'une demande sur 10 est surveillée. Si vous ne définissez pas cette variable, la valeur par défaut `10` est utilisée.
KNJ_MIN_CLOCK_TRACE	Facultative	Seuil de temps de réponse pour collecter la trace de méthode, en millisecondes	Si le temps de réponse d'une instance de demande dépasse la valeur de cette variable, le collecteur de données collecte sa trace de méthode. La valeur par défaut est `0`. Si vous ne définissez pas cette variable, la valeur par défaut `0` est utilisée.
KNJ_MIN_CLOCK_STACK	Facultative	Seuil de temps de réponse pour collecter la trace de pile, en millisecondes	Si le temps de réponse d'une instance de demande dépasse la valeur de cette variable, le collecteur de données collecte sa trace de pile. La valeur par défaut est `0`. Si vous ne définissez pas cette variable, la valeur par défaut `0` est utilisée.
KNJ_ENABLE_METHODTRACE	Facultative	• `True` • `False`	Active ou désactive la trace de méthode. • Si vous définissez cette variable sur true, la trace de méthode pour les demandes est désactivée. • Si vous définissez cette valeur sur false, la trace de méthode pour les demandes est activée. Il s'agit de la valeur par défaut. Si vous ne définissez pas cette variable, la valeur par défaut `False` est utilisée et la trace de méthode pour les demandes est activée.
KNJ_ENABLE_DEEPDIVE	Facultative	• `True` • `False`	Si vous définissez cette variable sur true, les données de diagnostic sont envoyées au serveur. Par défaut, cette valeur est définie sur false, ce qui signifie que les données de diagnostic ne sont pas envoyées au serveur.

Tableau 189. Variables prises en charge (suite)

Nom de la variable	Importance	Valeur	Description
KNJ_ENABLE_TT	Facultative	• `true` • `false`	Active ou désactive le suivi des transactions d'AAR. • Si vous définissez cette variable sur true, le suivi des transactions d'AAR est activé. • Si vous définissez cette variable sur false, le suivi des transactions d'AAR est désactivé. Par défaut, cette valeur n'est pas définie, ce qui signifie que le suivi des transactions est désactivé.
KNJ_AAR_BATCH_FREQ	Facultative	Intervalle d'envoi des données AAR, en secondes	Indique l'intervalle auquel les données AAR sont envoyées par lot au serveur, en secondes. La valeur par défaut est de 60, ce qui signifie que les données AAR sont envoyées par lot au serveur toutes les minutes. **Remarque :** Cette variable fonctionne avec KNJ_AAR_BATCH_COUNT pour déterminer quand les données AAR sont envoyées par lot au serveur. Si la condition définie par l'une des deux variables est remplie, les données AAR sont envoyées par lot. Si les demandes contenues dans les données AAR atteignent leur nombre maximal, par exemple 100, dans un délai plus court que celui défini, les données sont tout de même envoyées immédiatement par lot.
KNJ_AAR_BATCH_COUNT	Facultative	Nombre maximal de demandes pouvant être contenues dans un lot de données AAR	Indique le nombre maximal de demandes pouvant être contenues dans un lot de données AAR avant que ce lot ne soit envoyé au serveur. La valeur par défaut est de 100, ce qui signifie que lorsque le nombre de demandes pouvant être contenues dans un lot de données AAR atteint 100, ce lot de données AAR est envoyé au serveur.

Tableau 189. Variables prises en charge (suite)

Nom de la variable	Importance	Valeur	Description
KNJ_LOG_LEVEL	Facultative	Niveau d'information imprimé dans le journal	Contrôle le niveau d'information imprimé dans le journal. Les niveaux suivants sont fournis : **off** Les journaux ne sont pas imprimés. **error** Les informations ne sont consignées qu'en cas d'erreur. **info** Les informations sont consignées lorsque le collecteur de données d'agent Node.js s'exécute normalement. Les données de surveillance brutes envoyées à l'agent sont également consignées. **debug** Les informations de niveau débogage, informations et erreur sont consignées dans le journal. Il peut s'agir notamment des données collectées, des données envoyées au serveur et de la réponse du serveur. **all** Toutes les informations sont consignées dans le journal. Par défaut, le niveau de consignation est `info`, ce qui signifie que les informations récapitulatives sur les actions du collecteur de données sont imprimées dans le journal. Les journaux sont imprimés dans la sortie standard.

Tableau 189. Variables prises en charge (suite)			
Nom de la variable	**Importance**	**Valeur**	**Description**
SECURITY_OFF	Facultative	• `true` • `false`	Active ou désactive la collecte des informations sensibles de l'utilisateur, telles que les cookies, le contexte de demande HTTP et le contexte de requête de base de données. • Si vous définissez cette variable sur true, les informations sensibles de l'utilisateur sont collectées. • Si vous définissez cette variable sur false, les informations sensibles de l'utilisateur ne sont pas collectées. Il s'agit de la valeur par défaut. Si vous ne spécifiez pas cette variable, la valeur par défaut `false` est utilisée et les informations sensibles de l'utilisateur ne sont pas collectées.

Annulation de la configuration du collecteur de données Node.js autonome pour les applications sur site

Si vous n'avez pas besoin de surveiller votre environnement Node.js ou si vous souhaitez mettre à niveau le collecteur de données Node.js autonome, vous devez d'abord annuler la configuration des paramètres précédents pour le collecteur de données Node.js autonome.

Procédure

1. Supprimez la ligne `require('ibmapm');` du fichier principal de l'application.

   Conseil : Si vous démarrez votre application en exécutant la commande **node app.js**, `app.js` est le fichier principal de votre application.
2. Supprimez `"ibmapm": "./ibmapm"` de la section de dépendances dans le fichier `package.json` de votre application Node.js.
3. Supprimez le dossier `node_modules` du répertoire de base de votre application.
4. Exécutez la commande `npm install` pour installer les dépendances de l'application.

Résultats

Vous avez correctement annulé la configuration du collecteur de données Node.js autonome.

Que faire ensuite

Une fois que vous avez configuré le collecteur de données, la console Cloud APM continue d'afficher le collecteur de données dans les applications auxquelles vous l'avez ajouté. La console Cloud APM indique qu'aucune donnée n'est disponible pour l'application et n'indique pas que le collecteur de données est hors ligne. Pour plus d'informations sur la manière de supprimer le collecteur de données d'applications et de groupes de ressources, voir «Suppression de collecteurs de données de la console Cloud APM», à la page 193.

Configuration du collecteur de données Node.js autonome pour les applications Kubernetes

Si vous avez installé l'application Node.js sur Kubernetes, vous pouvez configurer le collecteur de données Node.js pour qu'il collecte les informations relatives à cette application.

Avant de commencer

1. Assurez-vous que votre application Node.js peut s'exécuter correctement. Le collecteur de données Node.js autonome peut surveiller les versions de Node.js 8.0.0 et groupes de correctifs à venir, 10.0.0 et groupes de correctifs à venir, et 12.0.0 et groupes de correctifs à venir.
2. Téléchargez le package du collecteur de données à partir du site Web IBM Marketplace. Pour des instructions détaillées, voir «Téléchargement de vos agents et de vos collecteurs de données», à la page 105.

Procédure

1. Extrayez les fichiers du package du collecteur de données. Le module `nodejs_datacollector_8.1.4.0.6.tgz` est inclus dans le répertoire extrait.
2. Extrayez le fichier `nodejs_datacollector_8.1.4.0.6.tgz`, par exemple, en exécutant la commande suivante :

   ```
   tar -zxf nodejs_datacollector_8.1.4.0.6.tgz
   ```

3. Extrayez le fichier `ibmapm.tgz` dans le dossier `nodejs_dc` en exécutant la commande suivante :

   ```
   tar -zxf nodejs_dc/ibmapm.tgz
   ```

   Vous obtiendrez un dossier `ibmapm`.
4. Dans le fichier `package.json` de votre application Node.js, ajoutez la ligne suivante dans la section Dépendances :

   ```
   "ibmapm": "./ibmapm"
   ```

   A faire : veillez à inclure la virgule à la fin de chaque ligne du fichier, à l'exception de la dernière, et conservez la syntaxe correcte du fichier `package.json`.
5. Ajoutez la ligne suivante au début du fichier principal de l'application Node.js :

   ```
   require('./ibmapm');
   ```

   Si vous démarrez votre application en exécutant la commande **node app.js**, `app.js` est le fichier principal de votre application.
6. Régénérez votre image docker.

   Remarque : Si vous avez exécuté votre application Node.js dans d'autres environnements Docker, tels que Docker Swarm ou AWS Docker, vous devez "dockeriser" les étapes.

Que faire ensuite

Pour personnaliser la surveillance, vous pouvez ajouter des variables d'environnement dans votre fichier yaml de déploiement. Pour plus d'informations, voir «Personnalisation du collecteur de données Node.js autonome pour les applications Kubernetes», à la page 621.

Personnalisation du collecteur de données Node.js autonome pour les applications Kubernetes

Vous pouvez ajouter des variables d'environnement au fichier yaml de déploiement afin de personnaliser la surveillance de votre application Kubernetes.

Variables d'environnement définies par l'utilisateur pour le collecteur de données Node.js

Vous pouvez utiliser les informations du tableau suivant pour personnaliser la surveillance de Node.js sur Kubernetes.

Tableau 190. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance de Node.js sur Kubernetes

Nom de la variable	Importance	Valeur	Description
KNJ_SAMPLING	Facultative	Nombre des demandes par échantillonnage	Le nombre de demandes sur la base duquel un échantillon est prélevé. La valeur par défaut est `10`, ce qui signifie qu'une demande sur 10 est surveillée. Si vous ne définissez pas cette variable, la valeur par défaut `10` est utilisée.
KNJ_MIN_CLOCK_TRACE	Facultative	Seuil de temps de réponse pour collecter la trace de méthode, en millisecondes	Si le temps de réponse d'une instance de demande dépasse la valeur de cette variable, le collecteur de données collecte sa trace de méthode. La valeur par défaut est `0`. Si vous ne définissez pas cette variable, la valeur par défaut `0` est utilisée.
KNJ_MIN_CLOCK_STACK	Facultative	Seuil de temps de réponse pour collecter la trace de pile, en millisecondes	Si le temps de réponse d'une instance de demande dépasse la valeur de cette variable, le collecteur de données collecte sa trace de pile. La valeur par défaut est `0`. Si vous ne définissez pas cette variable, la valeur par défaut `0` est utilisée.
KNJ_ENABLE_METHODTRACE	Facultative	• `True` • `False`	Active ou désactive la trace de méthode. • Si vous définissez cette variable sur true, la trace de méthode pour les demandes est désactivée. • Si vous définissez cette valeur sur false, la trace de méthode pour les demandes est activée. Il s'agit de la valeur par défaut. Si vous ne définissez pas cette variable, la valeur par défaut `False` est utilisée et la trace de méthode pour les demandes est activée.
KNJ_ENABLE_DEEPDIVE	Facultative	• `True` • `False`	Si vous définissez cette variable sur true, les données de diagnostic sont envoyées au serveur. Par défaut, cette valeur est définie sur false, ce qui signifie que les données de diagnostic ne sont pas envoyées au serveur.

Tableau 190. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance de Node.js sur Kubernetes (suite)

Nom de la variable	Importance	Valeur	Description
KNJ_ENABLE_TT	Facultative	• `true` • `false`	Active ou désactive le suivi des transactions d'AAR. • Si vous définissez cette variable sur true, le suivi des transactions d'AAR est activé. • Si vous définissez cette variable sur false, le suivi des transactions d'AAR est désactivé. Par défaut, cette valeur n'est pas définie, ce qui signifie que le suivi des transactions est désactivé.
KNJ_AAR_BATCH_FREQ	Facultative	Intervalle d'envoi des données AAR, en secondes	Indique l'intervalle auquel les données AAR sont envoyées par lot au serveur, en secondes. La valeur par défaut est de 60, ce qui signifie que les données AAR sont envoyées par lot au serveur toutes les minutes. **Remarque :** cette variable fonctionne avec KNJ_AAR_BATCH_COUNT pour déterminer quand les données AAR sont envoyées par lot au serveur. Si la condition définie par l'une des deux variables est remplie, les données AAR sont envoyées par lot. Si les demandes contenues dans les données AAR atteignent leur nombre maximal, par exemple 100, dans un délai plus court que celui défini, les données sont tout de même envoyées immédiatement par lot.
KNJ_AAR_BATCH_COUNT	Facultative	Nombre maximal de demandes pouvant être contenues dans un lot de données AAR	Indique le nombre maximal de demandes pouvant être contenues dans un lot de données AAR avant que ce lot ne soit envoyé au serveur. La valeur par défaut est de 100, ce qui signifie que lorsque le nombre de demandes pouvant être contenues dans un lot de données AAR atteint 100, ce lot de données AAR est envoyé au serveur.

Tableau 190. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance de Node.js sur Kubernetes (suite)

Nom de la variable	Importance	Valeur	Description
KNJ_LOG_LEVEL	Facultative	Niveau d'information imprimé dans le journal	Contrôle le niveau d'information imprimé dans le journal. Les niveaux suivants sont fournis : **off** Les journaux ne sont pas imprimés. **error** Les informations ne sont consignées qu'en cas d'erreur. **info** Les informations sont consignées lorsque le collecteur de données d'agent Node.js s'exécute normalement. Les données de surveillance brutes envoyées à l'agent sont également consignées. **debug** Les informations de niveau débogage, informations et erreur sont consignées dans le journal. Il peut s'agir notamment des données collectées, des données envoyées au serveur et de la réponse du serveur. **all** Toutes les informations sont consignées dans le journal. Par défaut, le niveau de consignation est `info`, ce qui signifie que les informations récapitulatives sur les actions du collecteur de données sont imprimées dans le journal. Les journaux sont imprimés dans la sortie standard.

Tableau 190. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance de Node.js sur Kubernetes (suite)

Nom de la variable	Importance	Valeur	Description
SECURITY_OFF	Facultative	• `true` • `false`	Active ou désactive la collecte des informations sensibles de l'utilisateur, telles que les cookies, le contexte de demande HTTP et le contexte de requête de base de données. • Si vous définissez cette variable sur true, les informations sensibles de l'utilisateur sont collectées. • Si vous définissez cette variable sur false, les informations sensibles de l'utilisateur ne sont pas collectées. Il s'agit de la valeur par défaut. Si vous ne spécifiez pas cette variable, la valeur par défaut `false` est utilisée et les informations sensibles de l'utilisateur ne sont pas collectées.

Exemple de fichier yaml

```
spec:
      containers:
      - name: testapp
        image: mycluster.icp:8500/default/testapp:v1
        imagePullPolicy: Always
        ports:
        - containerPort: 3000
          protocol: TCP
        env:
        - name: KNJ_LOG_LEVEL
          value: "debug"
        - name: KNJ_ENABLE_TT
          value: "true"
        - name: KNJ_ENABLE_DEEPDIVE
          value: "true"
```

Annulation de la configuration du collecteur de données Node.js autonome pour les applications Kubernetes

Si vous n'avez pas besoin de surveiller votre environnement Node.js ou si vous souhaitez mettre à niveau le collecteur de données Node.js autonome, vous devez d'abord annuler la configuration des paramètres précédents pour le collecteur de données Node.js autonome.

Procédure

1. Supprimez la ligne `require('ibmapm');` du fichier principal de l'application.

   Conseil : Si vous démarrez votre application en exécutant la commande **node app.js**, `app.js` est le fichier principal de votre application.
2. Supprimez les dépendances suivantes du fichier `package.json`.

   ```
   "ibmapm": "./ibmapm"
   ```

   A faire : Ne supprimez pas les dépendances dont votre application a besoin.

Résultats
Vous avez correctement annulé la configuration du collecteur de données Node.js autonome.

Que faire ensuite
Une fois que vous avez configuré le collecteur de données, la console Cloud APM continue d'afficher le collecteur de données dans les applications auxquelles vous l'avez ajouté. La console Cloud APM indique qu'aucune donnée n'est disponible pour l'application et n'indique pas que le collecteur de données est hors ligne. Pour plus d'informations sur la manière de supprimer le collecteur de données d'applications et de groupes de ressources, voir «Suppression de collecteurs de données de la console Cloud APM», à la page 193.

Configuration de la surveillance d'OpenStack

Vous devez configurer Monitoring Agent for OpenStack pour qu'il puisse surveiller automatiquement l'environnement de l'Agent OpenStack.

Procédure

1. Configurez l'agent en répondant aux invites. Pour obtenir des instructions, voir «Configuration de l'Agent OpenStack», à la page 626.
2. Si vous voulez collecter des informations sur le processus, configurez le collecteur de données de l'Agent OpenStack. Pour plus d'informations, voir «Activation de la collecte des informations liées aux processus et des connexions SSH», à la page 628.
3. Entrez les valeurs de configuration pour que l'agent fonctionne. Pour obtenir des instructions, voir «Ajout des valeurs de configuration», à la page 630.

Configuration de l'Agent OpenStack

Pour un environnement type, si vous souhaitez que l'Agent OpenStack surveille automatiquement l'environnement OpenStack, vous devez configurer l'agent au préalable.

Avant de commencer
Assurez-vous d'avoir installé tous les logiciels requis, comme décrit dans la rubrique Préinstallation sur des systèmes Linux.

Procédure

Vous avez deux options pour configurer l'Agent OpenStack sur un système Linux :

- Pour configurer l'agent en exécutant le script et en répondant aux invites, voir «Configuration interactive», à la page 626.
- Pour configurer l'agent en éditant le fichier de réponses silencieux et en exécutant le script sans interaction, voir «Configuration en mode silencieux», à la page 627.

Configuration interactive

Procédure

1. Pour configurer l'agent, exécutez la commande suivante :

   ```
   rép_install/bin/openstack-agent.sh config nom_instance
   ```

   où *rép_install* représente le répertoire d'installation de votre Agent OpenStack. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.
2. Lorsque vous êtes invité à `entrer le nom d'instance`, spécifiez un nom d'instance.

   Important : L'Agent OpenStack est un agent à plusieurs instances et nécessite un nom d'instance pour chaque instance d'agent. Le nom d'instance que vous indiquez est inclus dans le nom de système

géré nom_instance:nom_hôte:sg. La longueur du nom d'instance que vous indiquez est limitée à 28 caractères sans la longueur de votre nom d'hôte. Par exemple, si vous indiquez OS1 comme nom d'instance, votre nom de système géré est OS1:nom_hôte:SG.

3. A l'invite Edit Monitoring Agent for OpenStack, appuyez sur Entrée pour continuer.
4. A l'invite Edit OpenStack environment authentication information, fournissez les informations suivantes :

```
OpenStack authentication url (default is: http://localhost:identity/v3):
OpenStack username (default is: admin):
Enter OpenStack password (default is: ):
Re-type: OpenStack password (default is: ):
OpenStack tenant name (default is: admin):
```

5. Lorsque le programme vous demande l'emplacement de l'exécutable Python, indiquez cet emplacement, par exemple /usr/bin/python.

   Vous pouvez trouver le chemin complet en exécutant la commande suivante dans votre environnement :

```
which python
```

6. Lorsque le programme vous demande le numéro de port, acceptez la valeur par défaut ou indiquez un numéro de port.

   Ce port sert à surveiller la communication interne entre le collecteur de données de l'Agent OpenStack et l'Agent OpenStack, qui sont installés seulement sur un serveur local. L'agent est en mode écoute sur ce port pour rechercher les données du collecteur de données. La valeur par défaut de 0 indique qu'un port éphémère est utilisé quand l'agent démarre. Sur un serveur avec des règles de sécurité strictes sur des ports, vous pouvez configurer un port spécifique pour que l'agent l'utilise. Ce port est réservé à l'usage interne par l'agent et n'est pas lié à l'environnement OpenStack.
7. Editez le fichier /etc/hosts sur votre système pour ajouter le mappage hôte de chaque noeud surveillé.

Configuration en mode silencieux

Procédure

1. Ouvrez le fichier sg_silent_config.txt dans un éditeur de texte. Ce fichier se trouve dans le répertoire *rép_install*/samples, où *rép_install* est le répertoire d'installation de l'Agent OpenStack.
2. Editez le fichier de configuration sg_silent_config.txt de l'Agent OpenStack.
3. Indiquez les valeurs des paramètres identifiés dans le fichier. Le fichier de réponses contient les commentaires qui définissent les paramètres disponibles et les valeurs à indiquer.
4. Sauvegardez le fichier et quittez l'application.
5. Editez le fichier /etc/hosts sur votre système pour ajouter le mappage hôte de chaque noeud surveillé.
6. A partir du répertoire *rép_install*/samples, exécutez la commande suivante pour configurer l'agent :

```
rép_install/bin/openstack-agent.sh config nom_instance chemin_fichier_réponses
```

   où *rép_instance* est le nom de l'instance à configurer et *chemin_fichier_réponses* le chemin d'accès complet au fichier de réponses silencieux. Définissez un chemin absolu vers ce fichier.

   Par exemple, si le fichier de réponses se trouve dans le répertoire par défaut, lancez la commande suivante.

```
/opt/ibm/apm/agent/bin/openstack-agent.sh config nom_instance
/opt/ibm/apm/agent/samples/sg_silent_config.txt
```

Résultats
L'agent est configuré.

Que faire ensuite

- Après la configuration de l'agent, vous pouvez démarrer l'instance d'agent en exécutant la commande :

  ```
  rép_install/bin/openstack-agent.sh start nom_instance
  ```

  où *nom_instance* représente le nom de l'instance d'agent à configurer.
- Pour connecter l'Agent OpenStack à un environnement OpenStack activé pour SSL, spécifiez le répertoire du certificat SSL de votre serveur OpenStack en définissant la variable suivante :

  ```
  OS_cert_path=répertoire du fichier certificate.crt
  ```

  La variable OS_cert_path se trouve dans la section OS_authentication_info du fichier ksg_dc_*nom_instance*.cfg.
- Si vous souhaitez collecter des informations sur le processus, configurez le collecteur de données de l'Agent OpenStack en effectuant les étapes de la rubrique «Activation de la collecte des informations liées aux processus et des connexions SSH», à la page 628.
- Si vous souhaitez modifier le niveau de trace de l'agent à des fins d'identification et de résolution des problèmes, éditez la valeur de la variable **KBB_RAS1** dans le fichier *rép_install*/config/sg.environment en suivant les instructions du fichier.

Activation de la collecte des informations liées aux processus et des connexions SSH

Si vous souhaitez collecter des informations sur le processus, configurez le collecteur de données d'agent pour l'Agent OpenStack et configurez les connexions SSH avec le serveur de composant OpenStack cible.

Pourquoi et quand exécuter cette tâche
Vous devez configurer une connexion SSH pour collecter des informations avant de démarrer l'Agent OpenStack. Pour configurer la connexion, utilisez l'outil d'assistance **ksg_setup_key.sh** ou **ksg_ssh_setup.py** fourni par le produit et décrit dans la procédure ci-après.

Si vous êtes habitué aux connexions SSH, vous pouvez également utiliser les commandes Linux **ssh-keygen** et **ssh-copy-id** pour configurer la connexion.

Procédure

1. Accédez au répertoire *rép_install*/config, où *rép_install* est le répertoire d'installation de l'agent.
2. Editez le fichier ksg_dc_*nom_instance*.cfg où *nom_instance* est le nom spécifié pour l'instance d'agent.

   Le fichier est créé après le démarrage de l'instance d'agent. Si le fichier n'existe pas, copiez *rép_install*/lx8266/sg/bin/ksg_dc.cfg dans le répertoire *rép_install*/config et renommez le fichier ksg_dc_*nom_instance*.cfg.

   Par exemple, si le nom d'instance est OS1, changez le nom en ksg_dc_OS1.cfg.
3. Dans le fichier ksg_dc_ *nom_instance* .cfg, définissez la valeur du paramètre **collect_process_information** sur YES.
4. Dans la section **OS_process_collection**, spécifiez la valeur du paramètre **ssh_user_host** avec les utilisateurs et les noms d'hôte ou adresses IP des serveurs de composant OpenStack, en respectant le format de l'exemple suivant :

   ```
   ssh_user_host=root@9.112.250.248,user1@hostname
   ```
5. Sauvegardez les paramètres.
6. Pour que les paramètres soient pris en compte, redémarrez l'instance d'agent en exécutant les commandes suivantes :

```
rép_install/bin/openstack-agent.sh stop nom_instance
rép_install/bin/openstack-agent.sh start nom_instance
```

7. Configurez les connexions SSH avec le serveur de composant cible à l'aide d'une des méthodes suivantes :

   - Configurez les connexions une par une à l'aide du script `ksg_setup_key.sh` : accédez au répertoire *rép_install*`/lx8266/sg/bin` et exécutez le script `ksg_setup_key.sh` avec le nom d'hôte ou l'adresse IP et l'utilisateur pour établir les connexions SSH avec les serveurs de composant spécifiés à l'étape 4. Si vous suivez l'exemple de l'étape 4, vous devez exécuter le script deux fois pour configurer les connexions une par une :

     ```
     ./ksg_setup_key.sh 9.112.250.248 root
     ./ksg_setup_key.sh hostname user1
     ```

     Remarque : Vous devez fournir les mots de passe quand vous exécutez les scripts pour la première fois. Vous n'avez pas besoin de fournir de nouveau les mots de passe.

   - Configurez les connexions une par une dans un travail par lots, à l'aide de l'outil `ksg_ssh_setup.py` fourni par l'Agent OpenStack dans le répertoire *rép_install*`/lx8266/sg/bin`. Vous devez installer la bibliothèque Python pexpect avant d'utiliser cet outil.

     – Pour configurer les connexions SSH une par une, exécutez la commande :

       ```
       python ksg_ssh_setup.py -single
       ```

       Cette commande vous aide à configurer la connexion SSH au serveur cible distant. Vous devez fournir les informations suivantes :

       ```
       Entrez
       le nom d'hôte ou l'adresse IP de la machine cible distante : (entrez
       'END' pour terminer l'entrée.)
       Entrez le compte pour accéder à la machine distante (par exemple
       superutilisateur) :
       Entrez le mot de passe de l'utilisateur ci-dessus
       :
       ```

     – Pour configurer des connexions de SSH dans un travail par lots, exécutez la commande :

       ```
       python ksg_ssh_setup.py -ssh
       fichier_SSH
       ```

       où *fichier_SSH* est le fichier qui contient le serveur cible, l'utilisateur et le mot de passe. Vous devez créer le fichier selon le fichier `ksg_dc_ssh_list.txt` dans le même répertoire que l'outil Python, puis indiquer l'hôte et les informations utilisateur dans le fichier selon le format des exemples :

       ```
       hostname root passw0rd
       9.112.250.248 user1 passw0rd
       ```

   Remarque : vous devez les configurer de nouveau seulement en cas de changement de nom d'utilisateur ou de mot de passe pour le serveur cible. Vous n'avez pas besoin de configurer de nouveau les connexions après avoir redémarré l'agent ou changé la configuration de l'agent.

Résultats

Le collecteur de données est configuré et les connexions SSH sont configurées correctement. Vous pouvez à présent vous connecter à la console Cloud APM et utiliser l'éditeur d'applications pour ajouter l'instance de l'Agent OpenStack au tableau de bord des performances des applications. Lorsque vous ajoutez l'instance d'agent, sélectionnez **Environnement OpenStack** dans la liste des composants.

Que faire ensuite

- Lorsque vous cliquez sur **API End Point Summary By Sevice Type** > **Détails de noeuds finals d'API**, un message `Aucune donnée disponible` apparaît dans les widgets de groupe **Historique du**

nombre d'échecs de détection d'API et **Historique du pourcentage d'échecs de détection d'API**. Cliquez sur un noeud final d'API qui apparaît dans **Détails de noeuds finals d'API** pour afficher les données de surveillance dans les deux widgets de groupe.

- Lorsque vous cliquez sur **Récapitulatif des processus par composant** > **Détails de processus** ou **Statut de la connexion au serveur SSH** > **Détails de processus**, un message `Aucune donnée disponible` apparaît dans les widgets de groupe **Historique d'utilisation de l'UC par les processus** et **Historique d'utilisation de la mémoire par les processus**. Cliquez sur un processus qui apparaît dans **Détails de processus** pour afficher les données de surveillance dans les deux widgets de groupe.

Ajout des valeurs de configuration

Vous devez fournir les valeurs des configurations locale et distante nécessaires au fonctionnement de l'agent.

Si vous utilisez le mode interactif pour configurer l'agent, un panneau est affiché pour que vous puissiez entrer chaque valeur. S'il existe une valeur par défaut, celle-ci figure déjà dans la zone. Si une zone représente un mot de passe, deux zones de saisie s'affichent. Vous devez entrer la même valeur dans chaque zone. Les valeurs que vous entrez ne s'affichent pas de manière à préserver la sécurité de ces valeurs.

Si vous utilisez le mode silencieux pour configurer l'agent, vous pouvez éditer le fichier *fichier_réponses* dans le répertoire *rép_install*`/samples` pour ajouter les valeurs de configuration. Une fois que vous avez sauvegardé les modifications, suivez les instructions de l'étape «6», à la page 627 et exécutez la commande suivante pour que les modifications soient appliquées :

```
rép_install/bin/openstack-agent.sh start nom_instance
```

où *nom_instance* représente le nom de l'instance d'agent à configurer.

Une fois la configuration terminée, vous trouverez les valeurs configurées dans le fichier `.cfg` de l'instance d'agent, par exemple, *nom_hôte*`_sg_`*nom_instance*`.cfg`.

La configuration de cet agent est organisée en groupes :

Informations d'authentification d'environnement OpenStack (OPENSTACK_CONNECTION)
Informations d'authentification d'environnement OpenStack

Les éléments de configuration définis dans ce groupe figurent toujours dans la configuration de l'agent.

Ce groupe définit des informations qui s'appliquent à l'ensemble de l'agent.

URL d'authentification OpenStack (KSG_OPENSTACK_AUTH_URL)
auth_url de l'environnement OpenStack

Type : chaîne.

Cette valeur est requise.

Valeur par défaut : `http://localhost:identity/v3`

Mot de passe OpenStack (KSG_OPENSTACK_PASSWORD)
Mot de passe de l'administrateur

Type : mot de passe.

Cette valeur est requise.

Valeur par défaut : Néant

Nom du titulaire OpenStack (KSG_OPENSTACK_TENANT_NAME)
Nom du titulaire OpenStack, également connu comme nom de projet

Type : chaîne.

Cette valeur est requise.

Valeur par défaut : admin

Nom d'utilisateur OpenStack (KSG_OPENSTACK_USERNAME)
Administrateur devant se connecter à l'environnement OpenStack

Type : chaîne.

Cette valeur est requise.

Valeur par défaut : admin

Python (KSG_PYTHON)
Emplacement de l'exécutable Python

Les éléments de configuration définis dans ce groupe figurent toujours dans la configuration de l'agent.

Ce groupe définit des informations qui s'appliquent à l'ensemble de l'agent.

Emplacement de l'exécutable Python (KSG_PYTHON_LOCATION)
Exécutable Python qui sera utilisé pour exécuter le collecteur de données de l'agent OpenStack. Vous pouvez rechercher le chemin complet en exécutant la commande suivante dans votre terminal : "which python".

Type : chaîne.

Cette valeur est requise.

Valeur par défaut : Néant

Socket (KSG_SOCKET)
Source de données de socket

Les éléments de configuration définis dans ce groupe sont toujours présents dans la configuration de l'agent.

Ce groupe définit des informations qui s'appliquent à l'ensemble de l'agent.

Numéro de port (CP_PORT)
Port sur lequel l'agent est à l'écoute des données provenant des clients du socket. La valeur 0 indique qu'un port éphémère sera utilisé. Ce port ne correspond à AUCUN port utilisé par votre application. Il est réservé à un usage interne par l'agent.

Type : numérique.

Cette valeur est facultative.

Valeur par défaut : 0

Configuration de la surveillance d'Oracle Database

Monitoring Agent for Oracle Database fournit des fonctions de surveillance de la disponibilité, des performances et de l'utilisation des ressources de la base de données Oracle. Vous pouvez configurer plusieurs instances d'Agent Oracle Database pour surveiller différentes bases de données Oracle. La fonction de surveillance à distance est également fournie par cet agent.

Avant de commencer

- Avant de configurer Agent Oracle Database, vous devez accorder des privilèges au compte utilisateur Oracle utilisé par Agent Oracle Database. Pour plus d'informations sur les privilèges, voir Accord de privilèges à l'utilisateur de l'agent de base de données Oracle.
- Si vous surveillez une base de données Oracle à distance, l'agent doit être installé sur un ordinateur sur lequel le logiciel de base de données Oracle ou Oracle Instant Client est installé.

Pourquoi et quand exécuter cette tâche

Les instructions figurant dans cette rubrique concernent l'édition la plus récente de l'agent, sauf indication contraire. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent.

Pour la surveillance des performances générales de la base de données Oracle, Agent Oracle Database permet de surveiller la disponibilité, les performances, l'utilisation des ressources et les activités de la base de données Oracle, par exemple :

- Disponibilité des instances dans la base de données Oracle surveillée.
- Informations de ressources, telles que mémoire, caches, segments, limitation, espace table, annulation (rollback), attribut système et statistiques système.
- Informations d'activité, telles que statistiques SE, sessions, conflit et journal des alertes.

L'Agent Oracle Database est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement. De plus, chaque instance d'agent peut surveiller plusieurs bases de données.

Le nom de système géré pour l'Agent Oracle Database comprend le nom de connexion de base de données que vous indiquez, un nom d'instance d'agent que vous indiquez et le nom d'hôte de l'ordinateur sur lequel l'agent est installé. Par exemple, `pc:connection_name-instance_name-host_name:SUB`, où *pc* est votre code produit à deux caractères et *SUB* le type de base de données (les valeurs possibles sont RDB, ASM ou DG). Il est limité à 32 caractères. Le nom d'instance que vous indiquez est limité à 23 caractères, moins la longueur de votre nom d'hôte et connexion de base de données. Par exemple, si vous définissez **dbconn** pour le nom de connexion de base de données, **Oracle02** comme nom d'instance d'agent et que votre nom d'hôte est *Prod204a*, votre nom de système géré est `RZ:dbconn-oracle02-Prod204a:RDB`. Cet exemple utilise 22 des 23 caractères disponibles pour le nom de connexion de base de données, le nom d'instance d'agent et le nom d'hôte.

- Si vous indiquez un nom d'instance long, le nom du système géré est tronqué et le code d'agent ne s'affiche pas correctement.
- La longueur des variables *nom_connexion*, *nom_instance* et *nom_hôte* est tronquée si elle dépasse 23 caractères.
- Pour éviter qu'un nom de sous-noeud soit tronqué, modifiez la convention de dénomination du sous-noeud en paramétrant les variables d'environnement suivantes : **KRZ_SUBNODE_INCLUDING_AGENTNAME**, **KRZ_SUBNODE_INCLUDING_HOSTNAME** et **KRZ_MAX_SUBNODE_ID_LENGTH**.
- Si vous attribuez la valeur NO à la variable **KRZ_SUBNODE_INCLUDING_AGENTNAME**, la partie ID sous-noeud du nom de sous-noeud ne contient pas le nom de l'instance d'agent. Par exemple,
  - Nom de sous-noeud par défaut : *ConnexionBD-Instance-nomHôte*
  - Nom de sous-noeud avec variable d'environnement définie sur NO : *ConnexionBD-nomHôte*
- Si vous définissez **KRZ_SUBNODE_INCLUDING_HOSTNAME** sur NO, la partie ID sous-noeud du nom de sous-noeud ne contient pas le nom d'hôte. Par exemple,
  - Nom de sous-noeud par défaut : *ConnexionBD-Instance-nomHôte*
  - Nom de sous-noeud avec variable d'environnement définie sur NO : *ConnexionBD-Instance*

Procédure

1. Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser la fenêtre **IBM Performance Management** ou le fichier de réponses silencieux.
   - «Configuration de l'agent sur des systèmes Windows», à la page 633.
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 641.
2. Pour configurer l'agent sur des systèmes d'exploitation Linux et UNIX, vous pouvez exécuter le script et répondre aux invites ou utiliser le fichier de réponses silencieux.
   - «Configuration de l'agent en répondant à des invites», à la page 637.

- «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 641.

Que faire ensuite

Pour la configuration avancée uniquement, l'administrateur de la base de données Oracle doit permettre à l'utilisateur Oracle d'exécuter le script `krzgrant.sql` pour accéder à la base de donnés. Voir Exécution du script krzgrant.sql.

Dans la console Cloud APM, accédez à votre Tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont :

- Linux AIX `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Pour identifier et résoudre les incidents, reportez-vous au forum Cloud Application Performance Management.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent sur les systèmes d'exploitation Windows à l'aide de la fenêtre **IBM Performance Management**. Une fois que vous avez mis à jour les valeurs de configuration, démarrez l'agent pour sauvegarder les valeurs mises à jour.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur le modèle **Monitoring Agent for Oracle Database**, puis cliquez sur **Configure agent**.

   A faire : Après avoir configuré une instance d'agent pour la première fois, l'option **Configure agent** est désactivée. Pour reconfigurer l'instance d'agent, cliquez dessus avec le bouton droit de la souris et sélectionnez **Reconfigure**.
3. Dans la fenêtre Monitoring Agent for Oracle Database, procédez comme suit :
   a) Entrez un nom d'instance unique pour l'instance de Monitoring Agent for Oracle Database et cliquez sur **OK**.
4. Dans le panneau Default Database Configuration de la fenêtre **Configure ITCAM Extended Agent for Oracle Database**, procédez comme suit :
   a) Entrez le **`nom d'utilisateur par défaut`**. Il s'agit de l'ID utilisateur de la base de données par défaut utilisé pour les connexions à la base de données.

      Il s'agit de l'ID utilisé par l'agent pour accéder à l'instance de la base de données surveillée. Cet ID utilisateur doit disposer de privilèges de sélection sur les vues et les tables de performances dynamiques nécessaires à l'agent.
   b) Entrez le **`mot de passe par défaut`**. Il s'agit du mot de passe associé à l'ID utilisateur de la base de données par défaut spécifié.
   c) Si la version de l'agent Oracle est 8.0, procédez comme suit.
      1) Entrez le **`fichier jar d'Oracle JDBC`**. Il s'agit du chemin complet du fichier jar du pilote Oracle JDBC utilisé pour communiquer avec la base de données Oracle. Le pilote Oracle Java Database Connectivity (JDBC) qui prend en charge les versions de la base de données Oracle surveillées par l'agent Oracle doit être disponible sur l'ordinateur de l'agent.
   d) Si la version de l'agent Oracle est 6.3.1.10, procédez comme suit.

1) Si l'Agent Oracle Database est installé sur le serveur de base de données Oracle surveillé, sélectionnez **Use libraries in Oracle home** et entrez le **répertoire de base d'Oracle**. (Facultatif) Le paramètre `Oracle Home Directory` peut ne pas être défini pour la surveillance locale ; la variable d'environnement système *ORACLE_HOME* sera utilisée.

2) Si l'Agent Oracle Database est distant du serveur de base de données Oracle surveillé, sélectionnez **Use libraries in Oracle instant client** et entrez le **répertoire d'installation du client Oracle Instant**.

e) Pour définir les options de configuration avancées, cochez **Show advanced options** ; sinon, passez à l'étape 5.

f) Le paramètre `Net Configuration Files Directories` peut ne pas être défini et le répertoire par défaut est utilisé. Si la version de l'agent Oracle est 6.3.1.10, vous pouvez indiquer plusieurs répertoires de fichiers de configuration en séparant leur nom par un point-virgule (;). Pour l'agent Oracle version 8.0, seul un répertoire est pris en charge.

Ce paramètre contient le(s) fichier(s) de configuration réseau de la base de données Oracle. Le répertoire est défini par la variable d'environnement *TNS_ADMIN* pour chaque instance de base de données Oracle. Le répertoire par défaut est `%ORACLE_HOME%\NETWORK\ADMIN`. Si cet élément n'est pas configuré, le répertoire par défaut est utilisé. Pour désactiver l'utilisation du répertoire par défaut, définissez la variable d'environnement d'agent suivante sur false : `KRZ_LOAD_ORACLE_NET=false`.

g) Ne définissez pas le paramètre `Customized SQL definition file name`. Il n'est pas utilisé.

h) Indiquez si le programme d'écoute dynamique par défaut est configuré sur ce poste de travail.

Le programme d'écoute dynamique par défaut est `(PROTOCOL=TCP)(HOST=localhost)(PORT=1521)`. Si le programme d'écoute dynamique par défaut est configuré sur ce poste de travail, définissez cette valeur sur Yes.

i) Cliquez sur **Suivant**.

5. Dans le panneau **Instance configuration** de la fenêtre **Configure ITCAM Extended Agent for Oracle Database**, procédez comme suit :

Définissez dans ce panneau les instances de connexion à la base de données réelles. Vous devez en ajouter au moins une. Vous pouvez également y éditer et y supprimer des instances de connexion à la base de données. S'il existe plusieurs configurations d'instance de connexion à la base de données, utilisez l'option **Database connections** pour choisir l'instance à éditer ou supprimer.

a) Appuyez sur **New** dans la section **Database connections**.

b) Définissez un alias pour la connexion à la base de données dans **Database Connection Name**.

Cet alias vous permet de représenter la connexion à la base de données avec les restrictions suivantes. Seuls les lettres, les chiffres arabes, le caractère souligné et le caractère moins peuvent être utilisés dans le nom de connexion. La longueur maximale d'un nom de connexion est de 25 caractères.

c) Définissez le paramètre **Connection Type**

1) (Facultatif) Basic

Le type de connexion le plus courant et par défaut est **Basic**. Si vous n'êtes pas sûr du type de connexion dont vous avez besoin, il est recommandé de choisir celui-ci.

a) Sélectionnez le type de connexion **Basic** lorsque la base de données cible surveillée est une instance unique, telle qu'une instance de système de fichiers standard ou une instance ASM unique.

b) Définissez le nom d'hôte ou l'adresse IP de la base de données dans la zone `Hostname`.

c) Entrez le numéro de port utilisé par la base de données dans la zone `Port`.

d) Sélectionnez **Service Name** ou **SID**.

i. Si **Service Name** est sélectionné, entrez le nom du service qui est une représentation logique d'une base de données, une chaîne qui est le nom de service de base de données globale.

Un nom de service est une représentation logique d'une base de données, à savoir la manière dont une base de données est présentée aux clients. Une base de données peut être présentée sous forme de services multiples et un service peut être implémenté en tant qu'instances de base de données multiples. Le nom de service est une chaîne qui correspond au nom de base de données global, à savoir un nom composé du nom de la base de données et du nom de domaine, saisie lors de l'installation ou de la création de la base de données. Si vous n'êtes pas sûr de connaître le nom de la base de données global, vous pouvez l'obtenir à partir de la valeur du paramètre SERVICE_NAMES dans le fichier de paramètres d'initialisation.

ii. Si **SID** est sélectionné, entrez l'ID système Oracle qui identifie une instance d'une base de données active.

Il s'agit de l'identificateur système Oracle qui identifie une instance spécifique d'une base de données.

Passez à l'étape 5d.

2) (Facultatif) TNS

a) Sélectionnez le type de connexion **TNS** si la variable d'environnement système *ORACLE_HOME* est définie et que l'alias TNS de la base de données cible surveillée est défini dans le fichier `$ORACLE_HOME/network/admin/tnsnames.ora`.

b) Entrez le nom de l'**`alias TNS`**.

Passez à l'étape 5d.

3) (Facultatif) Advanced

a) Sélectionnez le type de connexion **avancé** lorsqu'il existe plusieurs instances Oracle dans plusieurs noeuds physiques pour la base de données surveillée. Par exemple, un ASM avec une base de données Real Applications Cluster (RAC).

b) Entrez la **`chaîne de connexion Oracle`**.

Cet attribut prend en charge toutes les méthodes d'affectation de nom Oracle Net comme suit :

- Chaîne URL SQL Connect de format `://host:port/service name`. Par exemple, `//dlsun242:1521/bjava21`.
- Paire mot clé-valeur Oracle Net. Par exemple,

```
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=dlsun242) (PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=bjava21)))
```

- Entrées **TNSNAMES**, telles que **inst1** avec la variable d'environnement *TNS_ADMIN* ou *ORACLE_HOME* définie et les fichiers de configuration configurés.

Passez à l'étape 5d.

d) Cochez **Use a different user name and password** pour que cette connexion utilise des données d'identification différentes de celles par défaut que vous avez définies à l'étape 4a et à l'étape 4b ci-dessus. Sinon, passez à l'étape 5g.

e) Entrez le **`nom d'utilisateur de la base de données`** pour cette connexion.

Il s'agit de l'ID utilisé par l'agent pour accéder à l'instance de la base de données surveillée. Cet ID utilisateur doit disposer de privilèges de sélection sur les vues et les tables de performances dynamiques nécessaires à l'agent.

f) Entrez le **`mot de passe de la base de données`**. Il s'agit du mot de passe associé à l'ID utilisateur de base de données spécifié.

g) Sélectionnez un **rôle** qui correspond aux droits accordés aux données d'identification de la connexion à la base de données.

Le rôle est l'ensemble de privilèges à associer à la connexion. Pour un utilisateur disposant du privilège système SYSDBA, indiquez un rôle qui comprend ce privilège. Pour les instances ASM, utilisez le rôle **SYSDBA** ou **SYSASM**.

h) Cochez **Show remote log monitoring options** si vous surveillez des journaux d'alertes Oracle distants à partir de cette instance d'agent ; sinon, passez à l'étape 5k.

i) Entrez le **chemin d'accès au fichier journal des alertes Oracle** ou utilisez **Browse** pour le sélectionner.

Chemins d'accès complets des fichiers journaux d'alertes mappés des instances distantes de cette connexion de la base de données. L'agent surveille les journaux d'alertes en lisant ces fichiers. Ils se trouvent généralement à l'emplacement $ORACLE_BASE/diag/rdbms/*NOM_BDD*/*ID_SYS*/trace/alert_*ID_SYS*.log. Par exemple, si *NOM_BDD* et *ID_SYS* sont définis sur db11g et *ORACLE_BASE* est défini sur /home/dbowner/app/oracle, le journal des alertes figure à l'emplacement /home/dbowner/app/oracle/diag/rdbms/db11g/db11g/trace/alert_db11g.log.

Windows Si l'Agent Oracle Database s'exécute et lit les fichiers journaux d'alerte via le réseau, le chemin de fichier distant doit suivre la convention de dénomination universelle des systèmes Windows. Par exemple, \\tivx015\path\alert_orcl.log.

Windows

Important : Entrez à la fois le chemin d'accès et le nom du fichier journal des alertes. Aucun pilote de réseau mappé n'est pris en charge pour les chemins des journaux d'alertes.

Linux AIX Si l'Agent Oracle Database se trouve sur un serveur distant, un système de fichiers monté en local est requis pour surveiller ses journaux d'alertes distants.

Windows Séparez plusieurs fichiers par un point-virgule (;).

Linux AIX Plusieurs fichiers sont séparés par un signe deux-points (:).

Chaque fichier est mis en correspondance avec une instance de base de données en utilisant le modèle de nom de fichier alert_*instance*.log. S'il n'existe pas de correspondance, il est ignoré.

Les fichiers journaux des alertes de l'instance locale de la base de données sont reconnus automatiquement.

j) Sélectionnez ou saisissez le **jeu de caractères du fichier journal des alertes Oracle**. Il s'agit de la page de codes des fichiers journaux des alertes mappés.

Si ce paramètre est vide, les paramètres régionaux en cours du système sont utilisés, par exemple :

- ISO8859_1, ISO 8859-1 Europe occidentale
- UTF-8, UTF-8 Unicode
- GB18030, chinois simplifié GB18030
- CP950, chinois traditionnel
- EUC_JP, japonais
- EUC_KR, coréen

Pour la liste complète des pages de codes, voir Pages de codes prises en charger ICU.

k) Cliquez sur **Apply** pour sauvegarder les paramètres de cette instance de connexion à la base de données dans la section **Database connections**.

l) (Facultatif) Testez la connexion à la nouvelle base de données.

1) Sélectionnez la nouvelle connexion à la base de données dans la section **Database connections**.

2) Cliquez sur **Tester la connexion**.

3) Observez les résultats dans la fenêtre **Tester la connexion**.

- Exemple de **résultat au test** réussi :

```
Testing connection config1 ...
Success
```

- Exemple de **résultat au test** échoué :

```
Testing connection config1 ...
KBB_RAS1_LOG; Set MAXFILES to 1
ORA-12514: TNS:listener does not currently know of service requested in connect
descriptor
Failed
```

m) Cliquez sur **Suivant**.

6. Lisez les informations contenues dans le panneau **Summary** de la fenêtre **Configure ITCAM Extended Agent for Oracle Database**, puis cliquez sur **OK** pour terminer la configuration d'une instance d'agent.
7. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Monitoring Agent for Oracle Database**, puis cliquez sur **Start**.

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de l'agent en répondant à des invites

Pour configurer l'agent sur des systèmes d'exploitation Linux et UNIX, exécutez le script de configuration de ligne de commande et répondez à ses invites.

Procédure

1. Ouvrez le répertoire *rép_install*/bin, où *rép_install* est le répertoire d'installation de l'Agent Oracle Database.
2. (Facultatif) Pour répertorier les noms des éventuelles instances d'agent configurées existantes, exécutez la commande **./cinfo -o rz**.
3. Pour configurer l'Agent Oracle Database, exécutez la commande **./oracle_database-agent.sh config** *nom_instance*.
4. A l'invite `Edit 'Monitoring Agent for Oracle Database' settings`, appuyez sur **Entrée**. La valeur par défaut est `Oui`.
5. Pour entrer les informations sur la `configuration de base de données par défaut`, procédez comme suit :

   Remarque : La section `Configuration par défaut de base de données` ne correspond pas à la configuration de l'instance de connexion à la base de données. Il s'agit d'un modèle de section qui permet de définir les valeurs par défaut lorsque vous ajoutez les configurations d'instance de connexion à la base de données réelles, qui commence à l'étape 6.

   a) Lorsque le système demande de saisir le `nom d'utilisateur par défaut`, entrez l'ID utilisateur de la base de données par défaut pour les connexions à la base de données et appuyez sur **Entrée**.

   Il s'agit de l'ID utilisé par l'agent pour accéder à l'instance de la base de données surveillée. Cet ID utilisateur doit disposer de privilèges de sélection sur les vues et les tables de performances dynamiques nécessaires à l'agent.

   b) Lorsque le système demande de saisir le `mot de passe par défaut`, tapez le mot de passe associé à l'ID utilisateur de base de données par défaut défini et appuyez sur **Entrée**. Confirmez ensuite le mot de passe si le système vous le demande.

   c) Si la version de l'agent Oracle est 8.0, procédez comme suit.

   1) Entrez le **fichier jar d'Oracle JDBC**. Il s'agit du chemin complet du fichier jar du pilote Oracle JDBC utilisé pour communiquer avec la base de données Oracle. Le pilote Oracle Java Database Connectivity (JDBC) qui prend en charge les versions de la base de données Oracle surveillées par l'agent Oracle doit être disponible sur l'ordinateur de l'agent.

   d) Si la version de l'agent Oracle est 6.3.1.10, procédez comme suit.

1) Lorsque le système demande de saisir le `répertoire de base Oracle`, si l'Agent Oracle Database est installé sur le serveur de base de données Oracle surveillé, entrez le `répertoire de base Oracle` et appuyez sur **Entrée**. Si l'Agent Oracle Database n'est pas installé sur le serveur de base de données Oracle qui va être surveillé, ne définissez pas ce paramètre, appuyez sur **Entrée** et passez à l'étape suivante. Pour effacer la valeur du `répertoire de base Oracle`, appuyez sur la barre d'espace, puis sur **Entrée**.

   Remarque : (Facultatif) Vous pouvez ne pas définir le `répertoire de base Oracle` et le `répertoire d'installation du client Oracle Instant` pour la surveillance locale ; la variable d'environnement système *ORACLE_HOME* sera utilisée.

2) Si l'Agent Oracle Database est éloigné du serveur de base de données Oracle surveillé, entrez le `répertoire d'installation du client Oracle Instant` et appuyez sur **Entrée**. Si vous avez défini le `répertoire de base Oracle` à l'étape «5.d.i», à la page 638, cette valeur est ignorée.

e) Le paramètre `Net Configuration Files Directories` peut ne pas être défini et le répertoire par défaut est utilisé. Si la version de l'agent Oracle est 6.3.1.10, vous pouvez saisir plusieurs répertoires de fichiers de configuration en utilisant Windows ";" ou Linux AIX ":" pour séparer les répertoires. Pour l'agent Oracle version 8.0, seul un répertoire est pris en charge. Appuyez sur **Entrée**.

   Ce paramètre contient le(s) fichier(s) de configuration réseau de la base de données Oracle. Le répertoire est défini par la variable d'environnement *TNS_ADMIN* pour chaque instance de base de données Oracle. Le répertoire par défaut est Linux AIX `$ORACLE_HOME/network/admin` ou Windows `%ORACLE_HOME%\NETWORK\ADMIN`. Si cet élément n'est pas configuré, le répertoire par défaut est utilisé. Pour désactiver l'utilisation du répertoire par défaut, définissez la variable d'environnement d'agent suivante sur false : `KRZ_LOAD_ORACLE_NET=false`.

f) Indiquez si le programme d'écoute dynamique par défaut est configuré sur ce poste de travail, puis appuyez sur **Entrée**.

   Le programme d'écoute dynamique par défaut est `(PROTOCOL=TCP)(HOST=localhost)(PORT=1521)`. Si le programme d'écoute dynamique par défaut est configuré sur ce poste de travail, définissez cette valeur sur True.

g) Ne définissez pas le paramètre `Customized SQL definition file name`. Il n'est pas utilisé.

6. L'invite `Edit 'Database Connection' settings` apparaît une fois que la sortie suivante s'affiche à l'écran :

```
Instance Configuration :
Summary :
Database Connection :
```

   Remarque : Définissez dans cette étape les instances de connexion à la base de données réelles. Vous devez en ajouter au moins une. Vous pouvez également y éditer et y supprimer des instances de connexion à la base de données. S'il existe plusieurs configurations d'instance de connexion à la base de données, utilisez l'option `Next` pour ignorer les instances qui n'ont pas besoin d'être modifiées ou supprimées jusqu'à accéder à l'instance que vous devez modifier ou supprimer.

7. Pour ajouter une nouvelle connexion de base de données, tapez 1 et appuyez sur **Entrée**.
8. Pour entrer les informations de connexion de base de données par défaut, procédez comme suit :

a) Lorsque le système demande le `nom de connexion à la base de données`, tapez un alias pour la connexion à la base de données, puis appuyez sur **Entrée**.

   Cet alias vous permet de représenter la connexion à la base de données avec les restrictions suivantes. Seuls les lettres, les chiffres arabes, le caractère souligné et le caractère moins peuvent être utilisés dans le nom de connexion. La longueur maximale d'un nom de connexion est de 25 caractères.

b) Lorsque le système demande le `type de connexion`, sélectionnez l'un des types de connexion suivants :

   1) (Facultatif) Basic

Le type de connexion le plus courant et par défaut est **Basic**. Si vous n'êtes pas sûr du type de connexion dont vous avez besoin, il est recommandé de choisir celui-ci.

a) Sélectionnez le type de connexion **Basic** si la base de données cible surveillée est une instance unique, telle qu'une instance de système de fichiers standard ou une instance ASM unique.

b) Lorsque le système demande le `nom d'hôte`, tapez le nom d'hôte ou l'adresse IP de la base de données Oracle et appuyez sur **Entrée**.

c) Lorsque le système demande le `port`, tapez le numéro de port et appuyez sur **Entrée**.

d) Entrez l'un des deux paramètres suivants : `Service Name` ou `SID`.

i. (Facultatif) Lorsque le système demande le `nom du service`, tapez le nom du service qui est une représentation logique d'une base de données, une chaîne qui est le nom de service de base de données globale, appuyez sur **Entrée** et passez à l'étape 8c.

Un nom de service est une représentation logique d'une base de données, à savoir la manière dont une base de données est présentée aux clients. Une base de données peut être présentée sous forme de services multiples et un service peut être implémenté en tant qu'instances de base de données multiples. Le nom de service est une chaîne qui correspond au nom de base de données global, à savoir un nom composé du nom de la base de données et du nom de domaine, saisie lors de l'installation ou de la création de la base de données. Si vous n'êtes pas sûr de connaître le nom de la base de données global, vous pouvez l'obtenir à partir de la valeur du paramètre SERVICE_NAMES dans le fichier de paramètres d'initialisation. Ce paramètre peut rester vide si vous définissez `SID` à l'étape «8.b.i.4.b», à la page 639.

ii. (Facultatif) Lorsque le système demande le `SID`, tapez le SID (System Identifier) Oracle qui identifie une instance d'une base de données active, appuyez sur **Entrée** et passez à l'étape 8c.

Ce paramètre est l'identificateur système Oracle qui identifie une instance spécifique d'une base de données. Si le `nom de service` a été défini à l'étape «8.b.i.4.a», à la page 639, vous pouvez ne pas définir cet élément.

2) (Facultatif) TNS

a) Sélectionnez le type de connexion **TNS** lorsque la variable d'environnement système *ORACLE_HOME* est définie et que l'alias TNS de la base de données cible surveillée est défini dans le fichier `$ORACLE_HOME/network/admin/tnsnames.ora`.

b) Tapez le nom d'alias TNS, appuyez sur **Entrée** et passez à l'étape 8c.

3) (Facultatif) Advanced

a) Sélectionnez le type de connexion **avancé** lorsqu'il existe plusieurs instances Oracle dans plusieurs noeuds physiques pour la base de données surveillée. Par exemple, un ASM avec une base de données Real Applications Cluster (RAC).

b) Tapez la chaîne de connexion Oracle, appuyez sur **Entrée** et passez à l'étape 8c.

Cet attribut prend en charge toutes les méthodes d'affectation de nom Oracle Net comme suit :

- Chaîne URL SQL Connect de format `://host:port/service name`. Par exemple, `//dlsun242:1521/bjava21`.
- Paire mot clé-valeur Oracle Net. Par exemple,

```
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=dlsun242) (PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=bjava21)))
```

- Entrées **TNSNAMES**, telles que **inst1** avec la variable d'environnement *TNS_ADMIN* ou *ORACLE_HOME* définie et les fichiers de configuration configurés.

Remarque : La description qui s'affiche lors de la configuration de ligne de commande peut contenir une barre oblique inversée avant le signe deux points (\:) et le signe égal (\=). Ne

saisissez pas de barre oblique inversée dans la chaîne de connexion. Cette barre s'affiche dans la description pour mettre en échappement le comportement normal d'interprétation du signe égal dans une commande et l'interpréter sous la forme de texte.

c) Passez à l'étape 8c.

c) Lorsque le système demande le `nom d'utilisateur de base de données`, tapez l'ID utilisateur de base de données de la connexion et appuyez sur **Entrée**.

Pour les instances de système de fichiers standard, cet ID utilisateur doit disposer des privilèges de sélection sur les vues et les tables de performances dynamiques nécessaires à l'agent.

Pour les instances ASM, utilisez un compte disposant du rôle **SYSDBA** ou **SYSASM**. Par exemple, le compte sys.

d) Lorsque le système demande le `mot de passe de base de données`, tapez le mot de passe associé à l'ID utilisateur de base de données défini.

e) Lorsque le système demande le `rôle`, sélectionnez le rôle qui correspond aux droits accordés à l'ID utilisateur spécifié et appuyez sur **Entrée**.

Le rôle est l'ensemble de privilèges à associer à la connexion. Pour un utilisateur disposant du privilège système SYSDBA, indiquez un rôle qui comprend ce privilège.

Pour les instances ASM, utilisez le rôle **SYSDBA** ou **SYSASM**.

f) Lorsque le système demande les `chemins des fichiers journaux d'alertes Oracle (y compris le nom du fichier journal des alertes)`, tapez les chemins des journaux d'alerte et appuyez sur **Entrée**.

Ce paramètre concerne les chemins d'accès complets des fichiers journaux d'alertes mappés des instances distantes de cette connexion de la base de données. L'agent surveille les journaux d'alertes en lisant ces fichiers. Ils se trouvent généralement à l'emplacement $ORACLE_BASE/diag/rdbms/*NOM_BDD*/*ID_SYS*/trace/alert_*ID_SYS*.log. Par exemple, si *NOM_BDD* et *ID_SYS* sont définis sur db11g et *ORACLE_BASE* est défini sur /home/dbowner/app/oracle, le journal des alertes figure à l'emplacement /home/dbowner/app/oracle/diag/rdbms/db11g/db11g/trace/alert_db11g.log.

Windows Si l'Agent Oracle Database s'exécute et lit les fichiers journaux d'alerte sur le réseau, le chemin de fichier distant doit suivre la convention de dénomination universelle des systèmes Windows. Par exemple, \\tivx015\path\alert_orcl.log.

Important : Entrez à la fois le chemin d'accès et le nom du fichier journal des alertes. Aucun pilote de réseau mappé n'est pris en charge pour les chemins des journaux d'alertes.

Linux AIX Si l'Agent Oracle Database s'exécute, un système de fichiers monté localement est requis pour les journaux d'alertes distants.

Windows Séparez plusieurs fichiers par un point-virgule (;).

Linux AIX Plusieurs fichiers sont séparés par un signe deux-points (:).

Chaque fichier est mis en correspondance avec une instance de base de données en utilisant le modèle de nom de fichier `alert_`*`instance`*`.log`. S'il n'existe pas de correspondance, il est ignoré.

Les fichiers journaux des alertes de l'instance locale de la base de données peuvent être reconnus automatiquement.

g) Lorsque le système demande le **`jeu de caractères du fichier journal des alertes Oracle`**, tapez la page de codes des fichiers journaux d'alertes associés, puis appuyez sur **Entrée**.

Si ce paramètre est vide, les paramètres régionaux en cours du système sont utilisés, par exemple :

- ISO8859_1, ISO 8859-1 Europe occidentale
- UTF-8, UTF-8 Unicode

- GB18030, chinois simplifié GB18030
- CP950, chinois traditionnel
- EUC_JP, japonais
- EUC_KR, coréen

Pour la liste complète des pages de codes, voir Pages de codes prises en charger ICU.

9. A l'invite `Edit 'Database Connection' settings`, le nom de la connexion à la base de données que vous avez défini à l'étape 8a s'affiche. Vous pouvez l'éditer à nouveau ou le supprimer. Si plusieurs instances de connexion à la base de données sont déjà configurées, cliquez sur **Next** pour les parcourir.
10. (Facultatif) Pour ajouter une autre connexion à la base de données afin de surveiller plusieurs instances de base de données avec cette instance d'agent, entrez 1, appuyez sur **Entrée** et revenez à l'étape 8.
11. Une fois que vous avez terminé de modifier les connexions à la base de données, entrez 5 et appuyez sur **Entrée** pour quitter le processus de configuration.
12. Pour démarrer l'agent, entrez la commande suivante :
`*rép_install*/bin/oracle_database-agent.sh start *nom_instance*`.

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

1. Ouvrez le fichier `oracle_silent_config.txt` dans un éditeur de texte :
   - Linux AIX `*rép_install*/samples/oracle_database_silent_config.txt`.
   - Windows `*rép_install*\samples\oracle_database_silent_config.txt`
2. Pour **`Default Username`**, entrez le nom de l'utilisateur de base de données par défaut pour les connexions à la base de données qui sont créées pour cette instance d'agent. Par exemple, **`KRZ_CONN_USERID=`**`user1`.

   Remarque : Cet utilisateur doit disposer de privilèges suffisants pour exécuter les tâches, telles que l'interrogation des tables, que cet agent exécute lorsqu'il est connecté à la base de données.
3. Pour **`Default Password`**, vous devez entrer le mot de passe associé à l'utilisateur de base de données par défaut spécifié. Par exemple, **`KRZ_CONN_PASSWORD=`**`mot de passe`.
4. Si la version de l'agent Oracle est 8.0, procédez comme suit.
   a) Entrez le **`fichier jar d'Oracle JDBC`**. Il s'agit du chemin complet du fichier jar du pilote Oracle JDBC utilisé pour communiquer avec la base de données Oracle.

Le pilote Oracle Java Database Connectivity (JDBC) qui prend en charge les versions de la base de données Oracle surveillées par l'agent Oracle doit être disponible sur l'ordinateur de l'agent.

5. Si la version de l'agent Oracle est 6.3.1.10, procédez comme suit.
   a) Si l'Agent Oracle Database est installé sur le serveur de base de données Oracle surveillé, entrez le `répertoire de base Oracle`. Par exemple, **KRZ_ORACLE_HOME=**`chemin du répertoire de base`.

      Remarque : pour les paramètres facultatifs comme celui-ci, supprimez le symbole dièse (#) en préfixe pour les utiliser.

      Si l'Agent Oracle Database n'est pas installé sur le serveur de base de données Oracle qui va être surveillé, ne définissez pas ce paramètre et passez à l'étape suivante.

      Remarque : (facultatif) vous pouvez ne pas définir le `répertoire de base Oracle` et le `répertoire d'installation du client Oracle Instant` (mise en commentaire en insérant le symbole dièse (#) à la première position de la ligne du paramètre dans le fichier texte de configuration en mode silencieux) ; la variable d'environnement système *ORACLE_HOME* sera utilisée.

   b) Si l'Agent Oracle Database est éloigné du serveur de base de données Oracle surveillé, entrez le `répertoire d'installation du client Oracle Instant`. Si vous avez saisi le `répertoire de base Oracle` à l'étape précédente, cette valeur est ignorée.

      - Windows Définissez le chemin de dossier complet du répertoire de **base Oracle** qui contient les fichiers de la bibliothèque `Oracle Call Interface (OCI)`. Si le chemin complet du fichier `oci.dll` est `C:\instantclient_10_2\oci.dll`, vous devez définir le chemin `C:\instantclient_10_2`. Par exemple, **KRZ_INSTANT_CLIENT_LIBPATH=**`C:\instantclient_10_2`
      - AIX Définissez le chemin de dossier complet du répertoire de **base Oracle** qui contient les fichiers de la bibliothèque `Oracle Call Interface (OCI)`. Si le chemin complet du fichier `libocci.so.10.1` est `/home/tivoli/oci/libocci.so.10.1`, vous devez définir le chemin `/home/tivoli/oci`. Par exemple, **KRZ_INSTANT_CLIENT_LIBPATH=**`/home/tivoli/oci`

6. Le paramètre `Net Configuration Files Directories` peut ne pas être défini et le répertoire par défaut est utilisé. Agent Oracle Database utilise ce chemin de fichier pour obtenir le fichier `tnsnames.ora`. Ce répertoire est défini par la variable d'environnement *TNS_ADMIN* pour chaque instance de base de données Oracle. Le répertoire par défaut est Linux AIX `$ORACLE_HOME/network/admin` ou Windows `%ORACLE_HOME%\NETWORK\ADMIN`. Si vous définissez ce paramètre avec plusieurs répertoires de fichiers de configuration réseau, utilisez Windows ";" ou Linux AIX ":" pour séparer les répertoires.

   Si vous surveillez des bases de données Oracle à distance, vous pouvez copier les fichiers de configuration réseau du système distant vers le système où l'agent est installé. En outre, vous pouvez fusionner le contenu des fichiers de configuration réseau sur le système distant avec les fichiers de configuration réseau sur le système où l'agent est installé.

7. Pour l'**écoute dynamique**, vérifiez que le programme d'écoute dynamique est configuré. Le programme d'écoute dynamique par défaut est (PROTOCOL=TCP)(HOST=localhost)(PORT=1521). Si le programme d'écoute dynamique par défaut est configuré, définissez cette valeur sur TRUE comme indiqué ici ; **KRZ_DYNAMIC_LISTENER=**TRUE.

   Les valeurs valides sont TRUE et FALSE.

8. Ne définissez pas le paramètre `Customized SQL definition file name`. Il n'est pas utilisé.
9. Les instances de connexion à la base de données réelles sont définies à partir de cette étape. Vous devez en ajouter au moins une. Les entrées d'une instance sont fournies dans le fichier `oracle_silent_config.txt` avec le nom d'instance *config1*. Si vous modifiez le nom d'instance, veillez à modifier toutes les références.

   Cet alias vous permet de représenter la connexion à la base de données avec les restrictions suivantes. Seuls les lettres, les chiffres arabes, le caractère souligné et le caractère moins peuvent

être utilisés dans le nom de connexion. La longueur maximale d'un nom de connexion est de 25 caractères.

10. Pour le **type de connexion**, définissez l'un des types de connexion suivants : **De base**, **TNS**, ou **Avancé**. Par exemple, **KRZ_CONN_TYPE.config1=**Basic.
11. Pour le type de connexion que vous avez sélectionné à l'étape précédente, spécifiez les paramètres requis :

    De base

    - Pour le **nom d'hôte**, définissez le nom d'hôte ou l'adresse IP de la base de données Oracle, par exemple, **KRZ_CONN_HOST.config1=** nom_hôte.
    - Pour le **port**, définissez le port d'écoute de la base de données Oracle, par exemple, **#KRZ_CONN_PORT.config1=** 1521.
    - Pour le **nom de service**, définissez la représentation logique de la base de données en utilisant une chaîne pour le nom de base de données global, par exemple, **KRZ_CONN_SERVICE.config1=** orcl.

      Important : Si vous ne définissez pas le nom de service, vous devez spécifier l'identificateur système Oracle (SID).

      Pour le **SID (System Identifier) Oracle**, définissez un SID qui identifie une instance d'une base de données active, par exemple, **KRZ_CONN_SID.config1=** sid.

    TNS

    Pour l'**alias TNS**, définissez le nom d'alias réseau depuis le fichier tnsnames.ora. Par exemple, **KRZ_CONN_TNS.config1=** alias_tns.

    Avancé

    Pour la **chaîne de connexion Oracle**, définissez la chaîne de connexion de base de donnée d'OCI. Par exemple, **KRZ_CONN_STR.config1=** //host:port/service

    Cette chaîne prend en charge toutes les méthodes de dénomination Oracle Net, comme indiqué ci-dessous :

    - Pour une chaîne URL SQL Connect :

      ```
      //host:[port][/service name]
      ```

    - Pour une paire mot clé/valeur Oracle Net

      ```
      "(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=dlsun242) (PORT=1521))
      (CONNECT_DATA=(SERVICE_NAME=bjava21)))"
      ```

    Cette chaîne prend également en charge les entrées **TNSNAMES** , par exemple, **inst1**, où la variable d'environnement *TNS_ADMIN* ou *ORACLE_HOME* est définie et les fichiers de configuration sont configurés.

    Important : Cet attribut s'applique uniquement au type de connexion avancée.
12. Pour le **nom d'utilisateur de base de données**, vous pouvez définir le nom de l'utilisateur de base de données de la connexion, par exemple, **KRZ_CONN_USERID=**UserID.

    Cet utilisateur doit disposer des privilèges suffisants pour pouvoir exécuter les tâches que l'agent doit exécuter (création, modification et suppression de tables, par exemple) lorsqu'il est connecté à la base de données.

    Si cette zone est vide, l'agent utilise le nom d'utilisateur par défaut dans la section de configuration de base de données par défaut. Si le **nom d'utilisateur de base de données** n'a pas été configuré, le nom d'utilisateur par défaut est utilisé pour la connexion.
13. Pour le **mot de passe de base de données**, vous pouvez définir le mot de passe associé à l'utilisateur de base de données défini, par exemple, **KRZ_CONN_PASSWORD=**Password.

    Si cette zone est vide, l'agent utilise le mot de passe par défaut dans la section de configuration de base de données par défaut. Si le **mot de passe de base de données** n'est pas défini, le mot de passe par défaut est utilisé pour la connexion.

14. Pour le **rôle**, vous pouvez définir l'ensemble de privilèges associés à la connexion, par exemple **KRZ_CONN_MODE.config1=**DEFAULT.

    Les valeurs valides sont notamment *SYSDBA*, *SYSOPER*, *SYSASM* et *DEFAULT*.

    Pour un utilisateur disposant du privilège système *SYSDBA*, vous pouvez définir une connexion qui inclut ce privilège. Si cet élément n'est pas défini, vous pouvez affecter le rôle *DEFAULT* à l'utilisateur.
15. Pour les **chemins des fichiers journaux d'alertes Oracle**, qui incluent le nom de fichier journal des alertes, vous pouvez définir le chemin de fichier absolu des fichiers journaux d'alertes mappés des instances de base de données distante dans cette connexion de base de données. Par exemple, **KRZ_LOG_PATHS.config1=**chemin_journal_alertes.

    Windows Utilisez le point-virgule (;) pour séparer plusieurs fichiers.

    Linux AIX Utilisez le signe deux-points (:) pour séparer plusieurs fichiers.

    Chaque fichier est mis en correspondance avec une instance de base de données par le modèle de nom de fichier alert_*instance*.log. Sinon, il est ignoré si aucune correspondance n'existe.

    Les fichiers journaux d'alertes d'instance de base de données locale sont reconnus automatiquement.

    Si les **chemins des fichiers journaux d'alertes Oracle** n'ont pas été définis, le journal d'alertes n'est pas disponible.
16. Pour le **jeu de caractères des fichiers journaux d'alertes Oracle**, vous pouvez définir la page de codes des fichiers journaux d'alertes associés. Par exemple, **KRZ_LOG_CHARSET.config1=** jeu_caractères

    Si cette zone est vide, les paramètres régionaux en cours du système sont utilisés, comme indiqué ici :

    ```
    ISO8859_1: ISO 8859-1 Western European encoding
    UTF-8: UTF-8 encoding of Unicode
    GB18030: Simplified Chinese GB18030 encoding
    CP950: Traditional Chinese encoding
    EUC_JP: Japanese encoding
    ```
17. Sauvegardez et fermez le fichier oracle_database_silent_config.txt. Entrez : *rép_install*/bin/oracle_database-agent.sh config *nom_instance rép_install*/samples/oracle_database_silent_config.txt
    où *nom_instance* est le nom à attribuer à l'instance.
18. Pour démarrer l'agent, entrez la commande suivante : *rép_install*/bin/oracle_database-agent.sh start *nom_instance*.

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Accord de privilèges à l'utilisateur de l'agent de base de données Oracle

Une fois que vous avez installé l'agent, vous devez accorder des privilèges au compte utilisateur Oracle utilisé par Agent Oracle Database.

Vous pouvez accorder des privilèges aux utilisateurs suivants :

- Utilisateurs d'instance (non ASM) de système de fichiers standard
- Utilisateurs non SYS d'instance ASM with RAC

Attribution de privilèges aux utilisateurs pour les instances de système de fichiers standard
Pour les instances de système de fichiers standard, l'ID utilisateur Oracle utilisé par l'Agent Oracle Database doit disposer des privilèges de sélection sur les vues de performances dynamiques, les tables

et les vues de dictionnaire de données requises par l'agent. Il doit également disposer des autres privilèges sur les systèmes et objets Oracle nécessaires pour exécuter certaines commandes de base de données.

Procédure

1. (Facultatif) S'il n'existe pas d'ID utilisateur de base de données, créez-en un à l'aide des fonctions Oracle en exécutant la commande suivante : `create user` *`nom_utilisateur`* `identified by` *`mot_de_passe`*
2. Accordez à l'ID utilisateur Oracle créé en exécutant le script **krzgrant.sql** fourni avec Agent Oracle Database, des privilèges de sélection sur les vues de performances dynamiques, les tables et les vues de dictionnaire de données. Cette étape doit être effectuée préalablement à la configuration de l'agent. Pour consulter les instructions de personnalisation et d'exécution du script **krzgrant.sql**, voir «Personnalisation du script krzgrant.sql», à la page 645 et «Exécution du script krzgrant.sql», à la page 646.

   Remarque : Les privilèges de sélection sur les vues de performances dynamiques, les tables et les vues de dictionnaire de données dépendent des capacités de la base de données Oracle dans des environnements d'application spécifiques. Vous pouvez accorder des privilèges Oracle autorisés à l'ID utilisateur de base de données Oracle uniquement pour les vues de performances dynamiques, les tables et les vues de dictionnaire de données utilisées par Agent Oracle Database.
3. Accordez à l'ID utilisateur Oracle qu'utilise Agent Oracle Database d'autres privilèges d'objet Oracle et privilèges système en utilisant les fonctions Oracle.

Personnalisation du script krzgrant.sql

Si vous ne voulez pas autoriser les privilèges de sélection autorisés Oracle sur certaines vues de performances dynamiques, tables et vues de dictionnaire de données dans le script **krzgrant.sql**, vous pouvez personnaliser le script avant de l'exécuter.

Remarque : L'instance d'agent vérifie tous les privilèges par défaut du script **krzgrant.sql** et fait état d'un événement d'agent signalant un manque de privilèges lors du démarrage de l'agent. Vous pouvez désactiver la vérification des privilèges en utilisant le paramètre de variable suivant : KRZ_CHECK_ORACLE_PRIVILEGE=FALSE. L'étape de test de connexion de la configuration de l'interface graphique vérifie l'ensemble des privilèges Oracle définis dans le fichier `krzgrant.sql`. Si vous confirmez que l'utilisateur Oracle dispose bien des privilèges adéquats, ignorez l'échec de vérification des privilèges lors de l'étape de test de connexion.

Modifiez le fichier `krzgrant.sql` dans un éditeur de texte en clair pour supprimer ou ajouter le préfixe '--' au début des instructions d'attribution de droits afin d'éviter l'exécution d'attribution de privilèges pour les vues et les tables Oracle non autorisées.

Par exemple, remplacez les lignes suivantes :

```
    execute immediate 'grant select on DBA_HIST_SNAPSHOT to '||userName;
    execute immediate 'grant select on DBA_HIST_SQLSTAT to '||userName;
    execute immediate 'grant select on DBA_HIST_SQLTEXT to '||userName;
    execute immediate 'grant select on DBA_HIST_SQL_PLAN to '||userName;
    execute immediate 'grant select on DBA_HIST_SYSMETRIC_SUMMARY to '||userName;
```

par ces lignes :

```
--    execute immediate 'grant select on DBA_HIST_SNAPSHOT to '||userName;
--    execute immediate 'grant select on DBA_HIST_SQLSTAT to '||userName;
--    execute immediate 'grant select on DBA_HIST_SQLTEXT to '||userName;
--    execute immediate 'grant select on DBA_HIST_SQL_PLAN to '||userName;
--    execute immediate 'grant select on DBA_HIST_SYSMETRIC_SUMMARY to '||userName;
```

Attribution de privilèges aux utilisateurs non SYS pour les instances ASM
Vous devez vous connecter aux instances ASM qui utilisent les rôles SYSDBA et SYSASM pour les utilisateurs. Si vous ne souhaitez pas utiliser le compte SYS pour vous connecter aux instances ASM, créez un compte utilisateur et attribuez les rôles SYSDBA et SYSASM au compte.

Procédure

1. Exécutez les commandes suivantes pour créer un compte utilisateur et attribuer des rôles :
   - Connectez-vous à la base de données ASM avec le rôle SYSASM afin de créer un utilisateur pour un agent et lui accorder le rôle SYSDBA ou SYSASM :
     a. `create user nom_utilisateur identified by mot_de_passe`
     b. `grant sysdba to nom_utilisateur`

     ou

     `grant sysasm to nom_utilisateur`
2. Lors de la création de la connexion ASM dans la fenêtre de configuration, indiquez l'utilisateur *UserName* et le rôle SYSDBA ou SYSASM.

   Remarque : Si vous choisissez le rôle SYSASM pour accéder à la base de données ASM, vous devez configurer l'instance d'agent en utilisant le répertoire de base Oracle ou le répertoire client Oracle Instant pour vous connecter à la base de données Oracle.

Exécution du script `krzgrant.sql`

Avant de commencer

- Si vous n'exécutez pas le script **`krzgrant.sql`**, un événement est généré dans l'espace de travail des événements d'agent.
- Pour effectuer la procédure d'installation, voir Chapitre 6, «Installation des agents», à la page 123.

Après l'installation, le script **`krzgrant.sql`** se trouve dans le répertoire suivant :

- Windows *rép_install*\TMAITM6_X64
- Linux AIX *rép_install*/*architecture*/rz/bin

où :

rép_install
Répertoire d'installation de l'Agent Oracle Database.

architecture
Identificateur de l'architecture système d'IBM Application Performance Management ou de Cloud APM. Par exemple, lx8266 représente Linux Intel version 2.6 (64 bits). Pour obtenir la liste complète des codes d'architecture, voir le fichier *rép_install*/registry/archdsc.tbl.

Le script **`krzgrant.sql`** est utilisé comme suit : `krzgrant.sql` *ID_utilisateur répertoire_temporaire*

où :

ID_utilisateur
ID de l'utilisateur Oracle. Doit être créé avant l'exécution de ce ficher SQL. Exemple de valeur : *tivoli*.

Répertoire_temporaire
Nom du répertoire temporaire destiné à recevoir le fichier de sortie `krzagent.log` du script **`krzgrant.sql`**. Ce répertoire doit exister avant que vous n'exécutiez ce script SQL. Par exemple : `rép_install/tmp`.

Vous devez disposer du rôle d'autorisation d'administrateur de la base de données Oracle et du droit en écriture sur le répertoire temporaire pour effectuer la procédure qui suit.

Procédure

1. Dans la ligne de commande, exécutez les commandes de définition des variables d'environnement.
   - Windows

     ```
     SET ORACLE_SID= sid
     SET ORACLE_HOME= home
     ```

   - Linux AIX

     ```
     ORACLE_SID = sid
     export ORACLE_SID
     ORACLE_HOME = home
     export ORACLE_HOME
     ```

   où :

   sid
   Identificateur du système Oracle, sensible à la casse.

   home
   Répertoire de base de l'instance Oracle surveillée.
2. A partir de la fenêtre de ligne de commande utilisée pour définir les variables d'environnement, démarrez Oracle SQL Plus ou un autre outil de lancement d'instructions SQL.
3. Connectez-vous à la base de données Oracle en tant qu'utilisateur Oracle disposant des privilèges administrateur.
4. Accédez au répertoire contenant le script **krzgrant.sql** et exécutez la commande suivante pour attribuer les privilèges de sélection :

   ```
   @krzgrant.sql ID_utilisateur répertoire_temporaire
   ```

   Le résultat est consigné dans le fichier `krzagent.log` du répertoire temporaire. Ce journal enregistre les vues et les tables pour lesquelles l'agent Agent Oracle Database a reçu les privilèges de sélection.

   Une fois les privilèges accordés, vous pouvez configurer et démarrer l'Agent Oracle Database.

Configuration de la surveillance du système d'exploitation

Les agents Monitoring Agent for Linux OS, Monitoring Agent for UNIX OS et Monitoring Agent for Windows OS sont configurés automatiquement. Vous pouvez configurer la surveillance des fichiers journaux pour les agents de système d'exploitation afin de pouvoir surveiller les fichiers journaux d'application. Vous pouvez exécuter les agents de système d'exploitation en tant qu'utilisateur non superutilisateur. Il existe également d'autres options de configuration pour l'agent de système d'exploitation Linux.

Exécution des agents de système d'exploitation en tant qu'utilisateur non superutilisateur

Vous pouvez exécuter Monitoring Agent for Windows OS, Monitoring Agent for UNIX OS et Monitoring Agent for Linux OS en tant qu'utilisateur non superutilisateur.

Pour exécuter l'agent Windows OS en tant qu'utilisateur non superutilisateur, voir «Exécution de Monitoring Agent for Windows OS en tant qu'utilisateur non superutilisateur», à la page 648.

Pour exécuter Monitoring Agent for UNIX OS et Monitoring Agent for Linux OS en tant qu'utilisateur non superutilisateur, voir «Démarrage des agents en tant qu'utilisateur non superutilisateur», à la page 1042.

Restriction :

Lorsqu'il s'exécute sans privilèges superutilisateur, l'agent ne peut pas accéder à `/proc/pid/status` et ne peut donc pas générer de rapport sur les attributs suivants :

- -User CPU Time (UNIXPS.USERTIME)

- -System CPU Time (UNIXPS.SYSTEMTIM)
- -Total CPU Time (UNIXPS.TOTALTIME)
- -Thread Count (UNIXPS.THREADCNT)
- -Child User CPU Time (UNIXPS.CHILDUTIME)
- -Child System CPU Time (UNIXPS.CHILDSTIME)
- -Total Child CPU Time (UNIXPS.CHILDTIME)
- -Wait CPU Time (UNIXPS.WAITCPUTIM)
- -Terminal (UNIXPS.USERTTY)

Ces attributs ne sont pas visibles dans la console Cloud APM mais sont disponibles pour créer des seuils.

Exécution de Monitoring Agent for Windows OS en tant qu'utilisateur non superutilisateur

Vous pouvez exécuter l'agent Windows OS en tant qu'utilisateur non superutilisateur, mais certaines fonctions ne sont pas disponibles.

Lorsque vous exécutez l'agent Windows OS en tant qu'utilisateur non superutilisateur, certaines fonctions ne sont pas disponibles dans les groupes d'attributs suivants si elles sont la propriété exclusive du compte administrateur :

- Registre
- Tendance de fichier
- Modification de fichier

Le déploiement à distance d'autres agents n'est pas disponible car des droits d'administrateur sont nécessaires pour installer les nouveaux agents.

Pour Agent Management Services, le programme de surveillance ne peut pas arrêter ni démarrer d'agent pour lequel il ne dispose pas des droits appropriés.

Pour créer un utilisateur non superutilisateur, créez un utilisateur limité (non superutilisateur) et attribuez-lui des droits sur le registre, comme dans l'exemple suivant :

- Accès complet à `HKEY_LOCAL_MACHINE\SOFTWARE\Candle`
- Accès en lecture à `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion \Perflib`

L'utilisateur qui démarre Monitoring Agent for Windows OS – Service principal doit disposer des droits nécessaires pour gérer Monitoring Agent for Windows OS - Service de surveillance. Celui qui démarre Monitoring Agent for Windows OS – Service de surveillance doit également disposer des droits nécessaires pour gérer tous les services administrés par Agent Management Services, notamment Monitoring Agent for Windows OS - Service principal. Pour accorder à des utilisateurs les droits de gestion des services système dans Windows, utilisez les modèles de sécurité et la stratégie de groupe, ou éditez le fichier `Subinacl.exe`. Pour plus d'informations, reportez-vous à la documentation Microsoft à l'adresse suivante : http://support.microsoft.com/kb/325349(http://support.microsoft.com/kb/325349).

L'exemple suivant montre comment accorder à des utilisateurs les droits de gestion des services système à l'aide des modèles de sécurité :

1. Cliquez sur **Démarrer** > **Exécuter**, puis entrez `mmc` dans la zone Ouvrir et cliquez sur **OK**.
2. Dans le menu **Fichier**, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.
3. Cliquez sur **Ajouter** > **Configuration et analyse de la sécurité**, puis cliquez de nouveau sur **Ajouter**.
4. Cliquez sur **Fermer** puis sur **OK**.
5. Dans l'arborescence de la console, cliquez avec le bouton droit de la souris sur **Configuration et analyse de la sécurité**, puis sur **Ouvrir une base de données**.
6. Indiquez un nom et un emplacement pour la base de données, puis cliquez sur **Ouvrir**.
7. Dans la boîte de dialogue **Importer un modèle** qui s'affiche, cliquez sur le modèle de sécurité que vous souhaitez importer, puis sur **Ouvrir**.

8. Dans l'arborescence de la console, cliquez avec le bouton droit de la souris sur **Configuration et analyse de la sécurité**, puis sur **Analyser l'ordinateur maintenant**.
9. Dans la boîte de dialogue **Effectuer l'analyse** qui s'affiche, acceptez le chemin par défaut du fichier journal qui s'inscrit dans la zone du chemin du fichier journal des erreurs. Vous pouvez aussi indiquer un autre emplacement. Cliquez sur **OK**.
10. Une fois l'analyse terminée, configurez les autorisations pour le service comme suit :
    a. Dans l'arborescence de la console, cliquez sur **Services système**.
    b. Dans le panneau de droite, cliquez deux fois sur Monitoring Agent for Windows OS - Service principal.
    c. Sélectionnez la case à cocher **Définir cette règle dans la base de données**, puis cliquez sur **Modifier la sécurité**.
    d. Pour configurer des autorisations pour un nouvel utilisateur ou un nouveau groupe, cliquez sur **Ajouter**.
    e. Dans la boîte de dialogue **Sélectionner les utilisateurs, les ordinateurs ou les groupes**, saisissez le nom de l'utilisateur ou du groupe pour lequel vous souhaitez définir des autorisations, puis cliquez sur **OK**. Dans la liste **Autorisations par utilisateur et groupe**, cochez la case **Autoriser** (à côté de **Démarrer**). L'autorisation d'arrêt et d'interruption étant sélectionnée par défaut, l'utilisateur ou le groupe a toute latitude pour démarrer, arrêter ou interrompre le service.
    f. Cliquez sur **OK** deux fois.
11. Répétez l'étape 10 pour configurer les autorisation de service de Monitoring Agent for Windows OS - Service de surveillance.
12. Pour appliquer les nouveaux paramètres de sécurité à l'ordinateur local, cliquez avec le bouton droit de la souris sur **Configuration et analyse de la sécurité**, puis cliquez sur **Configurer l'ordinateur maintenant**.

Remarque : Vous pouvez utiliser également l'outil de ligne de commande Secedit pour configurer et analyser la sécurité du système. Pour plus d'informations sur Secedit, cliquez sur **Démarrer** > **Exécuter**, puis entrez `cmd` et cliquez sur **OK**. A l'invite de commande, entrez `secedit /?`, puis appuyez sur la touche **ENTREE**. Lorsque vous appliquez des paramètres à l'aide de cette méthode, tous les paramètres du modèle sont réappliqués. Il est possible que cette méthode redéfinisse certaines autorisations de fichier, registre ou service précédemment configurées.

L'exemple suivant montre comment définir Monitoring Agent for Windows OS et les services de surveillance pour la connexion en tant qu'utilisateur non superutilisateur à l'aide de la console Windows Services :

1. Cliquez sur **Démarrer** > **Exécuter**, puis entrez `services.msc` et cliquez sur **OK**.
2. Sélectionnez **Monitoring Agent for Windows OS - Service principal**.
3. Cliquez avec le bouton droit de la souris sur **Propriétés**.
4. Vérifiez que le type de démarrage est réglé sur Automatique.
5. Sélectionnez l'onglet **Ouvrir une session**, puis **Ouvrir une session en tant que "Ce compte"** et entrez l'ID et le mot de passe. Cliquez sur **OK**.
6. Sélectionnez **Monitoring Agent for Windows OS - Programme de surveillance**.
7. Cliquez avec le bouton droit de la souris sur **Propriétés**.
8. Vérifiez que le type de démarrage est réglé sur Manuel.
9. Sélectionnez l'onglet **Ouvrir une session**, puis **Ouvrir une session en tant que "Ce compte"** et entrez l'ID et le mot de passe. Cliquez sur **OK**.

Configuration de la surveillance des fichiers journaux de l'agent de système d'exploitation

Les agents Monitoring Agent for Linux OS, Monitoring Agent for UNIX OS et Monitoring Agent for Windows OS sont configurés automatiquement. Toutefois, vous pouvez configurer la surveillance des fichiers

journaux pour les agents de système d'exploitation afin de pouvoir surveiller les fichiers journaux d'application.

Une fois filtrées par les agents, les données sont envoyées sous forme d'un événement de journal à la console console Cloud APM.

Ajout ou suppression de la configuration de surveillance des fichiers journaux pour les agents de système d'exploitation
Vous pouvez ajouter la configuration de surveillance des fichiers journaux pour les agents de système d'exploitation afin de permettre à ces derniers de filtrer les données des fichiers journaux. Vous pouvez ensuite, le cas échéant, supprimer la configuration de la surveillance des fichiers journaux pour les agents de système d'exploitation.

Avant de commencer
Les agents de système d'exploitation incluent désormais un exemple de fichier regex1.conf et de fichier regex1.fmt que vous pouvez consulter avant de configurer les fichiers .conf et .fmt. Ces fichiers se trouvent ici :

- Sous UNIX/Linux : `<rép_install>/samples/logfile-monitoring`
- Sous Windows : `<rép_install\samples\logfile-monitoring`

A l'aide d'un éditeur de texte, créez un fichier de configuration `.conf` et un fichier de format `.fmt`. Pour plus d'informations sur le contenu de ces fichiers, voir «Fichier de configuration», à la page 655 et «Fichier de format », à la page 665. Vous devez veiller à sauvegarder ces fichiers sur le système à partir duquel vous accédez à la console Performance Management, de sorte que vous puissiez les télécharger sur le serveur Cloud APM.

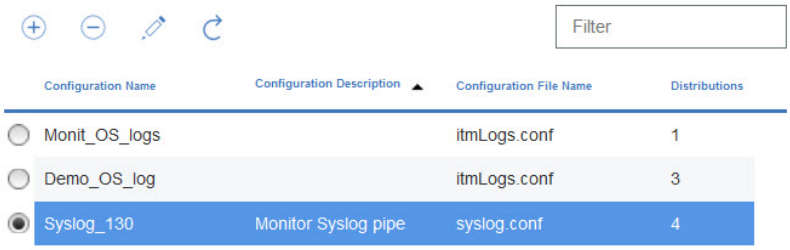
Pourquoi et quand exécuter cette tâche
Pour permettre aux agents du système d'exploitation de surveiller les fichiers journaux, vous devez télécharger le fichier de configuration et le fichier de format, et préciser à quel agent de système d'exploitation la configuration s'applique. L'agent de système d'exploitation reçoit par téléchargement les fichiers `.conf` et `.fmt` et surveille les fichiers journaux indiqués dans la configuration.

Procédure

Ajout de la configuration de surveillance des fichiers journaux pour les agents de système d'exploitation

1. Cliquez sur **Configuration du système** > **Configuration d'agent**.
2. En fonction du système où vous souhaitez surveiller les fichiers journaux, cliquez sur l'onglet **Système d'exploitation Unix**, **Système d'exploitation Linux** ou **Système d'exploitation Windows**.
3. Pour créer une configuration, cliquez sur l'icône (+) pour ouvrir la fenêtre **New Log File Configuration**. Entrez un nom et une description de la configuration.
4. Pour afficher le contenu des fichiers `.conf` et `.fmt`, cliquez sur **Visualiser**.
5. Pour transférer la configuration à l'aide du serveur Cloud APM, sélectionnez le fichier `.conf` et le fichier `.fmt` sur le système où vous ouvrez la console Performance Management et cliquez sur **Terminé**.
6. Dans l'onglet de l'agent de système d'exploitation, sélectionnez la configuration que vous envoyez par téléchargement.

   Important : Les fichiers `.conf` et `.fmt` qui sont distribués aux agents sont renommés en utilisant le nom de configuration que vous définissez.



7. Pour déployer la configuration, dans la table **Log Configuration Distributions List**, sélectionnez les agents vers lesquels vous souhaitez déployer la configuration et cliquez sur **Appliquer les modifications**.

Suppression de la configuration de surveillance des fichiers journaux pour les agents de système d'exploitation

8. Sélectionnez le nom de configuration.
9. Supprimez les systèmes gérés et cliquez sur **Appliquer les modifications**.

   Important :

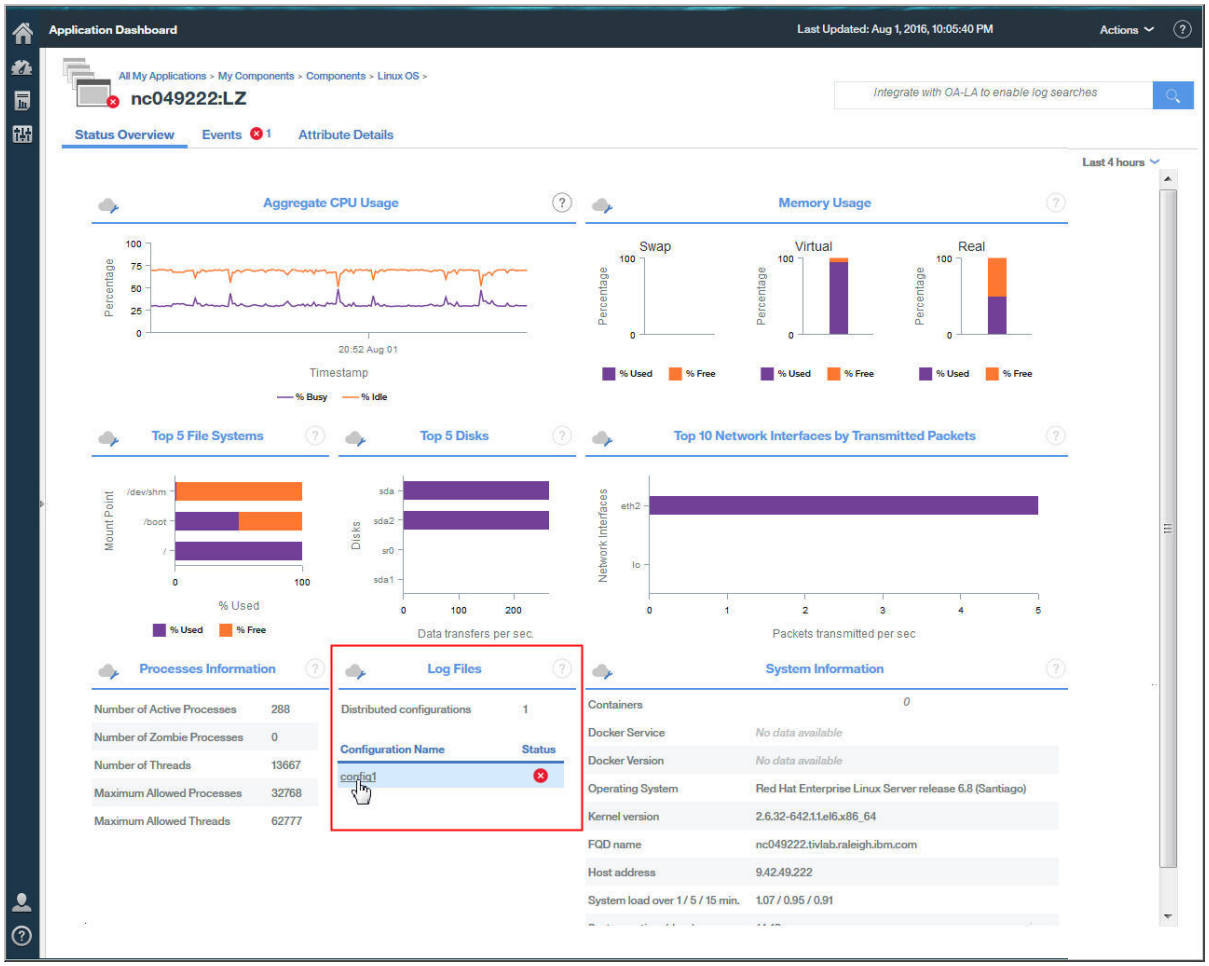
   Une fois que vous avez supprimé la configuration de la surveillance des fichiers journaux, la ressource de surveillance correspondante est conservée et reste en ligne jusqu'au redémarrage de l'agent de système d'exploitation. Les ressources de surveillance des fichiers journaux hors ligne sont supprimées une fois écoulé le délai indiqué dans l'option **Délai avant suppression d'un système hors ligne**.

Affichage du contenu de surveillance du fichier journal

Vous pouvez afficher la configuration de surveillance du fichier journal pour les agents de système d'exploitation déployés pour surveiller les fichiers journaux.

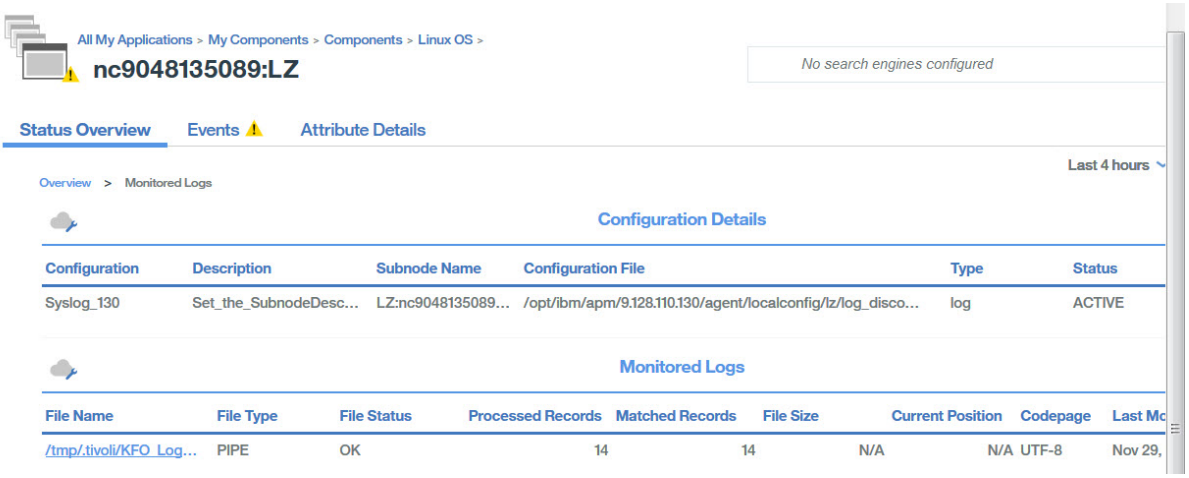
Procédure

1. Cliquez sur **Performance** > **Tableau de bord de performance d'application**, puis sélectionnez une application incluant l'agent de système d'exploitation où vous avez déployé la configuration de surveillance des fichiers journaux.
2. Descendez dans la hiérarchie jusqu'au tableau de bord de l'agent de système d'exploitation puis dans le widget Fichiers journaux, cliquez sur le profil pour afficher les configurations de surveillance des journaux distribuées et les journaux surveillés.

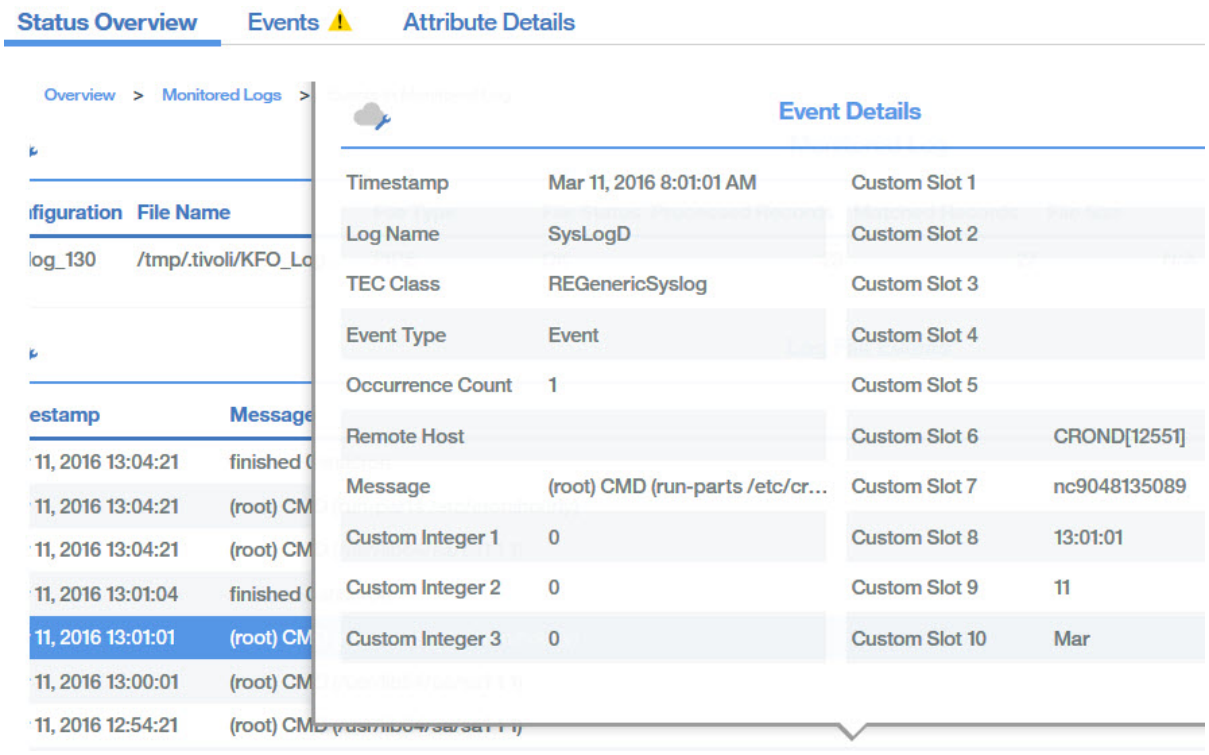


Les informations de configuration incluent le nom de la configuration, la description associée, le sous-noeud, le fichier de configuration, le statut et le code d'erreur.

3. Cliquez sur le nom du fichier journal pour afficher tous les événements de fichier journal qui sont associés au fichier journal.



4. Cliquez sur l'événement pour afficher les détails associés, par exemple toutes les zones définies dans le fichier de format.



Affichage des événements de surveillance des fichiers journaux
Après avoir configuré l'agent de système d'exploitation pour surveiller les fichiers journaux des applications, vous pouvez créer des seuils afin de déclencher des alarmes sur les conditions de fichier journal dont vous souhaitez être alerté.

Procédure

1. Dans la barre de navigation, cliquez sur l'icône **Configuration du système** > **Gestionnaire de seuils**.
2. Sélectionnez le système d'exploitation cible pour **Type de source de données**.
3. Cliquez sur Ajouter pour créer un nouveau seuil.
4. Définissez une gravité pour l'événement qui dépasse ce seuil.
5. Sélectionnez le jeu de données pour lequel vous souhaitez créer un seuil. Les jeux de données suivants sont admissibles pour la surveillance des fichiers journaux :
   - K*pp* : statistiques RegEx des fichiers journaux
   - K*pp* : statut des fichiers journaux
   - K*pp* : événements de profil des fichiers journaux
6. Cliquez sur **Ajouter** pour ajouter une condition. Dans la zone **Ajouter une condition**, sélectionnez un attribut et un opérateur, puis entrez une valeur de seuil.

   Au besoin, répétez cette procédure pour ajouter d'autres conditions à votre seuil.
7. Dans la section Affectation de groupes, sélectionnez le groupe de ressources auquel vous souhaitez affecter le seuil.
8. Cliquez sur **Sauvegarder**.
9. Dans la barre de navigation, cliquez sur l'icône **Configuration du système** > **Configuration avancée**.
10. Dans la catégorie **Intégration d'UI**, définissez la valeur **Activer les événements sous-noeud** sur True.
11. Cliquez sur **Sauvegarder**.

Résultats
Lorsque la condition indiquée a la valeur true, l'événement de fichier journal qui déclenche l'alerte apparaît dans l'onglet Evénements.

Variables d'environnement de la surveillance des fichiers journaux
Vous pouvez définir des variables d'environnement pour la surveillance des fichiers journaux dans les fichiers d'environnement de l'agent de système d'exploitation.

Définissez les variables d'environnement ci-dessous et remplacez K*PC* par le code de l'agent de système d'exploitation, où *PC* est le code d'agent de deux caractères, par exemple, klz est le code de l'agent de système d'exploitation Linux.

K*PC*_FCP_LOG
Cette variable est disponible dans le fichier *rép_install*/config/.*pc*.environment. La valeur par défaut est True et permet d'activer ou de désactiver la fonction de surveillance des journaux.

K*PC*_FCP_LOG_PROCESS_MAX_CPU_PCT
Ce paramètre est le pourcentage maximal autorisé de toutes les unités centrales système utilisées par l'agent au cours d'une minute. Les valeurs admises sont comprises entre 5 et 100. La valeur par défaut est 100. Ce paramètre est associé à la fonctionnalité de régulation de l'UC. Si vous définissez une valeur inférieure à 5, la valeur minimale de 5 est utilisée.

K*PC*_FCP_LOG_PROCESS_PRIORITY_CLASS
Ce paramètre définit la priorité du planificateur du système d'exploitation pour le processus. A est la priorité la plus faible, C la valeur par défaut du système d'exploitation et F la priorité la plus haute. Le paramètre est l'une des valeurs suivantes : A, B, C, D, E, F. Ces valeurs sont remplacées par toutes les valeurs que vous indiquez dans le fichier .conf.

K*PC*_FCP_LOG_SEND_EVENTS
Le paramètre par défaut est True et est utilisé par l'agent de système d'exploitation pour envoyer des événements au serveur Cloud APM.

K*PC*_FCP_LOG_SEND_EIF_EVENTS
Le paramètre par défaut est True. Si ce paramètre a pour valeur Yes, l'agent envoie les données d'événement au serveur Cloud APM ou à un récepteur EIF tel que la sonde OMNIbus EIF. Si ce paramètre a pour valeur No, l'agent n'envoie pas les données d'événement. La définition de ce paramètre est globale et s'applique à l'ensemble des profils de surveillance.

Remarque : Le récepteur EIF consomme des événements. Sinon, des problèmes peuvent se produire lorsque les données s'accumulent dans le cache de l'agent.

K*PC*_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN
Les agents de système d'exploitation qui surveillent les événements des fichiers journaux présentent une limitation de sous-noeud. Pour gérer les événements des fichiers journaux, le nom de système géré (MSN) du sous-noeud possède la structure suivante : UX:*NOMHOTECITRA_NOMPROFIL*. La longueur maximale du nom de sous-noeud est 32 caractères. Si le nom de système géré de sous-noeud généré dépasse cette longueur, il est tronqué à 32 caractères. Il correspond à la sous-chaîne extraite du nom du profil.

Dans le fichier de configuration d'agent de système d'exploitation, utilisez les variables suivantes pour gérer les noms de profil trop longs :

- Agent de système d'exploitation UNIX : KUX_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN=true
- Agent de système d'exploitation Linux : KLZ_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN=true
- Agent de système d'exploitation Windows : KNT_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN=true

Par exemple, si vous avez un agent appelé aixhost_nc123456789A de 20 caractères, CTIRAHOSTNAME=aixhost_nc123456789A comprend 20 caractères.

Si vous avez deux profils appelés :

```
ProfileLong12A (14 caractères)
ProfileLong12B (14 caractères)
```

les noms de systèmes gérés de sous-noeud associés suivants sont attendus :

```
UX:aixhost_nc123456789A_ProfileLong12A (38 caractères)
UX:aixhost_nc123456789A_ProfileLong12B (38 caractères)
```

Toutefois, les noms de systèmes gérés de sous-noeud sont tronqués à 32 caractères et les noms effectifs sont les mêmes pour les deux :

```
UX:aixhost_nc123456789A_ProfileL
UX:aixhost_nc123456789A_ProfileL
```

Pour tronquer CTIRAHOSTNAME au lieu du nom de profil, définissez la variable *Kpc_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN=true*.

Ainsi, si *n* est la longueur du nom de profil, disons 14, la sous-chaîne du nom de système géré liée à *CTIRAHOSTNAME* est tronquée à partir de 32-n-3 caractères. La variable *CTIRAHOSTNAME* est donc la suivante : `aixhost_nc1234`. Les noms de systèmes gérés de sous-noeud distinctifs sont alors :

```
UX:aixhost_nc1234_ProfileLong12A
UX:aixhost_nc1234_ProfileLong12B
```

Fichier de configuration
Les agents de système d'exploitation utilisent un fichier de configuration qui est lu par l'agent à son démarrage. Le fichier contient des options de configuration et des filtres. Vous devez créer ce fichier de configuration, puis configurer l'instance d'agent afin qu'elle l'utilise.

L'horodatage du fichier de configuration est surveillé toutes les 60 secondes. Si l'horodatage du fichier change, l'agent réinitialise sa configuration de manière dynamique sans redémarrer. Pour plus d'informations, voir «Modification des fichiers de configuration et de format de l'agent», à la page 668.

Le fichier `.conf` de l'agent de système d'exploitation accepte les options suivantes :

codepage
Page de codes du fichier surveillé. Utilisez ce paramètre dans le fichier de configuration lorsque la page de codes du fichier surveillé est différente de celle du système. Indiquez la page de codes du fichier surveillé, par exemple ibm-5348_P100-1997, UTF-16 ou UTF-8.

ConfigFilesAreUTF8=Y
Ce paramètre indique que le fichier de configuration et le fichier de format sont au format UTF-8. Utilisez ce paramètre si le codage des fichiers de configuration est UTF-8 et que la page de codes du système ne l'est pas. L'agent prend en charge le codage système (valeur par défaut).

DupDetectionKeyAttributes
Liste d'attributs Cloud APM séparés par des virgules et utilisés pour identifier les événements en double. Si tous les attributs nommés sont identiques dans deux événements, ces deux événements sont considérés comme des doublons. Cette option s'applique uniquement aux événements. Pour plus d'informations, voir «Filtrage et récapitulatif des événements», à la page 1047.

Remarque :

1. Les noms d'attribut sont sensibles à la casse. Vous devez donc entrer le nom exactement comme décrit.
2. Si vous ne spécifiez pas de liste d'attributs, les valeurs sont définies sur `Class` et `Logname` par défaut.

ENFORCE_STRICT_TEC_COMPATIBILITY
Ce paramètre fait référence à tous les caractères espaces figurant dans les données du journal pour s'assurer que les caractères sont respectés. Par exemple, lorsque vous utilisez le format `"%s %s"` pour extraire des informations de messages de journal, l'agent de système d'exploitation recherche non seulement un espace littéral mais également tout autre espace existant, comme des tabulations ou des retours chariot.

Lorsque ce paramètre n'est pas défini, le comportement par défaut de l'agent de système d'exploitation lors de la recherche d'une chaîne de format de style Tivoli Enterprise Console consiste à rechercher autant de texte d'entrée que possible en traitant le format de gauche à droite.

Par exemple, pour la chaîne de format `%s:%s` et la chaîne d'entrée `one:two:three`, l'agent de système d'exploitation affecte `un.deux` au premier paramètre (correspondant au premier caractère `%s`) et `trois` au second paramètre.

Remarque :

1. Ce paramètre ne s'applique pas aux instructions de format qui utilisent la syntaxe d'expression régulière.
2. La définition de ce paramètre a un impact sur les performances. Pour améliorer le comportement et les performances du processus de mise en correspondance, évitez de définir ce paramètre et utilisez des expressions régulières à la place.

EventSummaryInterval
Indique la durée en secondes pendant laquelle l'agent recherche des événements en double à supprimer. Définissez ce paramètre à un entier positif. Cette option s'applique uniquement aux événements. Pour plus d'informations, voir «Filtrage et récapitulatif des événements», à la page 1047.

EventFloodThreshold
Indique quels événements sont envoyés lorsque le système détecte des doublons parmi les événements. La valeur de ce paramètre est `send_none`, `send_all`, `send_first` ou un entier positif. Cette option s'applique uniquement aux événements. Pour plus d'informations, voir «Filtrage et récapitulatif des événements», à la page 1047.

EventMaxSize
Taille en octets maximale d'un événement généré. Si vous le spécifiez, ce paramètre est utilisé à deux endroits :

1. Le paramètre peut être utilisé par l'agent afin de définir la taille de la mémoire tampon utilisée pour le traitement des événements. S'il n'est pas défini, cette mémoire tampon a par défaut une taille de 16384 octets. Si la taille de la mémoire tampon est insuffisante, les événements sont tronqués et risquent d'être supprimés.
2. Le paramètre peut être utilisé par l'émetteur EIF afin de définir la taille de la mémoire tampon utilisée pour l'envoi des événements à un récepteur EIF (tel que la sonde OMNIbus EIF). S'il n'est pas défini, cette mémoire tampon a par défaut une taille de 4096 octets. Si la taille de la mémoire tampon est insuffisante, les événements sont supprimés.

FileComparisonMode
Indique quels fichiers journaux sont surveillés lorsque plusieurs fichiers journaux correspondent à un modèle générique. Les valeurs suivantes sont disponibles :

CompareByAllMatches
Cette valeur est le comportement par défaut. Tous les fichiers correspondant au modèle générique spécifié dans le paramètre `LogSources` sont surveillés.

CompareByLastUpdate
Parmi les fichiers correspondant au masque indiqué dans le paramètre `LogSources`, le fichier dont l'horodatage de mise à jour est le plus récent est surveillé.

CompareBySize
Si au moins deux fichiers correspondent aux critères de modèle de nom de fichier spécifiés, seul le fichier le plus volumineux est surveillé. N'utilisez pas la valeur `CompareBySize` avec des fichiers correspondants multiples qui sont mis à jour en même temps et dont la taille de fichier augmente. Si le fichier le plus volumineux est soumis à des changements fréquents, la surveillance risque de redémarrer indéfiniment au début du nouveau fichier sélectionné. Dans le cas de correspondances multiples où un seul fichier est actif et mis à jour à la fois, utilisez plutôt la valeur `CompareBySize`.

CompareByCreationTime
Parmi les fichiers correspondant au masque indiqué dans le paramètre LogSources, le fichier dont l'horodatage de création est le plus récent est surveillé. Cette valeur est soumise aux restrictions suivantes :

- La valeur ne concerne que les systèmes d'exploitation Windows car les systèmes d'exploitation UNIX et Linux n'enregistrent pas l'heure de création effective des fichiers.
- La valeur n'est pas prise en charge pour les fichiers distants surveillés par le biais du protocole SFTP/SSH (Secure Shell File Transfer Protocol).

Conseil : Les valeurs CompareByLastUpdate, CompareBySize et CompareByCreationTime peuvent toutes être utilisées pour la rotation des fichiers journaux. CompareByLastUpdate est généralement utilisé pour ces fichiers.

FQDomain
Indique si l'agent a défini un nom de domaine et la manière dont il l'a défini :

- Si ce paramètre a pour valeur yes, l'agent détermine le nom de domaine.
- Si ce paramètre a pour valeur no, l'agent ne définit pas le nom de domaine. L'attribut fqhostname comporte une chaîne vide.
- Si ce paramètre n'a pas pour valeur yes ou no, le système accepte le nom de domaine comme valeur et l'ajoute au nom d'hôte.

Pour plus d'informations, voir «Fichier de format », à la page 665.

IncludeEIFEventAttr
L'agent inclut un attribut volumineux appelé *EIFEvent*, qui correspond à une représentation de l'événement envoyé via la fonction EIF si cette fonction est activée. Les informations contenues dans l'attribut *EIFEvent* peuvent également se trouver dans d'autres attributs. Sa taille élevée étant problématique, il est désactivé par défaut. Indiquez la valeur y pour réactiver l'attribut EIFEvent.

Remarque : L'utilisation de cet attribut risque d'entraîner l'échec des seuils si les événements sont volumineux. Dans ce contexte, un événement volumineux désigne un événement où le nombre total d'octets nécessaires pour contenir l'ensemble des valeurs, des attributs et de leurs noms représente une chaîne de plus de 3600 octets.

LognameIsBasename
Lorsque vous indiquez y, la valeur de l'attribut Logname est le nom de base du fichier journal où l'événement a été détecté. Cette option s'applique uniquement aux événements Performance Management. Le chemin est supprimé. Par exemple, /data/logs/journal.log devient journal.log. Si ce paramètre a pour valeur n, le chemin complet est indiqué. L'attribut étant limité à 64 caractères, le nom sera donc tronqué s'il est plus long. Pour cette raison, la valeur par défaut est y. Pour visualiser le chemin complet dans un attribut plus long, vous pouvez l'indiquer dans la section de mappages dans un format du fichier .fmt, par exemple filename FILENAME CustomSlot1. Le mappage complète l'attribut nommé filename avec le chemin complet du fichier dans lequel l'événement a été détecté et le mappe à l'entrée CustomSlot1 de 256 caractères.

LogSources
Indique les fichiers journaux texte à interroger pour les messages. Le chemin d'accès complet de chaque fichier doit être spécifié et les noms de fichier doivent être séparés par des virgules. Dans chaque nom de fichier, vous pouvez également utiliser un astérisque (*) pour représenter une séquence de caractères ou un point d'interrogation (?) pour représenter un caractère seul. Par exemple, journal* renvoie tous les fichiers journaux dont le nom commence par le mot journal alors que journal??? renvoie tous les fichiers journaux dont le nom inclut journal suivi de trois caractères. Ces caractères génériques ne s'appliquent qu'au nom de fichier ; vous devez spécifier le chemin de manière explicite.

Si vous souhaitez utiliser des expressions régulières ou la correspondance de modèles dans le chemin, voir la description du paramètre RegexLogSources.

Une source de fichier journal n'a pas besoin d'exister lorsque l'agent est démarré ; le fichier journal est interrogé lors de sa création.

NewFilePollInterval
Indique la fréquence en secondes à laquelle l'agent vérifie les nouveaux fichiers à surveiller. Par exemple, supposons qu'un nom de fichier indiqué dans le paramètre *LogSources* ou *RegexLogSources* du fichier de configuration n'existe pas encore. Lorsque l'agent démarre, il vérifie à nouveau l'existence des fichiers à l'issue de cet intervalle.

NumEventsToCatchUp
Indique l'événement à partir duquel l'agent démarre dans le journal. Ce paramètre offre une certaine flexibilité si la source surveillée est nouvelle ou que l'agent est arrêté pour une période prolongée. Les valeurs suivantes sont valides :

Remarque : Pour les fichiers texte, les valeurs `0` et `-1` s'appliquent. Pour le journal des événements Windows, les valeurs `0`, `-1` et n s'appliquent.

`0`
Démarre au niveau de l'événement suivant des journaux. Cette valeur est la valeur par défaut.

`-1`
Lorsque le paramètre a pour valeur `-1`, l'agent enregistre sa position dans le fichier surveillé. Si l'agent est arrêté et redémarré plus tard, il pourra ainsi traiter tous les événements consignés dans le journal pendant son arrêt. En l'absence de ce paramètre, l'agent ignore les événements qui se sont produits alors qu'il était arrêté et redémarre à partir de la fin du fichier. Ce paramètre ne s'applique ni aux canaux, ni à la surveillance de syslog sur les systèmes UNIX et Linux.

n
La valeur est un entier positif. L'agent démarre à partir du *nième* événement par rapport à l'événement le plus récent consigné dans les journaux. Autrement dit, il démarre *n* événements avant l'événement le plus récent consigné dans les journaux. Si *n* est supérieur au nombre d'événements disponibles, tous les événements disponibles sont traités.

Remarque : Vous pouvez utiliser la valeur n uniquement avec le journal d'événements Windows. Le système ignore la valeur n lorsque le paramètre `UseNewEventLogAPI` est défini sur *y*.

PollInterval
Indique la fréquence en secondes à laquelle le système interroge chaque fichier journal spécifié dans le paramètre `LogSources` au sujet des nouveaux messages. La valeur par défaut est 5 secondes.

Si vous avez mis à jour un adaptateur de journal des événements Windows à partir d'une version précédente et que le paramètre `PollingInterval` est défini sur une valeur dans le registre Windows, vous devez définir le paramètre `PollInterval` sur la même valeur dans le fichier de configuration d'agent Windows. Cette règle s'applique uniquement si vous remplacez un agent de système d'exploitation Tivoli Enterprise Console qui avaient des valeurs dans le registre.

ProcessPriorityClass
Définit la priorité de processus pour l'agent. Vous pouvez ajuster cette valeur afin d'améliorer les performances système lorsque l'agent traite de grands volumes d'événements et sollicite trop de ressources processeur. Les valeurs admises sont :

- `A` - Priorité très faible
- `B` - Priorité faible
- `C` - Priorité moyenne
- `D` - Priorité moyenne haute
- `E` - Priorité élevée
- `F` - Priorité très élevée
- `USE_CONF_FILE_VALUE` - La valeur indiquée dans le fichier de configuration est utilisée. Cette valeur est la valeur par défaut.

RegexLogSources
Indique les fichiers journaux texte à interroger pour les messages. Ce paramètre est identique au paramètre LogSources, à ceci près que les métacaractères d'expression régulière peuvent être utilisés dans la partie nom de base du nom de fichier et dans un sous-répertoire du nom de fichier. Il

offre plus de flexibilité que le paramètre LogSources, car il permet de décrire plusieurs fichiers à surveiller dans plusieurs répertoires.

Par exemple, la définition de `/var/log/mylog*` pour l'instruction LogSources est comparable à l'utilisation du métacaractère point `(.)` suivi du métacaractère astérisque `(*)` pour former `/var/log/mylog.*` dans l'instruction RegexLogSources. Dans cet exemple, le système interroge tous les fichiers journaux du répertoire `/var/log` dont le nom de base commence par le mot `journal` suivi de zéro caractère ou plus. Avec la chaîne `/var/log/journal.+`, le système interroge tous les fichiers journaux du répertoire `/var/log` dont le nom de base commence par le mot `journal` suivi d'un caractère ou plus.

A l'instar de LogSources, le chemin d'accès complet de chaque fichier doit être spécifié et les noms de fichier doivent être séparés par des virgules. Notez toutefois que les virgules sont des caractères valides dans les expressions régulières. Pour établir une distinction entre une virgule utilisée dans une expression régulière et une virgule utilisée pour séparer des noms de fichier, les virgules utilisées dans une expression régulière doivent être associées au caractère d'échappement barre oblique inversée `(\)`.

Par exemple, si vous souhaitez rechercher des journaux correspondant à l'une des expressions régulières `/logs/.*\.log` et `/other/logs/[a-z]{0,3}\.log`, vous devez associer la clause `{0,3}` de la seconde expression au caractère d'échappement afin que l'agent ne la considère pas comme le début d'une nouvelle expression : `RegexLogSources=/logs/.*\.log,/other/logs/[a-z]{0\,3}\.log`

Si des métacaractères sont utilisés dans le nom de chemin, ils ne peuvent être utilisés que dans un seul sous-répertoire du chemin. Par exemple, vous pouvez spécifier `/var/log/[0-9\.]*/journal.*` pour avoir des métacaractères dans un sous-répertoire. La chaîne `[0-9\.]*` fait correspondre les sous-répertoire de `/var/log` comportant uniquement des chiffres et des points `(.)`. La chaîne `mylog.*` fait correspondre les noms des fichiers des sous répertoires `/var/log` qui commencent par le mot `journal` et suivis de zéro caractère ou plus.

Etant donné que certains systèmes d'exploitation utilisent la barre oblique inversée `(\)` comme séparateur de répertoire, il peut être confondu avec un métacaractère d'échappement d'expression régulière. Pour éviter cette confusion, des barres obliques doivent toujours être utilisées pour désigner des répertoires. Par exemple, les fichiers Windows qui sont spécifiés sous la forme `C:\temp\mylog. *` peuvent signifier que le `\t` est un caractère de tabulation abrégé. Par conséquent, utilisez toujours des barres obliques `(/)` comme séparateurs de répertoire sur tous les systèmes d'exploitation. Par exemple, `C:/temp/mylog.*` représente tous les fichiers du répertoire `C:/temp` qui commencent par `mylog`.

Si plusieurs sous-répertoires contiennent des métacaractères, un message de trace est également généré. Par exemple, `c:/[0-9\.]*/temp.files/journal.*` inclut deux sous-répertoires qui contiennent des métacaractères. `[0-9\.]*` est le premier sous-répertoire défini avec des métacaractères et `temp.files` est le deuxième sous-répertoire qui utilise le métacaractère point `(.)`. Dans ce cas, l'agent considère que le premier sous-répertoire défini avec le métacaractère est utilisé et que les répertoires suivants possédant des métacaractères sont ignorés.

SubnodeName
Valeur de chaîne pouvant être utilisée pour remplacer le nom par défaut affecté à un sous-noeud de profil de surveillance. Par défaut, le nom de sous-noeud affecté à un profil de surveillance correspond au nom de base du fichier de configuration utilisé pour ce profil. En utilisant ce paramètre, il est possible d'affecter un nom de sous-noeud différent.

SubnodeDescription
Valeur de chaîne pouvant être utilisée pour affecter une valeur à l'attribut *Subnode Description* de *LFAProfiles*.

UnmatchLog
Permet d'indiquer un fichier dans lequel sont consignés les événements supprimés qui ne peuvent pas être analysés dans une classe d'événement par l'agent. Les événements supprimés peuvent ensuite être analysés pour déterminer si le format de fichier de l'agent doit faire l'objet de

modifications. Les événements correspondant à un masque qui utilise *DISCARD* n'apparaissent pas dans le journal de non correspondance, car ils correspondent à un masque.

Cette option est utilisée dans un environnement de test pour valider les filtres dans le fichier de format. Elle peut entraîner la saturation de votre système de fichiers si vous la conservez pendant des périodes prolongées.

Options pour la surveillance à distance des fichiers via le protocole SSH

A part **SshHostList**, qui est une liste, tous les paramètres ne peuvent avoir qu'une seule valeur, qui est appliquée à tous les hôtes distants spécifiés dans **SshHostList**.

Seuls les fichiers journaux texte sont pris en charge. Le rapport d'erreur AIX, syslog et le journal des événements Windows ne sont pas pris en charge.

Conseil : Vous pouvez configurer syslog pour placer sa sortie dans un fichier journal, puis surveiller à distance ce fichier texte avec l'agent de système d'exploitation.

SshAuthType
Doit avoir pour valeur *PASSWORD* ou *PUBLICKEY*. Si ce paramètre a pour valeur *PASSWORD*, la valeur de **SshPassword** est considérée comme le mot de passe à utiliser pour l'authentification SSH avec tous les systèmes distants. S'il a pour valeur *PUBLICKEY*, la valeur de **SshPassword** est considérée comme la phrase de passe qui contrôle l'accès au fichier de clés privées. Si ce paramètre a pour valeur *PUBLICKEY*, **SshPrivKeyfile** et **SshPubKeyfile** doivent également être indiqués.

SshHostList
Liste séparée par des virgules des hôtes distants à surveiller. Tous les fichiers journaux spécifiés dans les instructions **LogSources** ou **RegexLogSources** sont surveillés sur chacun des hôtes figurant dans cette liste. Si l'un des noms d'hôte indiqués est *localhost*, l'agent surveille le même ensemble de fichiers directement sur le système local. Lorsque vous indiquez *localhost*, le protocole SSH n'est pas utilisé pour accéder aux fichiers sur le système local ; les fichiers journaux sont lus directement.

SshPassword
Lorsque la valeur de **SshAuthType** est *PASSWORD*, cette valeur correspond au mot de passe du compte de l'utilisateur spécifié dans **SshUserid**. Vous pouvez indiquer le mot de passe du compte sous la forme d'un texte en clair ou indiquer un mot de passé chiffré à l'aide de la commande CLI IBM Tivoli Monitoring **itmpwdsnmp**. Pour savoir comment procéder pour chiffrer un mot de passe à l'aide de la commande **itmpwdsnmp**, voir «Surveillance des fichiers journaux distants : Chiffrement d'un mot de passe ou d'une phrase de passe», à la page 674.

Lorsque la valeur de **SshAuthType** est *PUBLICKEY*, cette valeur correspond à la phrase de passe qui permet de déchiffrer la clé privée spécifiée par le paramètre **SshPrivKeyfile**. Vous pouvez indiquer la phrase de passe sous la forme d'un texte en clair ou indiquer une phrase de passe chiffrée à l'aide de la commande CLI IBM Tivoli Monitoring **itmpwdsnmp**. Pour savoir comment procéder pour chiffrer un mot de passe à l'aide de la commande **itmpwdsnmp**, voir «Surveillance des fichiers journaux distants : Chiffrement d'un mot de passe ou d'une phrase de passe», à la page 674.

Remarque : Si la valeur de **SshAuthType** est *PUBLICKEY* et que vous avez configuré SSH afin qu'aucune phrase de passe ne soit nécessaire, **SshPassword** doit avoir pour valeur NULL. Pour associer **SshPassword** à la valeur NULL, l'entrée du fichier de configuration est :

```
SshPassword=
```

SshPort
Port TCP auquel se connecter pour utiliser SSH. Si ce paramètre n'est pas défini, il prend par défaut la valeur *22*.

SshPrivKeyfile
Si **SshAuthType** a pour valeur *PUBLICKEY*, cette valeur doit correspondre au chemin complet du fichier contenant la clé privée de l'utilisateur indiqué dans **SshUserid**, et **SshPubKeyfile** doit également être défini. Si **SshAuthType** n'a pas pour valeur *PUBLICKEY*, cette valeur n'est pas nécessaire et elle est ignorée.

SshPubKeyfile
Si **SshAuthType** a pour valeur *PUBLICKEY*, cette valeur doit correspondre au chemin complet du fichier contenant la clé publique de l'utilisateur indiqué dans **SshUserid**, et **SshPrivKeyfile** doit également être défini. Si **SshAuthType** n'a pas pour valeur *PUBLICKEY*, cette valeur n'est pas nécessaire et elle est ignorée.

SshUserid
Nom d'utilisateur sur des systèmes distants que l'agent utilise pour l'authentification SSH.

Option prise en charge sur les systèmes UNIX et Linux uniquement

Linux AIX

AutoInitSyslog
Si cette option a pour valeur `Yes`, l'agent configure automatiquement l'utilitaire syslog pour consigner un ensemble standard d'événements dans un canal surveillé par l'agent. En l'activant, vous pouvez surveiller les événements syslog sans être obligé de gérer et remettre à zéro les fichiers journaux. Si cette option n'est pas définie dans le fichier de configuration, cela revient à utiliser la valeur `No`.

Restriction : Cette option n'est pas prise en charge pour la surveillance du fichier journal à distance.

Options prises en charge sur les systèmes Windows uniquement

Windows

NTEventLogMaxReadBytes
Si vous utilisez l'ancienne interface du journal des événements NT (`UseNewEventLogAPI` non défini sur y) pour lire les données du journal des événements sur un système Windows, l'agent lit les données jusqu'à ce nombre d'octets chaque fois qu'il vérifie la présence de nouvelles données dans le journal des événements. Si ce paramètre a pour valeur `0`, l'agent essaie de lire toutes les nouvelles données comme il le faisait dans les versions antérieures. Cette activité peut solliciter l'agent pendant longtemps si le système comporte un grand volume d'événements. La valeur par défaut est `655360`. Si vous définissez ce paramètre, il se peut que l'agent ne s'arrête pas exactement à la valeur indiquée, mais plutôt vers le multiple le plus proche de la taille de la mémoire tampon interne par rapport à cette valeur.

PreFilter
Indique la façon dont les événements d'un journal d'événements Windows sont filtrés avant le traitement par l'agent. Les instructions `PreFilter` sont utilisées par `PreFilterMode` au moment où les filtres déterminent quels événements du journal des événements doivent être envoyés à l'agent. Un événement correspond à une instruction `PreFilter` lorsque chaque spécification *attribut=valeur* de l'instruction `PreFilter` correspond à un événement du journal d'événements. Une instruction PreFilter doit contenir au moins la spécification de journal et peut comporter jusqu'à trois spécifications supplémentaires (toutes facultatives) : l'ID d'événement, le type d'événement et la source d'événement. L'ordre des attributs dans l'instruction importe peu.

Le format de l'instruction `PreFilter` est le suivant :

```
PreFilter:Log=log_name;EventId=value; EventType=value;Source=value;
```

Vous pouvez indiquer plusieurs valeurs pour chaque attribut en les séparant par des virgules.

Chaque instruction `PreFilter` doit se trouver sur une ligne distincte.

Le paramètre `PreFilter` n'est pas obligatoire. Tous les événements du journal d'événements Windows sont envoyés à l'agent si aucun préfiltre n'est spécifié et que le paramètre `PreFilterMode=OUT` est utilisé.

PreFilterMode
Ce paramètre s'applique uniquement au journal d'événements Windows. Il permet de spécifier si les événements du journal des événements Windows correspondant à une instruction `PreFilter` sont envoyés (`PreFilterMode=IN`) ou ignorés (`PreFilterMode=OUT`). Les valeurs admises sont `IN`, `in`, `OUT` et `out`. La valeur par défaut est `OUT`.

Le paramètre PreFilterMode est facultatif. S'il n'est pas spécifié, seuls les événements ne correspondant à aucune instruction PreFilter sont envoyés à l'agent.

Remarque : Si vous définissez le paramètre PreFilterMode=IN, vous devez également définir les instructions PreFilter.

SpaceReplacement
Ce paramètre correspond pas défaut à TRUE pour le journal d'événements Windows (Windows Server 2008 uniquement) mais pas pour les versions précédentes du journal des événements. Lorsque le paramètre SpaceReplacement a pour valeur TRUE, tous les espaces figurant dans les zones security ID, subsource, Level et keywords des messages du journal d'événements sont remplacés par des traits de soulignement (_). Lorsque le paramètre SpaceReplacement a pour valeur FALSE, tous les espaces figurant dans les zones security ID, subsource, Level et keywords des messages du journal d'événements sont conservés. Pour plus d'informations sur ce paramètre, voir «Journal des événements Windows», à la page 1049.

UseNewEventLogAPI
Lorsque ce paramètre a pour valeur y sur les systèmes Windows, l'agent utilise la nouvelle interface de journal d'événements Windows pour analyser les journaux d'événements. Le paramètre est pris en charge sur les systèmes Windows 2008 et version ultérieure uniquement. Il permet d'accéder à la plupart des nouveaux journaux d'événements débutés dans Windows 2008, ainsi qu'aux applications qui s'exécutent dessus. Ce paramètre est ignoré sur les versions antérieures de Windows et sur les systèmes UNIX et Linux. Pour plus d'informations sur ce paramètre, voir «Journal des événements Windows», à la page 1049.

WINEVENTLOGS
Permet de contrôler quels journaux d'événements Windows sont contrôlés.

L'instruction WINEVENTLOGS est une liste délimitée par des virgules, sans espaces. Pour plus d'informations, voir «Journal des événements Windows», à la page 1049.

Remarque : Les retours chariot, tabulations ou nouvelles lignes figurant dans les événements Windows sont remplacés par des espaces.

Option prise en charge sur les systèmes AIX uniquement

AIX

AIXErrptCmd
Permet d'indiquer une chaîne de commande **errpt** (rapport d'erreur) qui sera exécutée par l'agent. Le résultat de la commande est importé dans le flux de données de journal faisant l'objet d'une surveillance.

Dans l'exemple de commande ci-dessous, l'agent recherche la chaîne *mmjjhhmmaa* et la remplace par la date et l'heure de démarrage. Seule la première occurrence de la chaîne est remplacée.

```
AIXErrptCmd=errpt -c -smmddhhmmyy
```

Bien que vous puissiez indiquer votre propre commande errpt, vous devez utiliser l'option -c (mode simultané) afin que la commande s'exécute en continu. Vous ne pouvez pas utiliser l'option -t, ni les options suivantes qui donnent lieu à la sortie détaillée : -a, -A ou -g.

Le flux de données est le résultat standard de la commande errpt. Par conséquent, les expressions régulières du fichier .fmt doivent être écrites de telle sorte qu'elles correspondent. Par exemple, la commande pourrait renvoyer la sortie de données suivante :

```
IDENTIFIER TIMESTAMP  T C RESOURCE_NAME  DESCRIPTION
F7FA22C9   0723182911 I O SYSJ2      UNABLE TO ALLOCATE SPACE IN FILE SYSTEM
2B4F5CAB   1006152710 U U ffdc       UNDETERMINED ERROR
2B4F5CAB   1006152610 U U ffdc       UNDETERMINED ERROR
```

Exemple de format qui utilise les lignes de données, mais pas l'en-tête :

```
REGEX GenericErrpt
^([A-F0-9]{8}) +([0-9]{10}) ([A-Z]) ([A-Z]) (\S+) +(.*)$
Identifier $1 CustomSlot1
```

```
Timestamp  $2 CustomSlot2
T          $3 CustomSlot3
C          $4 CustomSlot4
Resource   $5 CustomSlot5
msg        $6
END
```

Pour plus d'informations, voir *Monitoring an AIX Binary Log* dans le IBM Agent Builder - Guide d'utilisation.

Options qui s'appliquent uniquement lorsque des événements sont transmis à un récepteur EIF

Important : Ces options sont applicables à des événements EIF envoyés directement à Operations Analytics - Log Analysis, OMNIbus ou tout autre récepteur générique EIF. Elles ne sont pas destinées à être utilisées avec le serveur Cloud APM.

BufferEvents
Indique comment le stockage temporaire d'événements est activé. Les valeurs admises sont :

- **YES** - Stocke les événements dans le fichier spécifié par le paramètre BufEvtPath (valeur par défaut).
- **MEMORY_ONLY** - Stocke les événements dans une mémoire temporaire.
- **NO** - Ne stocke pas les événements dans une mémoire permanente ou temporaire.

BufEvtPath
Indique le chemin d'accès complet du fichier cache de l'agent. Si ce chemin d'accès n'est pas rectifié, la valeur par défaut est :

- AIX `/etc/Tivoli/tec/cache`
- Windows `\etc\Tivoli\tec\cache`

Remarque : Si des événements sont transmis à plusieurs serveurs, vous devez spécifier une valeur *BufEvtPath* pour chaque canal de transmission. Un numéro d'index est ajouté au nom *BufEvtPath* de chaque entrée supplémentaire. Par exemple, utilisez le paramètre *BufEvtPath1* pour préciser le nom de chemin du fichier cache de l'agent aux fins de transmission vers le premier serveur supplémentaire. La valeur définie pour chaque paramètre *BufEvtPath* doit être unique.

BufEvtMaxSize
Indique la taille maximale en kilo-octets du fichier cache de l'agent. La valeur par défaut est 64. Lorsque le paramètre *BufferEvents* a pour valeur Yes, le fichier cache stocke les événements sur le disque. La taille minimale pour le fichier est 8 ko. Le système ignore toutes les tailles de fichier inférieures et utilise à la place la valeur 8 ko. Il n'existe pas de limite supérieure pour la valeur que vous avez spécifiée pour la taille maximale du fichier.

Remarque : Si le fichier cache existe déjà, vous devez supprimer le fichier afin de prendre en compte vos modifications.

NO_UTF8_CONVERSION
Indique si Event Integration Facility (EIF) encode les données d'événement au format UTF-8. Lorsque vous associez ce paramètre à YES, Event Integration Facility n'encode pas les données d'événement au format UTF-8. Le système suppose que les données ont déjà un encodage UTF-8 lorsqu'elles sont transmises à Event Integration Facility. Toutefois, un préfixe est ajouté à l'indicateur pour signaler que les données possèdent un encodage in UTF-8 (si l'indicateur n'existe pas au début des données d'événement). La valeur par défaut est N0.

MaxEventQueueDepth
Spécifie le nombre maximal d'événements pouvant être placés en file d'attente à des fins de transmission. Lorsque la limite est atteinte, chaque nouvel événement placé dans la file d'attente supplante l'événement le plus ancien dans la file d'attente. Si vous ne définissez pas ce paramètre, la valeur par défaut est 1 000. Ce paramètre s'applique à l'ensemble des canaux de transmission si *NumAdditionalServers* est utilisé.

NumAdditionalServers
Cette entrée est nécessaire si vous souhaitez transmettre des événement à plusieurs serveurs d'objets Netcool/OMNIbus. Il permet d'indiquer le nombre de serveurs auxquels les événements sont transmis. Les valeurs admises sont comprises entre 1 et 8.

ServerLocation
Indique le nom de l'hôte sur lequel le serveur d'événements est installé. Indiquez le nom de hôte ou l'adresse IP. Utilisez le format à points pour l'adresse IP. Si vous le souhaitez, vous pouvez indiquer des valeurs de reprise en ligne pour les emplacements du serveur, telles que `ServerLocation1=2.3.4.5.2.3.4.6` ; si vous indiquez des valeurs pour *ServerLocation*, vous devez également indiquer une valeur *ServerPort* supplémentaire pour chaque *ServerLocation*.

Remarque : Si des événements sont transmis à plusieurs serveurs, vous devez indiquer une valeur *ServerLocation* pour chaque serveur. Un numéro d'index est ajouté au nom *ServerLocation* de chaque entrée supplémentaire. Par exemple, utilisez *ServerLocation1* pour spécifier le nom de l'hôte sur lequel le premier serveur supplémentaire est installé.

ServerPort
Indique le numéro de port sur lequel le récepteur EIF écoute les événements. Le paramètre *ServerPort* peut contenir jusqu'à huit valeurs, séparées par des virgules. Si vous indiquez des valeurs de basculement pour le paramètre *ServerLocation*, vous devez définir une valeur *ServerPort* équivalente. ServerPort n'est pas utilisé lorsque le paramètre *TransportList* est indiqué.

Remarque : Si des événements sont transmis à plusieurs serveurs, vous devez spécifier une valeur *ServerPort* pour chaque serveur. Un numéro d'index est ajouté au nom *ServerPort* de chaque entrée supplémentaire. Par exemple, utilisez *ServerPort1* afin d'indiquer le numéro de port sur lequel le récepteur EIF écoute les événements pour le premier serveur supplémentaire.

TransportList
Indique les noms définis par l'utilisateur des mécanismes de transport, séparés par des virgules. Lorsqu'un mécanisme de transport échoue pour des applications expéditrices, l'API utilise les mécanismes de transport suivants dans l'ordre indiqué dans la liste. Pour les applications réceptrices, l'API crée et utilise tous les mécanismes de transport. Le type et le canal de transport de chaque *nom_type* doivent être spécifiés au moyen des mots clés Type et Channels :

***nom_type*Type**

Indique le type de transport du mécanisme de transport défini par le paramètre *TransportList*. SOCKET est le seul type de transport pris en charge.

Le serveur et le port de chaque nom_canal sont indiqués par les paramètres *ServerLocation* et *ServerPort*.

***nom_type*Channels**

***nom_canal*Port**
Indique le numéro de port sur lequel le serveur de mécanismes de transport écoute le canal indiqué (indiqué par le paramètre *Channel*). Lorsque ce mot clé a pour valeur zéro, l'associateur de port est utilisé. Ce mot clé est obligatoire.

***nom_canal*PortMapper**
Active l'associateur de port pour le canal indiqué.

***nom_canal*PortMapperName**
Si l'associateur de port est activé, indique le nom de l'associateur de port.

***nom_canal*PortMapperNumber**
Indique l'ID enregistré par l'appel de procédure distante (RPC).

***nom_canal*PortMapperVersion**
Si l'associateur de port est activé, indique la version de l'associateur de port.

***nom_canal*ServerLocation**
Indique le nom du serveur d'événements et de la région sur laquelle le serveur de mécanismes de transport se trouve pour le canal indiqué. Le canal est défini par le paramètre *Channel*. Ce mot clé est obligatoire.

Le fichier de configuration EIF accepte les options EIF génériques lorsqu'il est utilisé directement avec OMNIbus. Ces options fonctionnent uniquement sur une connexion EIF avec OMNIbus. Ils n'affectent pas les événements qui sont envoyés au serveur Cloud APM. Pour plus d'informations sur ces options EIF, voir EIF keywords.

Fichier de format
Les agents de système d'exploitation extraient les messages des journaux système, puis établissent une concordance entre différents messages de journal à des classes d'événement. Pour effectuer cette association, ils utilisent un fichier de format comme fichier de recherche pour déterminer quelle classe d'événement ils doivent lire, sur quoi effectuer la correspondance et la manière de formater les données.

Lorsque le fichier de format est utilisé comme fichier de recherche, le système compare toutes les spécifications de format figurant dans le fichier en commençant par le début du fichier. Si deux classes correspondent ou qu'il existe plusieurs classes correspondantes pour un message, le système utilise la première expression qu'il trouve à partir de la fin du fichier. Si aucune correspondance n'est trouvée, l'événement est supprimé. Un événement supprimé est consigné dans le journal de non correspondance s'il est défini dans le fichier `.conf`.

La syntaxe d'expression régulière permettant de créer des masques pour établir des correspondances entre les messages de journal et des événements est décrite. Le filtrage d'expression régulière est pris en charge via des bibliothèques ICU (International Components for Unicode) pour vérifier si une valeur d'attribut examinée correspond ou non au modèle indiqué.

Pour plus d'informations sur l'utilisation d'expressions régulières, visitez la page sur les expressions régulières dans le document *ICU User Guide*.

Spécifications du fichier de format
Le fichier de format décrit les modèles que l'agent recherche pour faire correspondre des événements dans les journaux surveillés. Il se compose d'une ou de plusieurs spécifications de format.

Vous pouvez modifier le fichier de format pendant qu'une instance d'agent est en cours d'exécution. L'agent lit le fichier au démarrage et surveille son horodatage toutes les 60 secondes. Si l'horodatage du fichier change, l'agent réinitialise sa configuration de manière dynamique sans redémarrer. Pour plus d'informations, voir «Modification des fichiers de configuration et de format de l'agent», à la page 668.

Si vous créez de nouveaux modèles pour faire correspondre un événement, utilisez la nouvelle syntaxe d'expression régulière. Elle se compose des éléments suivants :

- En-tête de format
- Expression régulière
- Mappages d'attribut
- Instruction End

L'en-tête de format contient le mot clé **REGEX**, qui indique à l'agent que vous utilisez une expression régulière pour rechercher une correspondance au modèle dans le journal surveillé.

Vous affectez cette expression régulière à une classe d'événement comme indiqué dans l'exemple suivant :

```
REGEX REExample
```

Si vous utilisez la classe d'événement spéciale prédéfinie `*DISCARD*` comme classe d'événement, tous les enregistrements de journal correspondant au modèle associé sont supprimés et aucun événement n'est généré pour eux. Par exemple :

```
REGEX *DISCARD*
```

Lorsque le système a trouvé une correspondance, il ne consigne aucune donnée dans le journal de non concordance. Les correspondances d'enregistrements de statut du fichier journal incluent ces événements supprimés.

Remarque : Vous pouvez affecter plusieurs définitions d'événement soit à la même classe d'événement, soit à différentes classes d'événement. Le nom de classe est arbitraire ; vous pouvez l'utiliser pour spécifier le type d'événement ou regrouper des événements de différentes manières.

Placé en-dessous de l'en-tête de format, le contenu de format se compose d'une expression régulière sur la première ligne et de mappages. Chaque mappage figure sur une ligne distincte (voir exemple suivant).

Toutes les lignes correspondant aux expressions régulières sont sélectionnées et envoyées au serveur de surveillance en tant qu'événements. L'expression régulière contient des sous-expressions. Celles-ci vous permettent d'associer certaines parties spécifiques de ces lignes qui sont identiques à une variable appelée *attribut* (slot) dans la fonction d'intégration d'événements (EIF).

Le journal de surveillance illustré ici contient trois lignes que vous pouvez surveiller :

```
Error:  disk failure
Error: out of memory
WARNING: incorrect login
```

Par exemple, supposons que vous générez un événement pour une erreur spécifique, telle que les lignes commençant par `Error` et que vous ignorez les lignes commençant par `Warning`. L'expression régulière doit correspondre aux lignes commençant par `Error` et doit également comporter une sous-expression. La sous-expression est placée entre parenthèses et doit uniquement correspondre au texte de saisie que vous souhaitez affecter à l'attribut *msg*. La définition de format ci-dessous est une expression régulière simple composée d'une seule sous-expression :

```
REGEX REExample
Error: (.*)
msg $1
END
```

En fonction de cette spécification de format et de l'ensemble de données de journal précédent, l'agent génère deux événements. La classe d'événement REEXample est affectée à ces deux événements. Dans le premier événement, la valeur `disk failure` est affectée à l'attribut *msg*. De la même manière, la valeur out of memory est affectée à l'attribut *msg* dans le second événement. Comme la ligne `Warning` ne correspond pas à l'expression régulière, le système l'ignore et ne génère aucun événement.

Lorsque vous affectez la valeur $1 à l'attribut *msg*, vous lui affectez la valeur de la première sous-expression.

Si le journal a consigné les erreurs suivantes, vous pouvez affecter ces messages d'erreur à leur propre classe d'événement afin que le système vous informe immédiatement en cas de panne de disque :

```
Error: disk failure on device /dev/sd0: bad sector
Error: disk failure on device /dev/sd1: temperature out of range
```

Vous pouvez inclure une description du disque sur lequel l'erreur s'est produite et détailler plus précisément l'erreur de disque dans l'événement.

L'expression régulière suivante contient deux sous-expressions qui identifient ces informations :

```
REGEX DiskFailure
Error: disk failure on device (/dev/sd[0-9]):(.*)
device $1 CustomSlot1
msg $2
END
```

Vous affectez ces deux sous-expressions à des attributs d'événement. Les deux événements générés contiennent les valeurs suivantes :

```
"device=/dev/sd0" and "msg=bad sector"
"device=/dev/sd1" and "msg=temperature out of range"
```

Si vous utilisez la fonction d'intégration d'événements pour générer le premier événement, elle s'affiche comme indiqué dans l'exemple suivant :

```
DiskError;device='/dev/sd0';msg='bad sector';END
```

Si l'événement est envoyé au serveur Cloud APM, l'attribut nommé *msg* est affecté à l'attribut d'agent Performance Management qui porte le même nom. Mais l'attribut *device* ne comporte pas d'attribut prédéfini.

Si vous devez visualiser la valeur affectée à *device* directement dans la console Cloud APM ou créer des seuils associés, vous devez l'affecter à un attribut Performance Management.

L'agent de système d'exploitation inclut les treize attributs prédéfinis suivants :

- Dix attributs de type chaîne allant de *CustomSlot1* à *CustomSlot10*
- Trois attributs de type entier allant de *CustomInteger1* à *CustomInteger3*

L'utilisation de ces noms d'attribut dans le fichier de format entraîne la définition des attributs Performance Management qui portent le même nom. L'utilisation de ces attributs n'affecte pas le contenu de l'événement EIF envoyé directement à OMNIbus.

Remarque : Les noms d'attribut `CustomSlot` et `CustomInteger` sont sensibles à la casse. Vous devez donc entrer le nom exactement comme indiqué.

Vous affectez un attribut de la définition d'événement à l'un des ces attributs personnalisés Performance Management dans le fichier de format.

Vous affectez l'attribut *device* à l'attribut de type de chaîne Performance Management appelé *CustomSlot1*, comme indiqué dans l'exemple suivant :

```
REGEX DiskFailure
Error: disk failure on device (/dev/sd[0-9]):(.*)
device $1 CustomSlot1
msg $2
END
```

Lorsque l'événement s'affiche dans le Tableau de bord d'Application Performance, la valeur affectée à l'attribut *device* est affectée à l'attribut Performance Management appelé `CustomSlot1`. Vous pouvez afficher cette valeur dans la console Cloud APM ou l'utiliser pour définir des seuils. Vous pouvez affecter de la même manière n'importe quel attribut de la définition d'événement à l'un des dix attributs d'agent personnalisés en indiquant "`CustomSlot`*n*", où *n* est un nombre compris entre 1 à 10, à côté de la définition d'attribut.

Dans cet exemple, la première sous-expression est définie de manière spécifique sous la forme `(/dev/sd[0-9])`, mais la seconde sous-expression est définie de manière générale sous la forme `(.*)`. Lorsque vous définissez l'expression régulière de la manière la plus spécifique possible, vous améliorez les performances du système. Par conséquent, si vous entrez une recherche pour trouver une erreur sur une unité ne correspondant pas au message d'erreur spécifique défini ici, la procédure de recherche s'arrête immédiatement lorsque l'erreur est introuvable. Le système ne perd pas de temps à rechercher de correspondance.

Le mot clé *END* complète la spécification de format. L'en-tête de format, l'expression régulière et le mot clé *END* doivent commencer sur une nouvelle ligne comme indiqué dans l'exemple suivant :

```
REGEX REExample
Error:
msg $1
END <EOL>
<EOF>
```

Remarque : Pour le dernier format du fichier, vous devez insérer une nouvelle ligne après le mot clé `END` comme indiqué dans l'exemple. Sinon, le système générera une erreur d'analyse.

Les attributs entiers personnalisés *CustomInteger1* à *CustomInteger3* sont des attributs entiers 64 bits. Vous pouvez les utiliser de la même manière que les attributs chaînes `CustomSlot`. Vous pouvez utiliser ces attributs pour mapper des attributs ou des sous-expressions spécifiques du fichier journal à des

attributs Cloud APM spécifiques. Comme ces attributs sont numériques, vous pouvez leur appliquer des comparaisons arithmétiques (< et > par exemple), ce qui n'est pas possible avec les attributs de chaîne.

Remarque : Bien que ces valeurs soient considérées comme des entiers par le serveur Cloud APM, elles sont toujours traitées comme des chaînes pour EIF et dans le fichier de format. Pour utiliser un attribut entier dans une instruction PRINTF, vous l'identifiez donc toujours sous la forme “%s” et non “%d”.

L'exemple suivant illustre l'utilisation d'un attribut entier personnalisé. Supposons que le système reçoive un message UNIX syslog périodique indiquant le pourcentage d'espace libre sur le système de fichiers comme dans l'exemple d'enregistrement de journal suivant :

```
Oct 24 11:05:10 jimmy fschecker[2165]: Filesystem /usr is 97% full.
```

Vous pouvez utiliser l'instruction suivante dans le fichier de format pour vérifier le pourcentage d'espace libre sur le système de fichiers :

```
REGEX FileSystemUsage
^([A-Z][a-z]{2}) ([ 0-9][0-9]) ([0-9]{2}:[0-9]{2}:[0-9]{2}) (.*?) (.*?):
Filesystem (.*?) is ([0-9]+)% full\.$
Month   $1 CustomSlot1
Date    $2 CustomSlot2
Time    $3 CustomSlot3
Host    $4 CustomSlot4
Service $5 CustomSlot5
Filesystem     $6 CustomSlot6
PctFull         $7  CustomInteger1
msg          PRINTF("%s: %s% full", Filesystem, PctFull)
END
```

Remarque : Dans l'instruction précédente, le code figurant entre les symboles ^ et $ sur les lignes 2 et 3 doit figurer sur une seule ligne.

Il se peut que d'autres événements insèrent des valeurs dans l'attribut *CustomInteger1*. Pour ne pas faire de confusion entre les différents types d'événement, vous pouvez utiliser la valeur de l'attribut *Class* pour limiter son effet au type d'événement approprié. Par exemple, la formule de seuil suivante entraîne le déclenchement du seuil uniquement lorsqu'un événement de la classe d'événement *FileSystemUsage* possède une valeur supérieure ou égale à 95 dans *CustomInteger1*:

```
(  Class == 'FileSystemUsage' AND CustomInteger1 >= 95)
```

Un événement peut ensuite utiliser *CustomInteger1* pour d'autres objectifs et ne pas dépasser ce seuil accidentellement.

En résumé, vous pouvez maintenant créer un seuil dans Performance Management qui utilise des opérateurs arithmétiques dans les attributs `CustomInteger`, ce qui n'est pas possible avec les attributs `CustomSlots`.

Remarque : Si vous mappez des données qui ne sont pas des entiers à l'attribut `CustomInteger`, la valeur obtenue peut être zéro (0) ou une valeur inattendue.

Modification des fichiers de configuration et de format de l'agent

L'agent de système d'exploitation lit ses fichiers de configuration (`.conf`) et de format (`.fmt`) à son démarrage et surveille leur horodatage toutes les 60 secondes ensuite.

Si l'horodatage du fichier de configuration ou de format change, l'agent réinitialise sa configuration de manière dynamique sans redémarrer. Lors de la réinitialisation, la surveillance est interrompue momentanément. Lorsque la surveillance reprend, l'agent doit déterminer la position à partir de laquelle il doit redémarrer dans les journaux surveillés. L'agent se comporte donc de la même manière qu'un arrêt complet et un redémarrage.

Remarque : Lorsque l'agent se réinitialise après modification d'un fichier de configuration ou de format, le système réinitialise les informations des groupes d'attributs `Statistiques RegEx du fichier journal`, `Statut du fichier journal` et `Evénement de fichier journal`.

Par défaut, l'agent démarre la surveillance à partir de la fin du fichier à l'issue de la réinitialisation. Cette position de départ peut provoquer la disparition des événements qui se sont produits pendant

l'interruption de la surveillance. Pour vous assurer que ces événements sont bien récupérés à la reprise de la surveillance, utilisez le paramètre `NumEventsToCatchUp=-1`.

L'utilisation du paramètre `NumEventsToCatchUp=-1` entraîne la gestion d'un fichier de position. Le fichier de position est mis à jour chaque fois que l'agent lit le fichier journal. Lors de la mise à jour, le système enregistre la position de l'agent dans le fichier journal dans l'éventualité d'un redémarrage de l'agent. La gestion du fichier de position a un léger impact sur les performances système. Aussi, ne le gérez que lorsque c'est nécessaire. Pour plus d'informations sur `NumEventsToCatchUp`, voir «Fichier de configuration», à la page 655.

Remarque : Certaines valeurs de configuration ne sont pas présentes dans le fichier de configuration et sont définies lors de la configuration initiale. Si vous modifiez ces valeurs, vous devez redémarrer l'agent.

Héritage

Les fichiers de format utilisent l'héritage pour déduire les définitions d'attribut à partir d'une spécification de format définie précédemment.

Utilisez la relation FOLLOWS pour créer des spécifications de format spécifiques à partir de spécifications de format génériques à l'aide de l'héritage.

Tout d'abord, définissez une classe de base que vous appellerez `DiskFailure`. Par exemple :

```
REGEX DiskFailure
Disk Failure on device (.*)
device $1 CustomSlot1
END
```

Cette expression régulière effectue une correspondance pour les erreurs `Disk Failure on device/dev/sd0` dans le journal de surveillance afin que la valeur `/dev/sd0` soit affectée à l'attribut *device* (unité).

Cependant, vous pouvez également voir une version longue de ce message d'erreur dans le journal de surveillance.

Par exemple, le message d'erreur `Disk Failure on device /dev/sd0, error code: 13` peut s'afficher.

Ce message d'erreur est mis en correspondance avec un attribut comme indiqué dans l'exemple suivant :

```
REGEX DiskFailureError FOLLOWS DiskFailure
Disk Failure on device (.*), error code: ([0-9]*)
errcode $2 CustomSlot2
END
```

Désormais, l'événement inclut les attributs *device* et *errcode*. Comme la classe d'événement `DiskFailure` a déjà défini un attribut pour le nom d'unité, vous permettez à la sous-classe d'hériter de cet attribut et cet héritage vous évite de le déclarer une seconde fois. L'attribut étant défini en tant que $1, le système affectera la première sous-expression de l'expression régulière à cet attribut.

Cependant, la classe `DiskFailureError` définit également une deuxième sous-expression. Vous pouvez affecter cette sous-expression à un nouvel attribut appelé `errcode` et le définir en tant que $2 pour faire référence à la deuxième sous-expression de l'expression régulière. Ce type d'affectation est illustré dans l'exemple précédent qui présente un extrait du journal.

L'événement contient désormais l'attribut `device` qui est affecté de la valeur `/dev/sd0` et l'attribut `errcode` qui est affecté de la valeur 13. L'unité (device) est affectée à l'attribut CustomSlot1 tandis que le code d'erreur (errcode) est affecté à l'attribut CustomSlot2.

Les mappages d'attributs personnalisés Performance Management sont également hérités. Pour plus d'informations sur les mappages d'attributs personnalisés Performance Management, voir «Spécifications du fichier de format», à la page 665.

Multiligne
La syntaxe multiligne permet de comparer les enregistrements occupant plusieurs lignes à des modèles dans le journal que vous surveillez.

Indiquez le caractère de retour à la ligne \n dans l'expression régulière pour indiquer où le retour à la ligne apparaît dans le journal de surveillance. L'exemple suivant illustre le type de syntaxe multiligne :

```
REGEX REMultiLine
Line1:(.*)\nLine2(.*)
msg $1
second_msg $2
END
```

Remarque : Windows Indiquez une combinaison de retours chariot \r\n et de nouvelles lignes.

Si les messages d'erreur suivants sont consignés dans le journal, l'événement REMultiLine est créé :

```
Line1: An error occurred
Line2: The error was "disk error"
```

La valeur `An error occurred` est affectée à l'attribut `msg` tandis que la valeur `The error was "disk error"` est affectée à l'attribut `second_msg`.

Mappages
L'agent de système d'exploitation détermine la classe d'événement d'un message de journal système. Il détermine la classe d'événement en comparant le message à un masque dans le fichier de format.

L'agent convertit les messages de journal en instances de classe d'événement qui inclut les paires d'attributs `nom=valeur`. L'événement est ensuite envoyé au serveur d'événements.

L'agent détermine la classe d'événement d'un message de journal système à la source. Il détermine la classe d'événement en comparant le message de journal à un masque dans le fichier de format. Lorsque vous utilisez cette procédure de comparaison pour déterminer une classe, vous devez affecter des valeurs aux attributs.

Les valeurs d'attribut proviennent de différents endroits. Par exemple :

- Valeurs par défaut fournies par l'agent
- Entrées de journal correspondant à des sous-expressions spécifiques d'expressions régulières

Le fichier de format comporte une instruction de mappage qui respecte la syntaxe suivante :

```
nom    valeur CustomSlotn
```

Tout d'abord, vous spécifiez un identificateur pour décrire le `nom` d'un attribut (également appelé variable, emplacement ou identificateur de valeur). Ensuite, vous indiquez une valeur à affecter à cet attribut en utilisant l'une des valeurs décrites dans la section «Indicateurs de valeur», à la page 671.

Utilisez des attributs personnalisés pour afficher les données dans la console Performance Management et définir des seuils. Lorsque vous créez des seuils, toutes les valeurs d'attributs personnalisés sont des chaînes. Les attributs personnalisés sont également nécessaires au fonctionnement du mécanisme de détection des événements en double car vous devez identifier les attributs utilisés pour la détermination des doublons. Pour plus d'informations sur le filtrage d'événements, voir «Filtrage et récapitulatif des événements», à la page 1047. `msg` est un nom d'attribut spécial qui possède ses propres valeurs dans la table d'événements. Vous n'avez pas besoin d'utiliser d'attribut personnalisé pour `msg`.

Vous pouvez limiter la portée d'un attribut de façon à ce qu'il n'existe que dans la définition de format. Lorsque vous définissez l'attribut, vous devez faire précéder le nom d'attribut par un tiret. Par exemple :

```
-name    valeur
```

Les attributs que vous définissez de cette façon ne sont pas inclus dans l'événement final. Cependant, vous pouvez faire référence à l'attribut à d'autres endroits dans la définition de format, notamment au sein d'une instruction PRINTF. Dans l'exemple REGenericSyslog suivant, l'attribut `service` n'est pas inclus dans l'événement que vous générez, mais vous pouvez y faire référence dans l'instruction PRINTF.

Il conserve la même valeur qui était appliquée à l'attribut d'origine lorsqu'il était spécifié sans tiret. Grâce à cette procédure, vous pouvez utiliser des variables temporaires de la définition de format qui ne sont pas incluses dans l'événement final. Par exemple, vous pouvez définir une classe d'événement REGenericSyslog pour comparer des événements UNIX syslog génériques de la manière suivante :

```
REGEX REGenericSyslog
^([A-Z][a-z]{2}) ([ 0-9][0-9]) ([0-9]{2}:[0-9]{2}:[0-9]{2}) (.*?) (.*?): (.*)$
month $1
date $2
time $3
host $4
-service $5
msg $6
syslog_msg PRINTF("service %s reports %s", service, msg)
END
```

Indicateurs de valeur
Les mappages d'une spécification de format affectent des valeurs aux attributs.

La partie mappage d'une spécification de format comporte les types de spécificateur de valeur suivants :

- $i
- Constante de chaîne
- Instruction PRINTF

$i

L'attribut $i indique la position d'une sous-expression dans une chaîne de format. Chaque sous-expression est numérotée ; les numéros sont compris entre 1 et le nombre maximal de sous-expressions figurant dans la chaîne de format.

La valeur d'un indicateur de valeur $i (également appelé variable, emplacement ou attribut) correspond à la partie du message de journal système qui est rapprochée par la sous-expression correspondante.

Dans l'exemple suivant, l'agent Log File convertit un message de journal de l'utilitaire UNIX syslog en événement syslog comportant des valeurs définies :

```
REGEX REGenericSyslog
^([A-Z][a-z]{2}) ([ 0-9][0-9]) ([0-9]{2}:[0-9]{2}:[0-9]{2})
 (.*?) (.*?): (.*)$
month   $1
date    $2
time    $3
host    $4
service $5
msg     $6
END
```

Chaque sous-expression numérotée de $1 à $6 correspond à un élément entre parenthèses de l'expression régulière.

L'événement syslog suivant :

```
Apr  6 10:03:20 jimmy syslogd 1.4.1: restart.
```

a donc les valeurs suivantes :

```
month=Apr
date=6
time=10:03:20
host=jimmy
service=syslogd 1.4.1
msg=restart.
```

Par exemple, la valeur 10:03:20 correspond au troisième élément entre parenthèses de l'expression régulière dans l'événement syslog ; elle est affectée à l'attribut time *$3*. De la même manière, la

valeur `jimmy` correspond au quatrième élément entre parenthèses de l'expression régulière ; elle est affectée à l'attribut host *$4*.

Constante de type chaîne

La constante de type chaîne déclare que la valeur de l'attribut est la chaîne spécifiée. Si la valeur d'attribut est une constante unique sans espace, vous devez la spécifier sans guillemets doubles (" ") comme indiqué dans l'exemple suivant :

```
severity WARNING
```

Si la valeur d'attribut comporte des espaces, vous devez par contre utiliser des guillemets doubles comme indiqué dans l'exemple suivant :

```
component "Web Server"
```

Instruction PRINTF

L'instruction PRINTF crée des valeurs d'attribut plus complexes à partir d'autres valeurs d'attribut. Elle se compose du mot clé PRINTF suivi d'une chaîne de format printf() de type C, ainsi que d'un ou de plusieurs noms d'attribut.

La chaîne de format ne prend en charge que l'indicateur de composant %s. Les valeurs des attributs utilisés dans l'instruction PRINTF doivent être dérivées à partir d'une spécification de valeur *$i* ou d'une spécification de valeur de chaîne constante (vous ne pouvez pas les déduire à partir d'une autre instruction PRINTF).

Utilisez la valeur des attributs d'argument pour composer une nouvelle chaîne constante en fonction de la chaîne de format. Cette nouvelle chaîne constante devient la valeur de l'attribut.

Dans l'exemple précédent où vous avez défini la classe de base REGenericSyslog, ainsi que les attributs *service* et *msg*, vous pouvez définir un attribut appelé *syslog_msg* à l'aide du mot clé PRINTF.

```
syslog_msg PRINTF("service %s reports %s", service, msg)
```

Si le journal consigne le message suivant :

```
Apr  6 10:03:20 jimmy syslogd 1.4.1: restart.
```

Le système génère une nouvelle chaîne constante, qui comporte les valeurs d'attribut provenant de la chaîne de format :

```
syslog_msg="service syslogd 1.4.1 reports restart."
```

Mots clé
Utilisez les mots clés dans le fichier de format pour affecter des valeurs qui se développent au moment de l'exécution.

Les mots clés suivants se développent au moment de l'exécution :

- DEFAULT
- FILENAME
- LABEL
- REGEX

DEFAULT

Le mot clé DEFAULT permet d'affecter une valeur DEFAULT à un attribut spécifique. L'agent de système d'exploitation affecte une valeur par défaut interne à des attributs décrits dans le tableau suivant :

Tableau 191. Attributs et valeur DEFAULT	
Attributs	**Description**
hostname	Nom d'hôte abrégé du système sur lequel s'exécute l'agent. Il n'inclut pas le nom de domaine du système.
origin	Adresse IP du système sur lequel s'exécute l'agent.
fqhostname	Nom d'hôte complet du système sur lequel s'exécute l'agent. Il inclut le nom de domaine du système.
RemoteHost	Lorsqu'un événement apparaît sur le système local, cet attribut est vide. Si un événement se produit sur un système distant, *RemoteHost* contient une chaîne sous la forme *utilisateur@hôte:port*, qui indique le nom de l'hôte distant d'où provient l'événement, ainsi que l'utilisateur et le port utilisés pour la connexion sur cet hôte.

La valeur affectée à l'attribut *fqhostname* est influencée par les paramètres FQDomain (facultatifs) suivants dans le fichier `.conf` :

- Si vous associez FQDomain à `yes`, l'agent détermine le nom de domaine du système.
- Si vous associez FQDomain à `no` ou que vous ne lui affectez pas de valeur, l'agent ne définit pas de nom de domaine et une chaîne vide est affectée à l'attribut *fqhostname*.
- Si FQDomain n'a pas pour valeur `yes` ou `no`, le système accepte le nom de domaine comme valeur et l'ajoute au nom d'hôte.

Dans l'exemple suivant, la définition de format contient trois attributs :

- *hostname* DEFAULT
- *origin* DEFAULT
- *fqhostname* DEFAULT

Si vous associez l'attribut `FQDomain` à `yes` dans le fichier `.conf` et que vous l'exécutez sur un ordinateur avec les propriétés suivantes :

- *hostname*: `myhost`
- *IP address*: `192.168.1.100`
- *domainname*: `mycompany.com`

un événement est créé et les trois attributs prennent les valeurs suivantes :

```
"hostname=myhost", "origin=192.168.1.100", "fqhostname=myhost.mycompany.com"
```

FILENAME

Le mot clé `FILENAME` indique le nom complet (chemin inclus) du fichier journal contenant le message. Si vous utilisez un seul agent pour surveiller plusieurs fichiers journaux et que vous devez identifier la source de l'événement, utilisez ce mot clé pour compléter un attribut d'événement avec le nom de fichier. Si le message provient du journal système, le mappage correspond à `EventLog` pour les agents de système d'exploitation Windows et à `SysLogD` pour les agents de système d'exploitation UNIX.

Remarque : Le chemin inclut un attribut pour ce mot clé.

LABEL
Le mot clé LABEL spécifie le nom d'hôte du système sur lequel s'exécute l'agent.

REGEX
Le mot clé REGEX développe l'expression régulière qui correspondait au message et a provoqué l'événement.

Longueur maximale des messages
Cette valeur correspond à la longueur maximale des messages que l'agent de système d'exploitation peut recevoir sans tronquer le message.

La longueur maximale des messages est différente dans Performance Management et Tivoli Netcool/OMNIbus.

Performance Management
Pour les événements envoyés à Performance Management, l'attribut `msgest` limité à 2048 octets. Les messages plus longs sont tronqués.

Tivoli Netcool/OMNIbus
Pour les événements envoyés à Netcool/OMNIbus via la sonde de Tivoli EIF, la taille totale de l'événement, y compris le nom de classe et tous les attributs et leurs valeurs, ne doivent pas dépasser 4 096 octets. Dans l'exemple d'événement EIF suivant, `;END` n'est pas comptabilisé dans la limite de 4096 octets. Tous les autres éléments sont néanmoins pris en compte, notamment les éléments de syntaxe (points-virgules, guillemets, signes égal).

```
Class;attr1=value1;attr2=value2;msg='Hello, world';END
```

Surveillance des fichiers journaux distants : Chiffrement d'un mot de passe ou d'une phrase de passe
Pour renforcer la sécurité du système, vous pouvez chiffrer les mots de passe et les phrases de passe transmis aux système distants lorsque vous utilisez la Surveillance des fichiers journaux distants.

Pourquoi et quand exécuter cette tâche
Le mot de passe et les phrases de passe chiffrés sont stockés dans le fichier de configuration (`.conf`). Pour plus d'informations sur le fichier de configuration, voir «Fichier de configuration», à la page 655.

Procédure

- Exécutez la commande **`itmpwdsnmp`** et entrez le mot de passe ou la phrase de passe à chiffrer :
  - Linux AIX La commande est exécutée à partir du répertoire d'installation de Cloud APM. Le chemin d'installation par défaut est `opt/ibm/apm/agent` et *rép_install* correspond à l'emplacement où vous avez installé l'agent.
  - Windows Le chemin d'installation par défaut est `C:\IBM\APM`.

  Linux Exemple d'exécution de la commande sous Linux :

```
$ export rép_install=/opt/ibm/apm/agent/bin
$ /opt/ibm/apm/agent/bin

Enter string to be encrypted:
motdepasse

Confirm string:
motdepasse

{AES256:keyfile:a}Z7BS23aupYqwlXb1Gh+weg==
$
```

  Dans cet exemple, le résultat de la commande, `{AES256:keyfile:a}Z7BS23aupYqwlXb1Gh +weg==`, est utilisé dans son intégralité pour définir **SshPassword** dans le fichier de configuration de l'agent. Le préfixe `{AES256:keyfile:a}` indique à l'agent que le mot de passe est chiffré.

  Pour chiffrer une phrase de passe pour un fichier de clés privées, procédez de la même manière.

Configuration du scriptage personnalisé de l'agent de système d'exploitation

Les agents Monitoring Agent for Linux OS, Monitoring Agent for UNIX OS et Monitoring Agent for Windows OS sont configurés automatiquement. Cette fonction permet aux utilisateurs de définir les scripts à exécuter sur les agents de système d'exploitation à une fréquence définie.

La fonction de scriptage personnalisé est activée par défaut. L'administrateur peut l'activer/la désactiver en définissant une nouvelle variable d'environnement *KXX_FCP_SCRIPT*=true/false (à la valeur true par défaut) dans le fichier de configuration de l'agent, où XX peut être :

- LZ pour Monitoring Agent for Linux OS

- UX pour Monitoring Agent for UNIX OS

- NT pour Monitoring Agent for Windows OS

Les détails sont fournis dans les sections suivantes.

Démarrage rapide du scriptage personnalisé

Ajoutez le scriptage personnalisé pour que les agents de système d'exploitation définissent les scripts à exécuter selon une fréquence définie.

La fonction est activée avec les valeurs par défaut dès que l'agent de système d'exploitation est démarré. La seule action à effectuer pour démarrer la fonction de scriptage est la suivante :

Créez un fichier de propriétés sous le répertoire par défaut (sous Linux ou UNIX, il s'agit de `rép_install/localconfig/`*`code du produit`*`/scripts_definitions` ; sous Windows, il s'agit de `rép_install\localconfig\nt\scripts_definitions`) en utilisant comme exemple le modèle fourni `script_property.txt`.

Seules deux propriétés sont requises :

ATTRIBUTE_NAME
Nom unique permettant d'identifier la définition de script dans le fichier de propriétés.

SCRIPT_PATH_WITH_PARMS
Chemin complet du script avec les arguments.

Les scripts shell, perl et d'autres types de script peuvent être utilisés. Spécifiez la commande complète à exécuter dans la propriété SCRIPT_PATH_WITH_PARMS.

Par exemple, `perl C:\IBM\scripts\Custom_Scripts\date.pl`. Dans cet exemple, assurez-vous que l'emplacement de `perl` peut être résolu par l'agent à l'aide de la variable PATH dans son environnement. Vous pouvez également indiquer le chemin complet où `perl` est installé.

Paramètres dans les fichiers d'environnement des agents de système d'exploitation

Vous pouvez définir les paramètres de script personnalisés dans les fichiers d'environnement des agents de système d'exploitation.

Il est possible de personnaliser la fonction de scriptage en définissant les paramètres dans les fichiers d'environnement des agents de système d'exploitation :

***rép_install*/config/lz.environment**
Fichier d'environnement de Monitoring Agent for Linux OS.

***rép_install*/config/ux.environment**
Fichier d'environnement de Monitoring Agent for UNIX OS.

***rép_install*\TMAITM6_x64\KNTENV**
Fichier d'environnement de Monitoring Agent for Windows OS 64 bits.

***rép_install*\TMAITM6\KNTENV**
Fichier d'environnement de Monitoring Agent for Windows OS 32 bits.

KXX_FCP_SCRIPT
La fonction de scriptage est activée par défaut. Pour la désactiver : `KXX_FCP_SCRIPT=false`

Selon les besoins, d'autres paramètres peuvent être définis dans les fichiers d'environnement de l'agent :

KXX_FCP_SCRIPT_DEFINITIONS
Emplacement de stockage des fichiers de propriétés.

L'emplacement par défaut sous Linux™ ou UNIX™ est *rép_install*/localconfig/*PC*/scripts_definitions, et *rép_install*\localconfig\nt\scripts_definitions sous Windows™

KXX_FCP_SCRIPT_INTERVAL

L'agent de système d'exploitation utilise la valeur de cette variable selon un intervalle en boucle, en secondes, pour vérifier l'exécution des scripts en cours et envoie les événements si la condition de filtre est satisfaite. La valeur minimale est de 30 secondes et la valeur maximale de 300 secondes. Les valeurs non valides sont réinitialisées à la valeur par défaut. La valeur par défaut est de 60 secondes.

Remarque : Ce paramètre est ignoré si KXX_FCP_SCRIPT_SYNC_INTERVALS est défini à la valeur USE_SCRIPT (voir la définition de KXX_FCP_SCRIPT_SYNC_INTERVALS).

KXX_FCP_SCRIPT_SYNC_INTERVALS

Si l'intervalle en boucle de l'agent défini par KXX_FCP_SCRIPT_INTERVAL est supérieur à la fréquence d'exécution du script, il arrive que les données produites par des boucles d'exécution du script soient perdues. Pour éviter ce comportement, la fréquence d'exécution du script peut être synchronisée avec l'intervalle de boucle de l'agent en attribuant à KXX_FCP_SCRIPT_SYNC_INTERVALS la valeur :

- USE_AGENT - La valeur de la fréquence d'exécution du script est forcée pour atteindre la valeur maximale entre KXX_FCP_SCRIPT_INTERVAL et EXECUTION_FREQUENCY qui est défini dans le fichier de propriétés.
- USE_SCRIPT - L'intervalle en boucle de l'agent est défini de manière dynamique à la valeur de fréquence minimale (EXECUTION_FREQUENCY dans le fichier de propriétés) entre tous les scripts définis. La valeur définie par KXX_FCP_SCRIPT_INTERVAL est ignorée. La fréquence des scripts reste identique à celle définie dans les fichiers de propriétés. Lorsque vous définissez USE_SCRIPT, l'intervalle de boucle de l'agent peut changer à chaque fois qu'une définition de script est ajoutée, modifiée ou supprimée. Il ne peut en aucun cas être inférieur à la valeur définie par KXX_FCP_OVERRIDE_MIN_FREQUENCY_LIMIT ou supérieur à 300 secondes.
- NO - Aucune synchronisation n'est effectuée et des résultats d'exécution risquent d'être perdus.

KXX_FCP_SCRIPT_DEFINITIONS_CHECK_INTERVAL

Au démarrage et à chaque intervalle défini par cette variable, l'agent de système d'exploitation vérifie les changements éventuels dans les scripts ou les fichiers de propriétés. Si la valeur KXX_FCP_SCRIPT_DEFINITIONS_CHECK_INTERVAL est inférieure à l'intervalle en boucle de l'agent, elle est réinitialisée à cette valeur. La valeur maximale autorisée par défaut est 300 secondes.

KXX_FCP_USER

e paramètres est valide uniquement sur les agents de système d'exploitation Linux™ ou UNIX™. Il définit l'user utilisé pour créer le processus fcp_daemon s'il est différent de l'utilisateur du processus d'agent de système d'exploitation ; tous les scripts sont exécutés par cet utilisateur. Sachez que le propriétaire de l'agent de système d'exploitation doit avoir des droits corrects pour créer le processus fcp_daemon. Sous Windows™, un utilisateur différent doit être défini pour la connexion au service "FCProvider" de Monitoring Agent for Windows OS. Cet utilisateur doit avoir des droits "Contrôle total" sur le répertoire d'installation de l'agent et les répertoires du référentiel de scripts. Pour plus d'informations, voir :

https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/install/install_linuxaix_agent_nonroot.html

KXX_FCP_MAX_CDP_DP_THREAD_POOL_SIZE
Il définit le nombre maximal de scripts pouvant être exécutés simultanément. La valeur maximale est 32.

KXX_FCP_MAX_DAEMON_RESTARTS

L'agent de système d'exploitation surveille le processus fcp_daemon : en cas de sortie anormale, il le redémarre. La valeur par défaut est 4. Le redémarrage s'effectue KXX_FCP_MAX_DAEMON_RESTARTS (fois au cours de la journée). La valeur 0 doit être utilisée pour éviter le redémarrage ; si -1 est définie, l'agent de système d'exploitation tente indéfiniment de redémarrer le processus fcp_daemon. Le compteur de redémarrage est réinitialisé lors du redémarrage de l'agent de système d'exploitation.

KXX_FCP_SEND_SCRIPT_RUNTIME_EVENTS

La valeur par défaut est true. Si la valeur est false, l'agent de système d'exploitation cesse d'envoyer des événements pour chaque ligne de la sortie standard du script. Dans ce cas, les sorties du script sont visibles dans les espaces de travail de la console, mais aucune situation ne s'affiche et aucune donnée d'historique n'est collectée.

KXX_FCP_OVERRIDE_MIN_FREQUENCY_LIMIT

Il est utilisé lorsque KXX_FCP_SCRIPT_SYNC_INTERVALS est défini sur USE_SCRIPT. Dans cette condition, il définit la valeur minimale de l'intervalle en boucle de l'agent de système d'exploitation.

L'utilisation de valeurs peu élevées pour l'intervalle en boucle de l'agent de système d'exploitation (inférieures à 5 secondes) est hautement invasive et peut avoir une incidence sur les performances de l'agent. S'il est nécessaire de collecter fréquemment les données (une fois par seconde, par exemple), il est conseillé de personnaliser un script. Le script met en cache les données à la fréquence nécessaire et renvoie les données collectées à l'agent de système d'exploitation à une fréquence plus élevée (toutes les 60 secondes par exemple).

Les variables Agent Builder (CDP) permettent également de contrôler le comportement du processus fcp_daemon :

CDP_DP_REFRESH_INTERVAL

(60 secondes par défaut) Heure de démarrage programmée du script global. Utilisé si la fréquence n'est pas transmise dans le fichier de propriétés du script.

CDP_DP_SCRIPT_TIMEOUT

(30 secondes par défaut) Durée d'exécution maximale du script global. Lorsque la durée d'exécution d'un script dépasse cette limite, son Status_Code a la valeur TIMEOUT

CDP_DP_KILL_ORPHAN_SCRIPTS

(Y|N - N par défaut) Comportement global utilisé par le processus fcp_daemon pour les scripts en dépassement de délai. Lorsqu'il a la valeur 'Y', les scripts sont arrêtés, sinon ils sont abandonnés. Cette valeur est ignorée pour un script spécifique si la clé KILL_AFTER_TIMEOUT est définie dans le fichier de propriétés du script

CDP_MAXIMUM_ROW_COUNT_FOR_CPCI_DATA_RESPONSES

(1000 par défaut) La valeur globale est ajoutée pour des raisons de performance afin de limiter le nombre maximal de lignes de sortie renvoyées par les scripts. Les lignes excédentaires sont ignorées. Les valeurs autorisées sont des entiers positifs. Les valeurs non valides sont remplacées par la valeur no limit (nombre illimité).

Le processus fcp_daemon prend également en charge les autres variables d'environnement qui sont utilisées pour contrôler les agents Agent Builder. Pour obtenir la liste complète, reportez-vous au manuel *IBM Agent Builder - Guide d'utilisation* ici : Chapitre 2, «Documentation au format PDF», à la page 43.

Paramètres dans les fichiers de propriétés

Vous pouvez définir les paramètres de script personnalisés dans les fichiers de propriétés.

Le répertoire KXX_FCP_SCRIPT_DEFINITIONS contient une liste des fichiers *.properties. Chaque fichier de propriétés contient une liste des scripts à exécuter avec leurs propriétés respectives au format `clé=valeur`. Les propriétés pouvant être définies (non sensibles à la casse) sont les suivantes :

ATTRIBUTE_NAME

Obligatoire - chaîne d'une longueur maximale de 256 caractères. Nom que vous attribuez à un script et ses attributs. Le nom ATTRIBUTE_NAME peut contenir des caractères alphanumériques et seul le trait de soulignement peut être utilisé comme caractère spécial. Si d'autres caractères spéciaux

(espace ou vide) sont utilisés, ils sont convertis en trait de soulignement (_). Lorsque plusieurs scripts sont répertoriés dans le même fichier de propriétés, des attributs ATTRIBUTE_NAME supplémentaires doivent être définis (un pour chaque script). Ce nom est la première valeur spécifiée pour chaque script défini et il indique le début des propriétés définies pour un script donné, jusqu'au ATTRIBUTE_NAME suivant.

SCRIPT_PATH_WITH_PARMS
Obligatoire - chaîne d'une longueur maximale de 512 caractères. Ce paramètre définit le chemin d'accès complet au script contenant les paramètres qui sont séparés par un espace. Aucun caractère spécial n'est admis. Les valeurs contenant des espaces vides doivent être placées entre apostrophes (') ou entre guillemets ("). Les variables d'environnement peuvent être transmises à condition d'être placées entre ${...} pour tous les systèmes d'exploitation. Les variables d'environnement doivent être disponibles dans le contexte des processus d'agent de système d'exploitation.

EXECUTION_FREQUENCY
Facultatif - la valeur par défaut est 60 secondes. Ce paramètre définit la fréquence d'exécution du script.

CUSTOM_NAME
Facultatif - chaîne d'une longueur maximale de 256 caractères. Ce paramètre peut être utilisé pour une description du script.

IS_ACTIVE
Facultatif - true|false. La valeur par défaut est true. Le script est activé. Si la valeur est false, le script n'est pas exécuté.

DISABLE_USE_AGENT_SYNC
Facultatif - true|false. La valeur par défaut est false. Si true est défini, la valeur EXECUTION_FREQUENCY du script est respectée également si la variable globale KXX_FCP_SCRIPT_SYNC_INTERVALS est définie sur USE_AGENT.

KILL_AFTER_TIMEOUT
Facultatif - true|false. La valeur par défaut est définie par la variable CDP_DP_KILL_ORPHAN_SCRIPTS. Lorsque la valeur est true, le script est arrêté en cas de dépassement du délai. Cela se produit lorsque la durée d'exécution du script est supérieure à la valeur indiquée par le paramètre CDP_DP_SCRIPT_TIMEOUT dans le fichier de configuration de l'agent de système d'exploitation. Sinon, ce paramètre est ignoré. Dans les deux cas, aucune donnée n'est collectée. Lorsque la variable KILL_AFTER_TIMEOUT est spécifiée, seul le script défini dans le fichier de propriétés est arrêté et non les processus enfant créés par le script. Cette fonction n'est pas prise en charge par les agents de système d'exploitation Solaris et Windows 32 bits et aucun script en dépassement de délai n'est abandonné.

Les lignes de sortie qui sont renvoyées par un script sont analysées.
Le script renvoie une sortie standard (considérée comme le premier jeton). Lorsque plusieurs valeurs sont renvoyées dans la ligne de sortie, elles sont ajoutées en tant que jetons supplémentaires. Il peut y avoir au maximum cinq valeurs de chaîne, cinq valeurs de type entier et cinq valeurs flottantes, selon une syntaxe prédéfinie.

OUTPUT_TYPE

STRING|INTEGER|FLOAT - Facultatif. La valeur par défaut est une chaîne. Elle définit le type du premier jeton renvoyé par chaque ligne du script ; OUTPUT_TYPE peut être :

- STRING (par défaut) - chaînes comportant jusqu'à 2048 caractères. Lorsqu'elle est utilisée, l'attribut "Standard_Output_String" de KXX_Custom_Scripts_Rtm_Smp est complété par le premier jeton.
- INTEGER - autorise l'obtention de valeurs numériques entre -9223372036854775806 et 9223372036854775806. Lorsqu'elle est utilisée, l'attribut "Standard_Output_Integer" de KXX_Custom_Scripts_Rtm_Smp est complété par le premier jeton.
- FLOAT - autorise l'obtention de valeurs numériques entre -92233720368547758.06 et 92233720368547758.06, avec une précision de deux décimales. Lorsqu'elle est utilisée, l'attribut "Standard_Output_Float" de KXX_Custom_Scripts_Rtm_Smp est complété par le premier jeton.

TOKEN_TYPES
STRING|INTEGER|FLOAT - Facultatif. Elle définit le type de sortie lorsque le premier jeton est suivi de plusieurs autres. L'utilisateur peut définir au maximum cinq valeurs de chaîne, cinq valeurs de type entier et 5 valeurs flottantes. Il s'agit d'une liste de types séparés par des virgules : <type_jeton>,<type_jeton>,... type_jeton peut être vide ou avoir l'une des valeurs suivantes (insensible à la casse) :

- - STRING ou S
- - INTEGER ou I
- - FLOAT ou F
- Si *TOKEN_TYPES* est vide, le jeton correspondant est ignoré.

  Exemples de présentations valides :
- - TOKEN_TYPES=S,I,S,,,F,,F,F
- - TOKEN_TYPES=String,integer,S,,,Float,,f,FLOAT

TOKEN_LABELS
STRING - Facultatif. 16 caractères au maximum pour chaque libellé. Elle définit les libellés des jetons définis dans TOKEN_TYPES. Cette valeur est une liste de libellés de jeton séparés par des virgules et elle doit correspondre aux jetons définis par TOKEN_TYPES. Exemple :

- TOKEN_TYPES=S,I,S,,,F,,F,F
- TOKEN_LABELS=Cpu Name,Cpu number,Description,,,value 1,,value 2,value 3
- TOKEN_LABELS est ignoré si TOKEN_TYPES n'est pas défini.

TOKEN_SEPARATOR
Facultatif - point-virgule ";" par défaut. Elle définit la chaîne utilisée comme séparateur pour scinder la ligne de sortie en jetons. Elle est ignorée si TOKEN_TYPES n'est pas défini. Une valeur à blanc (vide) est acceptée en tant que séparateur et plusieurs espaces consécutifs dans les lignes de sortie sont interprétés comme un espace unique.

Les deux paramètres suivants permettent de filtrer la sortie des lignes d'un script. Ils sont appliqués par l'agent de système d'exploitation au premier jeton uniquement et ils doivent être utilisés ensemble :

FILTER_VALUE
Facultatif. Valeur utilisée à des fins de comparaison. Elle est requise si FILTER_OPERATOR est défini. Si OUTPUT_TYPE est une chaîne, la valeur de filtre doit refléter exactement la valeur de chaîne renvoyée par le script à filtrer sans guillemets supplémentaires (aucun caractère générique n'est autorisé).

FILTER_OPERATOR
Facultatif. Opérateur utilisé à des fins de comparaison. Elle est requise si FILTER_VALUE est défini. Les valeurs acceptées pour FILTER_OPERATOR sont les suivantes :

- = (égal)
- != (non égal à)
- > (supérieur à) uniquement pour le type numérique
- >= (non inférieur à) uniquement pour le type numérique
- < (inférieur ou égal à) uniquement pour le type numérique
- <= (non supérieur à) uniquement pour le type numérique

Exemples de fichier de propriétés
Exemples de définition des paramètres dans les fichiers de propriétés.

#Première définition de script : le script ex_script1.sh est démarré toutes les 150 secondes. Il renvoie des valeurs folltantes et seules les lignes en sortie égales à 0.5 sont prises en compte par l'agent.

```
ATTRIBUTE_NAME=sample1
SCRIPT_PATH_WITH_PARMS=/opt/ibm/apm/agent/localconfig/lz/scripts_definitions/ex_script1.sh
```

```
EXECUTION_FREQUENCY=150
OUTPUT_TYPE=FLOAT
FILTER_VALUE=0.5
FILTER_OPERATOR==
```

#Deuxième définition de script : le script ex_script2.sh est démarré toutes les 60 secondes. Il renvoie des valeurs de type entier et seules les lignes différentes de 0 sont prises en compte par l'agent.

```
ATTRIBUTE_NAME=ex_script2
SCRIPT_PATH_WITH_PARMS=${CANDLE_HOME}/tmp/check_out.sh
EXECUTION_FREQUENCY=60
OUTPUT_TYPE=INTEGER
FILTER_VALUE=0
FILTER_OPERATOR=!=
```

#Troisième définition de script : le script ex_script3.sh est démarré toutes les 120 secondes avec trois paramètres d'entrée (le premier est de type entier, et le deuxième et le troisième de type chaîne). Il s'arrête s'il se bloque ou si sa durée d'exécution est supérieure à la valeur de délai définie.

```
ATTRIBUTE_NAME=ex_script3
SCRIPT_PATH_WITH_PARMS=/opt/scripts/ex_script3.sh 1 "second input parameter" "third input
parameter"
EXECUTION_FREQUENCY=120
OUTPUT_TYPE=STRING
KILL_AFTER_TIMEOUT=TRUE
```

#Quatrième définition de script : le script cpu_mem_percentage.sh est démarré toutes les 50 secondes et renvoie le cpuid sous forme de chaîne de sortie standard, deux valeurs flottantes pour le pourcentage d'UC en veille et le pourcentage d'UC utilisée, et deux valeurs de type entier pour l'utilisation de la mémoire et l'utilisation de la mémoire virtuellee. La barre verticale est utilisée comme séparateur pour analyser la sortie. Exemple de ligne devant être renvoyée par le script :

cpu2|35,5|65,5|3443|123800

```
ATTRIBUTE_NAME=cpu and mem Usage
SCRIPT_PATH_WITH_PARMS=${SCRIPT_HOME}/cpu_mem_percentage.sh
OUTPUT_TYPE=STRING
TOKEN_TYPES=F,F,I,I
TOKEN_LABELS= Idle CPU %, Used CPU %, Virt MEM used MB, MEM used MB
TOKEN_SEPARATOR=|
EXECUTION_FREQUENCY=50
```

Limitations et incidents recensés

Limitations et incidents recensés

- La fonction de scriptage n'est pas prise en charge sur les systèmes Windows 2003 64 bits.
- La fonction d'arrêt après expiration (Kill after timeout) n'est pas opérationnelle sur les agents de système d'exploitation Solaris et Windows 32 bits.
- Le processus fcp_daemon peut arrêter l'exécution des scripts dans Windows 32 bit si l'exécution des scripts ne se termine pas dans le délai prévu et si l'utilisateur a activé un suivi intensif. Si le processus fcp_daemon cesse d'exécuter les scripts, les données signalées sur la console reflètent l'heure d'exécution du dernier script lancé. Il se peut également que l'agent de système d'exploitation cesse de renvoyer des données. L'arrêt du processus fcp_daemon permet à l'agent de reprendre son fonctionnement normal.
- SCRIPT_NONZERO_RETURN est renvoyé à la place de SCRIPT_NOT_FOUND ou SCRIPT_LAUNCH_ERROR sous Solaris.
- La fonction de scriptage ne fournit pas la globalisation complète ; des problèmes peuvent survenir lors de l'utilisation de caractères nationaux dans les fichiers de propriétés ou les sorties des scripts.
- Sur l'agent de système d'exploitation Windows, il n'est pas possible d'exécuter des scripts résidant sur une unité réseau mappée.
- Lorsque l'agent de système d'exploitation Windows est mis à niveau, la fonction de scriptage n'est pas activée par défaut. Modifiez KNTENV et remplacez `KNT_FCP_SCRIPT=FALSE` par `KNT_FCP_SCRIPT=TRUE`

Traitement des incidents liés au scriptage personnalisé
Traitement des incidents liés au scriptage personnalisé

La variable *KBB_RAS1* standard s'applique à l'agent de système d'exploitation et aux processus fcp_daemon. Pour appliquer un paramètre de trace spécifique au processus fcp_daemon uniquement, utilisez la variable *KXX_FCP_KBB_RAS1*. Lorsque cette dernière est définie, la valeur indiquée par *KBB_RAS1* est ignorée par le processus fcp_daemon.

Pour tracer les opérations consignées par les unités d'exécution de base de l'agent de système d'exploitation de la fonction :

```
KBB_RAS1=ERROR (UNIT:factory ALL)
```

Pour tracer les requêtes de scriptage provenant du serveur APM et les événements envoyés au serveur, ajoutez les entrées suivantes :

Sur Monitoring Agent for Linux OS

```
(UNIT:klz34 ALL) (UNIT:klz36 ALL)
```

Sur Monitoring Agent for UNIX OS

```
(UNIT:kux48 ALL) (UNIT:kux50 ALL)
```

Sur Monitoring Agent for Windows OS

```
(UNIT:knt84 ALL) (UNIT:knt86 ALL)
```

Pour afficher les traces TEMA afin de vérifier l'exécution d'une situation privée, ajoutez les entrées suivantes :

```
(UNIT:kraavp all) (UNIT:kraapv all)
```

Pour voir l'exécution des scripts et la façon dont les données des scripts sont analysées, définissez :

```
KXX_FCP_KBB_RAS1=Error (UNIT:command ALL)
```

Pour traiter les incidents liés à la communication entre l'agent de système d'exploitation et le processus fcp_daemon, ajoutez ce niveau de trace à *KBB_RAS1* et *KXX_FCP_KBB_RAS1* :

```
(UNIT:cps_socket FLOW) (UNIT:cpci FLOW)
```

Pour voir en détail l'interaction entre le processus de l'agent de système d'exploitation et le processus fcp_daemon, ajoutez *KBB_RAS1* et *KXX_FCP_KBB_RAS1* :

```
(UNIT:cps_socket ALL) (UNIT:cpci ALL)
```

Scénario de démarrage rapide
Cette section décrit les étapes minimales nécessaires pour configurer le scriptage personnalisé pour un scénario exemple.

La section suivante décrit les étapes minimales requises pour configurer un Monitoring Agent for Linux OS de sorte qu'il exécute deux scripts personnalisés.

Description des scripts personnalisés

Dans cet exemple, l'utilisateur possède deux scripts sous un répertoire /scripts_repo :

checkDIRsize.sh – Ce script vérifie la taille d'un répertoire spécifié qui est transmis en tant que paramètre d'entrée. La sortie est un entier : 4594740

cpu_mem_usage.sh – Ce script vérifie les pourcentages d'UC utilisée et les mégaoctets de mémoire de permutation utilisée. La sortie est renvoyée au format suivant : cpu1|96,5|23800

Le premier jeton correspond à l'ID de l'UC, le deuxième au pourcentage d'UC utilisée et le troisième à la mémoire de permutation utilisée en mégaoctets.

La personnalisation à effectuer pour que Monitoring Agent for Linux OS puisse exécuter ces scripts.

La fonction est activée avec les valeurs par défaut dès que l'agent de système d'exploitation est démarré :

Vous créez les fichiers de propriétés AnyName.`properties` sous le répertoire par défaut `rép_install/localconfig/lz/scripts_definitions`. Dans cet exemple, créez deux fichiers de propriétés, un pour chaque script, nommés checkDIRsize.properties et cpu_mem_usage.properties :

```
#CheckDIRsize.properties
ATTRIBUTE_NAME=OPT_DIR_SIZE
SCRIPT_PATH_WITH_PARMS=/scripts_repo/checkDIRsize.sh /opt
EXECUTION_FREQUENCY=20
OUTPUT_TYPE=INTEGER
```

```
#cpu_mem_usage.properties
ATTRIBUTE_NAME=cpu_mem_usage
SCRIPT_PATH_WITH_PARMS=/scripts_repo/cpu_mem_percentage.sh
OUTPUT_TYPE=string
TOKEN_TYPES=F,I
TOKEN_LABELS= Used CPU %, Swap MEM used MB
TOKEN_SEPARATOR=|
EXECUTION_FREQUENCY=10
```

Vous n'êtes pas obligé de redémarrer l'agent de système d'exploitation après avoir ajouté (ou modifié) les deux fichiers de propriétés. L'agent de système d'exploitation vérifie le répertoire des définitions de script à une fréquence définie (300 secondes par défaut). Ouvrez la console qui présente alors les détails et les résultats sous l'espace de travail "Scripts personnalisés".

Configuration de la collecte de données du système de fichiers de l'agent du système d'exploitation Linux

Monitoring Agent for Linux OS est configuré automatiquement. Toutefois, vous pouvez configurer le comportement de la collecte de données du système de fichiers.

Monitoring Agent for Linux OS a un comportement par défaut pour la collecte de données du système de fichiers.

Le comportement par défaut consiste à surveiller les systèmes de fichiers à partir de `/etc/fstab` uniquement. Une variable d'environnement *KBB_SHOW_MTAB_FS* est définie dans le fichier `lz.environment` pour contrôler le comportement de la collecte des données du système de fichiers. Si vous souhaitez surveiller tous les systèmes de fichiers (répertoriés dans `/etc/fstab` et `/etc/mtab`), vous pouvez définir KBB_SHOW_MTAB_FS=true.

KBB_SHOW_MTAB_FS
Cette variable est disponible dans le fichier *rép_install*`/config/.lz.environment`. La valeur par défaut est `false` et définit l'agent de surveillance des systèmes de fichiers à partir de `/etc/fstab` uniquement. Si vous souhaitez surveiller tous les systèmes de fichiers (répertoriés dans `/etc/fstab` et `/etc/mtab`), remplacez la valeur par `true`. Par exemple, *KBB_SHOW_MTAB_FS=true*.

Configuration de la surveillance de PHP

Vous devez configurer Monitoring Agent for PHP pour qu'il puisse collecter des données de l'application PHP surveillée.

Avant de commencer

1. Veillez à bien installer le package php-process. Si vous utilisez la commande `yum install` pour installer PHP, exécutez la commande `yum install php-process` pour installer le package php-process.
2. Vérifiez que le serveur HTTPD Apache est démarré avant de configurer l'agent.

Ouvrez le fichier de configuration `httpd.conf` du serveur HTTP Apache et assurez-vous que les options `mod_status` et `ExtendedStatus On` sont activées. Par exemple :

```
ExtendedStatus On
<Location /server-status>
        SetHandler server-status
        Order deny,allow
        Allow from all
        Allow from 127.0.0.1
</Location>
```

Dans l'exemple donné, `http://127.0.0.1/server-status` doit fonctionner pour que l'agent fonctionne correctement.

Remarque : Lynx ou Links doit être installé sous Linux pour que l'agent obtienne les données de surveillance.

Vérifiez que la commande `apachectl status` fonctionne sur le serveur Apache surveillé sans que le code de la commande `apachectl` ne soit modifié. Lynx doit être installé pour que la commande `apachectl status` fonctionne correctement.

Pourquoi et quand exécuter cette tâche

Afin d'éviter tout problème de droits lorsque vous configurez l'agent, veillez à utiliser le même ID d'utilisateur superutilisateur ou non superutilisateur que celui utilisé pour installer l'agent. Si vous avez installé votre agent en tant qu'utilisateur sélectionné et que vous voulez le configurer en tant qu'utilisateur, voir «Configuration des agents en tant qu'utilisateur non superutilisateur», à la page 188. Si vous avez installé et configuré votre agent en tant qu'utilisateur sélectionné et que vous voulez le démarrer en tant qu'un autre utilisateur, voir «Démarrage des agents en tant qu'utilisateur non superutilisateur», à la page 1042.

L'Agent PHP est un agent d'instance multiple. Vous devez créer la première instance et démarrer l'agent manuellement. Le nom de système géré inclut le nom d'instance que vous spécifiez, *nom_instance*`:`*nom_hôte*`:`*cp* par exemple, où *cp* est le code produit à deux caractères. Il est limité à 32 caractères. Le nom d'instance que vous entrez est limité à 28 caractères, moins la longueur de votre nom d'hôte. Par exemple, si vous indiquez PHP2 comme nom d'instance, le nom du système géré est `PHP2:hostname:PJ`.

Important : Si vous indiquez un nom d'instance long, le nom du système géré est tronqué et le code d'agent ne s'affiche pas correctement.

Procédure

- Si votre environnement est identique aux paramètres par défaut, vous pouvez utiliser le chemin d'exécution binaire par défaut, le chemin d'accès au fichier `php.ini` par défaut et le port par défaut pour configurer l'agent :
  a) Entrez :
  rép_install`/bin/php-agent.sh config` *nom_instance rép_install*`/samples/php_silent_config.txt`
  Où *nom_instance* est le nom à attribuer à l'instance, et *rép_install* est le répertoire d'installation de l'Agent PHP. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.
  b) Pour démarrer l'agent, entrez la commande suivante :
  rép_install`/bin/php-agent.sh start` *nom_instance*
- Pour configurer l'agent en éditant le fichier de réponses silencieux et en exécutant le script sans intervenir, procédez comme suit :
  a) Ouvrez *rép_install*`/samples/php_silent_config.txt` dans un éditeur de texte.
  b) Pour **`Location of PHP execution binary`**, vous pouvez spécifier le répertoire où se trouve l'exécution PHP. L'emplacement par défaut est `/usr/local/bin`.
  c) Pour **`Location of PHP INI file`**, vous pouvez spécifier le répertoire où se trouve le fichier `php.ini`. L'emplacement par défaut est `/etc`.

d) Pour **Web server port**, vous pouvez indiquer le numéro de port du serveur Web qui exécute WordPress. La valeur par défaut est 80.

e) Pour **Application DocumentRoot**, vous pouvez spécifier le DocumentRoot de l'application PHP WordPress. Utilisez une virgule pour séparer plusieurs enregistrements. Pour permettre à l'agent de localiser tous les enregistrements d'événements, utilisez la valeur par défaut ALL.

f) Sauvegardez et fermez le fichier php_silent_config.txt, puis entrez :
rép_install/bin/php-agent.sh config *nom_instance rép_install*/samples/php_silent_config.txt
Où *instance_name* est le nom à attribuer à l'instance, et *rép_install* est le répertoire d'installation de l'Agent PHP. Le répertoire d'installation par défaut est /opt/ibm/apm/agent.

g) Pour démarrer l'agent, entrez la commande suivante :
rép_install/bin/php-agent.sh start *nom_instance*

- Pour configurer l'agent en exécutant le script et en répondant aux invites, procédez comme suit :

a) Entrez :
rép_install/bin/php-agent.sh config *nom_instance*
Où *nom_instance* est le nom à attribuer à l'instance, et *rép_install* est le répertoire d'installation de l'Agent PHP.

b) A l'invite Edit Monitoring Agent for PHP settings, entrez 1 pour continuer.

c) A l'invite Location of PHP execution binary, appuyez sur Entrée pour accepter l'emplacement par défaut ou indiquez un emplacement de votre choix.

d) A l'invite Location of PHP INI file, appuyez sur Entrée pour accepter l'emplacement par défaut ou indiquez un emplacement de votre choix.

e) A l'invite Web server port, appuyez sur Entrée pour accepter la valeur par défaut ou indiquez un autre numéro de port.

f) A l'invite Application DocumentRoot, appuyez sur Entrée pour accepter la valeur par défaut ou indiquez le DocumentRoot de l'application PHP WordPress. Vous pouvez utiliser une virgule pour séparer plusieurs enregistrements.

g) Pour démarrer l'agent, entrez la commande suivante :
rép_install/bin/php-agent.sh start *nom_instance*

Résultats
L'agent évalue uniquement les performances des requêtes PHP dans les applications WordPress. Le chargement CSS et JS n'est pas évalué. L'agent n'utilise pas les arguments d'URL pour identifier les URL.

Que faire ensuite

Vous pouvez vérifier que les données de l'Agent PHP s'affichent dans la console Cloud APM.

Vous devez vous assurer que le plug-in WordPress de l'agent est activé. Pour assurer l'activation, procédez comme suit :

1. Dans un navigateur Web, entrez l'URL http://*hostname*:*port*/wp-admin/.
2. Accédez à la page d'administration en sélectionnant **Plugins** > **Installed Plugins**.
3. Vérifiez que le plug-in Agent PHP est activé. Le plug-in de l'Agent PHP est répertorié en tant qu'**agent WordPress**. En général, le plug-in est déjà activé. Si ce n'est pas le cas, cliquez sur **Activate**.

Configuration de la surveillance PostgreSQL

Vous devez configurer Monitoring Agent for PostgreSQL pour qu'il puisse collecter des données de la base de données PostgreSQL surveillée.

Avant de commencer

Vous devez installer le pilote JDBC PostgreSQL avant d'installer cet agent. Le chemin d'accès à ce pilote est requis lors de la configuration de l'agent.

Le pilote JDBC de type 4 est la nouvelle version et est donc recommandé. L'utilisateur peut installer le sous-type de JDBC version 4 en fonction de la version JDK utilisée par l'agent. Pour plus d'informations sur le mappage de la version JDBC vers la version JDK, accédez au site https://jdbc.postgresql.org/download.html.

Quelques-uns des attributs collectés par l'agent s'appuient sur l'extension `pg_stat_statements`. Pour ajouter `pg_stat_statements`, installez au préalable le package `postgresql-contrib`. Vous devez modifier le fichier de configuration `postgresql.conf` pour que le serveur PostgreSQL puisse charger l'extension `pg_stat_statements`.

1. Ouvrez le fichier `postgresql.conf` dans un éditeur de texte et mettez à jour la ligne `shared_preload_libraries` :

   ```
   shared_preload_libraries = 'pg_stat_statements'
   pg_stat_statements.track_utility = false
   ```

   Ces modifications sont requises pour surveiller les instructions SQL, à l'exception des commandes d'utilitaire.

   Remarque : Le statut de `pg_stat_statements.track_utility` est défini ou modifié uniquement par un superutilisateur.
2. Redémarrez le serveur PostgreSQL après avoir mis à jour et sauvegardé le fichier `postgresql.conf`.
3. Exécutez la commande SQL suivante en utilisant psql, qui doit être connecté à la base de données qui sera fournie ultérieurement dans la configuration d'agent pour la connectivité JDBC :

   ```
   create extension pg_stat_statements;
   select pg_stat_statements_reset();
   ```

   Remarque : La commande `create extension` et la fonction `pg_stat_statements_reset()` ne sont exécutées que par un superutilisateur.

   La vue `pg_stat_statements` doit être activée pour une base de données spécifique. Pour plus de détails, voir https://www.postgresql.org/docs/9.6/static/pgstatstatements.html.

Le fichier `pg_hba.conf` est le fichier de base de données PostgreSQL, qui contient les paramètres d'authentification. Lorsque le paramètre `auth-method` est défini sur `ident` dans le fichier `pg_hba.conf`, l'Agent PostgreSQL ne peut pas se connecter à la base de données PostgreSQL. Vérifiez que les paramètres d'authentification pour le paramètre `auth-method` sont corrects. Par exemple, vous pouvez définir les valeurs suivantes pour le paramètre `auth-method` : `md5`, `trust` ou `password`.

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent PostgreSQL.

Pourquoi et quand exécuter cette tâche

L'Agent PostgreSQL est un agent d'instance multiple. Vous devez créer la première instance et démarrer l'agent manuellement. Le nom de système géré inclut le nom d'instance que vous spécifiez, *nom_instance*:*nom_hôte*:*cp* par exemple, où *cp* est le code produit à deux caractères. Il est limité à 32 caractères. Le nom d'instance que vous entrez est limité à 28 caractères, moins la longueur de votre

nom d'hôte. Par exemple, si vous indiquez PostgreSQL2 comme nom d'instance, le nom du système géré est PostgreSQL2:hostname:PN.

Important : Si vous indiquez un nom d'instance long, le nom du système géré est tronqué et le code d'agent ne s'affiche pas entièrement.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de l'agent sur des systèmes Windows

Vous pouvez utiliser la fenêtre IBM Cloud Application Performance Management pour configurer l'agent sur des systèmes Windows.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Monitoring Agent for PostgreSQL**, puis cliquez sur **Configuration de l'agent**.
3. Dans la zone **Enter a unique instance name**, entrez le nom d'instance de l'agent et cliquez sur **OK**.
4. Dans la fenêtre **Monitoring Agent for PostgreSQL**, procédez comme suit :
   a. Dans la zone **Adresse IP**, entrez l'adresse IP d'un serveur PostgreSQL à surveiller à distance. Si l'agent est installé sur le serveur à surveiller, conservez la valeur par défaut.

      Remarque :

      Pour la surveillance à distance, les données des widgets **Pourcentage actuel utilisé de l'unité centrale** et **Mémoire physique utilisée (Mo)** ne sont pas disponibles sur le tableau de bord. Ces widgets affichent **N/A**.
   b. Dans la zone **Nom de base de données JDBC**, indiquez un nom de base de données pour remplacer le nom de base de données par défaut postgres.
   c. Dans la zone **Nom d'utilisateur JDBC**, indiquez un nom d'utilisateur pour remplacer le nom d'utilisateur par défaut postgres.
   d. Dans la zone **Mot de passe JDBC**, entrez le mot de passe de l'utilisateur JDBC.
   e. Dans la zone **Confirmer le mot de passe JDBC**, entrez de nouveau le mot de passe.
   f. Dans la zone **Numéro de port JDBC**, indiquez un numéro de port pour remplacer le numéro de port par défaut 5432.
   g. Dans la zone **Fichier JAR JDBC**, indiquez le chemin d'accès au connecteur PostgreSQL pour le fichier JAR Java et cliquez sur **Suivant**.
   h. Dans la zone **Niveau de trace Java**, entrez le niveau de trace selon les instructions du support IBM. Le niveau de trace par défaut est Erreur.
   i. Cliquez sur **OK**. L'instance de l'agent est affichée dans la fenêtre IBM Performance Management.
5. Cliquez avec le bouton droit de la souris sur l'instance **Monitoring Agent for PostgreSQL**, puis cliquez sur **Démarrer**.

Que faire ensuite
Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console, voir «Démarrage de la console Cloud APM», à la page 1003.

Pour obtenir de l'aide sur le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration de l'agent sur des systèmes Linux

Pour configurer l'agent sur des systèmes d'exploitation Linux, vous pouvez exécuter le script ou répondre à des invites.

Procédure

1. Sur la ligne de commande, entrez la commande suivante :
   rép_install/bin/postgresql-agent.sh config *nom_instance*
2. A l'invite d'édition des paramètres PostgreSQL, entrez 1 pour continuer.
3. A l'invite d'entrée d'une valeur pour les paramètres suivants, appuyez sur Entrée pour accepter la valeur par défaut ou indiquez une autre valeur et appuyez sur Entrée :
   - Adresse IP

     Remarque :

     Entrez l'adresse IP d'un serveur PostgreSQL à surveiller à distance. Si l'agent est installé sur le serveur à surveiller, conservez la valeur par défaut.

     Pour la surveillance à distance, les données des widgets **Pourcentage actuel utilisé de l'unité centrale** et **Mémoire physique utilisée (Mo)** ne sont pas disponibles sur le tableau de bord. Ces widgets affichent **N/A**.
   - Nom de base de données JDBC
   - Nom d'utilisateur JDBC
   - Mot de passe JDBC
   - Numéro de port JDBC
   - Fichier JAR JDBC

   Important : La version du fichier JAR JDBC doit être identique à la version de la base de données PostgreSQL surveillée.
4. A l'invite d'entrée d'une valeur pour le paramètre `Niveau de trace Java`, entrez 2 pour accepter la valeur par défaut ou indiquez un niveau de trace selon les instructions du support IBM.
5. Exécutez la commande suivante pour démarrer l'agent :

   ```
   rép_install/bin/postgresql-agent.sh start nom_instance
   ```

Que faire ensuite
Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Pour obtenir de l'aide sur le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de

configuration pour créer une instance et mettre à jour les valeurs de configuration de l'agent. Ce mode de configuration est appelé mode silencieux.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'Agent PostgreSQL sur les systèmes Linux and Windows. Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

- Pour configurer l'agent en éditant le fichier de réponses silencieux et en exécutant le script sans répondre aux invites, procédez comme suit :
  1. Dans un éditeur de texte, ouvrez le fichier de réponses silencieux disponible à l'emplacement suivant : *rép_install*/samples/postgresql_silent_config.txt, où *rép_install* est le répertoire d'installation de l'Agent PostgreSQL. Le répertoire d'installation par défaut est /opt/ibm/apm/agent.
  2. Pour éditer le fichier de configuration en mode silencieux, procédez comme suit :
     a. Pour le paramètre **Adresse IP**, spécifiez l'adresse IP d'un serveur PostgreSQL à surveiller à distance. Si l'agent est installé sur le serveur à surveiller, conservez la valeur par défaut.

        Remarque :

        Pour la surveillance à distance, les données des widgets **Pourcentage actuel utilisé de l'unité centrale** et **Mémoire physique utilisée (Mo)** ne sont pas disponibles sur le tableau de bord. Ces widgets affichent **N/A**.
     b. Pour le paramètre **Nom de base de données JDBC**, indiquez un nom de base de données pour remplacer le nom de base de données par défaut postgres.
     c. Pour le paramètre **Nom d'utilisateur JDBC**, indiquez un nom d'utilisateur pour remplacer le nom par défaut postgres.
     d. Pour le paramètre **Mot de passe JDBC**, entrez le mot de passe de l'utilisateur JDBC.
     e. Pour le paramètre **Numéro de port JDBC**, indiquez un numéro de port pour remplacer le numéro de port par défaut 5432.
     f. Pour le paramètre **Fichier JAR JDBC**, indiquez le chemin d'accès au connecteur PostgreSQL pour le fichier JAR Java si le chemin d'accès par défaut est incorrect. Le chemin d'accès par défaut du fichier JAR Java est :

        /opt/PostgreSQL/lib/postgresql-9.3-1100.jdbc4.jar

        Important : La version du fichier JAR JDBC doit être compatible avec la version de la base de données PostgreSQL surveillée.
     g. Pour le paramètre **Niveau de trace Java**, indiquez le niveau de trace selon les instructions du support IBM. Le niveau de trace par défaut est Erreur.
  3. Sauvegardez et fermez le fichier de réponses silencieux, puis exécutez la commande suivante :

     ```
     rép_install/bin/postgresql-agent.sh config
     nom_instance
     rép_install/samples/postgresql_silent_config.txt
     ```

     Où *nom_instance* est le nom à attribuer à l'instance.
  4. Pour démarrer l'agent, entrez la commande suivante :

     ```
     rép_install/bin/postgresql-agent.sh start nom_instance
     ```

Que faire ensuite
Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Pour obtenir de l'aide sur le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration de la surveillance Python

Il est possible de surveiller à la fois les applications Python sur site et IBM Cloud. Effectuez les étapes de configuration correspondantes en fonction de votre type d'application.

Pourquoi et quand exécuter cette tâche

Configurez le collecteur de données Python pour surveiller vos applications Python sur site et IBM Cloud.

Procédure

- Configurez le collecteur de données pour surveiller les applications IBM Cloud.
  a) Configurez le collecteur de données Python afin qu'il collecte et envoie des données pour les applications IBM Cloud. Pour obtenir des instructions, voir «Configuration du collecteur de données Python pour les applications IBM Cloud», à la page 689.
  b) Facultatif : Personnalisez les fonctions de surveillance du collecteur de données Python. Pour plus d'informations, voir «Personnalisation du collecteur de données Python pour les applications IBM Cloud», à la page 690.
- Configurez le collecteur de données pour surveiller les applications sur site.
  a) Configurez le collecteur de données afin qu'il collecte et envoie des données au serveur Cloud APM. Pour obtenir des instructions, voir «Configuration du collecteur de données Python pour les applications sur site», à la page 695.
  b) Facultatif : Personnalisez les fonctions de surveillance du collecteur de données Python. Pour plus d'informations, voir «Personnalisation du collecteur de données Python pour les applications sur site», à la page 696.

Configuration du collecteur de données Python pour les applications IBM Cloud

Pour collecter des informations sur les applications Python sur IBM Cloud, vous devez configurer les collecteur de données Python.

Avant de commencer

1. Assurez-vous que les applications Python que vous voulez surveiller ont des noms uniques. Le collecteur de données Python gère deux applications différentes ayant le même nom comme une seule et même application, ce qui peut entraîner des problèmes d'affichage des données sur la console Cloud APM.
2. Téléchargez le package du collecteur de données à partir du site Web IBM Marketplace. Pour des instructions détaillées, voir «Téléchargement de vos agents et de vos collecteurs de données», à la page 105.

Pourquoi et quand exécuter cette tâche

Pour configurer le collecteur de données, déployez d'abord un serveur de modules PyPi, puis installez le collecteur de données dans une application Python Django.

Procédure

1. Extrayez les fichiers du package du collecteur de données. Le module `python_datacollector_8.1.4.0.tgz` est inclus dans le répertoire extrait.

2. Extrayez le module `python_datacollector_8.1.4.0.tgz`, par exemple, en exécutant la commande suivante :

```
tar -zxf python_datacollector_8.1.4.0.tgz
```

3. Recherchez le fichier `manifest.yml` du serveur de packages dans le répertoire d'extraction et définissez-y le domaine, l'hôte et le nom, comme illustré dans l'exemple suivant :

```
domain: mybluemix.net
name: pythondc
host: pythondc
```

   A faire : Les valeurs *host* et *name* doivent être identiques et uniques.

4. A partir du répertoire `python_dc`, envoyez l'application `pythondc` dans IBM Cloud en exécutant la commande suivante :

```
cf push
```

5. Dans le fichier `requirements.txt` de votre application Python, ajoutez les lignes suivantes :

```
cryptography==1.9.0
--extra-index-url https://<votre_nom_hôte_et_domaine>/python-dc-repos/simple/
ibm_python_dc
```

6. Dans le fichier `settings.py` de votre application Python, ajoutez `ibm_python_dc.kpg_plugin.ResourceMiddleware` au début de la section `MIDDLEWARE_CLASSES`, par exemple :

```
MIDDLEWARE_CLASSES = (
    "ibm_python_dc.kpg_plugin.ResourceMiddleware",
    "mezzanine.core.middleware.UpdateCacheMiddleware",
    'django.contrib.sessions.middleware.SessionMiddleware',
    'django.middleware.common.CommonMiddleware',
```

7. A partir du répertoire qui contient le fichier `manifest.yml` de votre application Python, exécutez la commande suivante :

```
cf push
```

   Conseil : Pour un fichier `manifest.yml` exemple, voir «Exemple de fichier manifest.yml», à la page 193.

Résultats
Le collecteur de données est configuré et il est connecté au serveur Cloud APM.

Que faire ensuite

Vous pouvez vérifier que les données de surveillance de votre application IBM Cloud sont affichées dans la console Cloud APM. Pour obtenir des instructions de démarrage de la console Cloud APM, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.

Personnalisation du collecteur de données Python pour les applications IBM Cloud
Vous pouvez ajouter des variables d'environnement dans l'interface utilisateur IBM Cloud pour personnaliser la surveillance de votre application IBM Cloud. Utilisez les informations suivantes pour ajouter des variables en fonction de vos besoins.

Variables d'environnement définies par l'utilisateur pour le collecteur de données Python

Vous pouvez utiliser les informations du tableau suivant pour personnaliser la surveillance de Python sur IBM Cloud.

Tableau 192. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance de Python sur IBM Cloud

Nom de la variable	Importance	Valeur	Description
APM_BM_GATEWAY_URL	Facultative	• https://*<IP ou nom d'hôte du serveur>*:443 • http://*<IP ou nom d'hôte du serveur>*:80	L'URL de la passerelle de serveur sur site cible.
APM_KEYFILE_PSWD	Facultative	Mot de passe chiffré du fichier de clés	Le mot de passe chiffré du fichier de clés qui est apparié avec le fichier de clés. Si vous êtes un utilisateur Linux, vous pouvez utiliser la commande `echo -n <mot de passe du fichier de clés> | base64` pour chiffrer votre mot de passe. **Remarque :** Définissez cette variable uniquement lorsque vous avez configuré la passerelle pour utiliser HTTPS.
APM_KEYFILE_URL	Facultative	http://*<serveur HTTP hébergé>*:*<port>*/keyfile.p12	L'URL de téléchargement du fichier de clés. **Remarque :** Définissez cette variable uniquement lorsque vous avez configuré la passerelle pour utiliser HTTPS.
KPG_ENABLE_DEEPDIVE	Facultative	• False • True	Active ou désactive la collecte des données de diagnostic. • True : La valeur par défaut. Si vous définissez cette variable sur `True`, les données de diagnostic sont collectées. • False : Si vous définissez cette variable sur `False`, les données de diagnostic ne sont pas collectées. Si vous ne définissez pas cette variable, les données de diagnostic sont collectées.

Tableau 192. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance de Python sur IBM Cloud (suite)

Nom de la variable	Importance	Valeur	Description
KPG_DD_CONFIG_FILE	Facultative	Nom de fichier du fichier de configuration de surveillance des diagnostics.	Nom de fichier du fichier de configuration de surveillance des diagnostics. Le nom de fichier par défaut est `kpg_dd_config.xml`. **Remarque :** Après avoir personnalisé les paramètres dans ce fichier, vous devez le placer dans le répertoire racine de l'application. Si vous ne définissez pas cette variable, le fichier de configuration par défaut `kpg_dd_config.xml` du module de collecteur de données est utilisé.
KPG_DD_APP_PATH	Facultative	Chemin d'accès de l'application Python.	Le chemin d'accès de l'application Python ou du module pour lequel le collecteur de données collecte des données de diagnostic. Séparez les chemins d'accès des différentes applications et modules Python que vous voulez surveiller à l'aide d'un point-virgule `;`. Si vous ne définissez pas cette variable, le collecteur de données collecte des données pour les demandes et les modules que votre d'application utilise. Les données des demandes dans la lib Python ne sont pas collectées.

Tableau 192. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance de Python sur IBM Cloud (suite)

Nom de la variable	Importance	Valeur	Description
KPG_DD_SECURITY_FILTER	Facultative	• True • False	• True : La valeur par défaut. Si vous définissez cette variable sur `True`, les valeurs (telles que les mots de passe) sont masquées dans les instructions SQL et les paramètres ne sont pas affichés dans le widget de groupe **Contexte des demandes**. • False : Si vous définissez cette variable sur `False`, les valeurs (telles que les mots de passe) ne sont pas masquées dans les instructions SQL et les paramètres sont affichés dans le widget de groupe **Contexte des demandes**. Si vous ne définissez pas cette variable, les valeurs (telles que les mots de passe) sont masquées dans les instructions SQL et les paramètres ne sont pas affichés dans le widget de groupe **Contexte des demandes**.
KPG_GC_STATS	Facultative	True	Toutes les fonctions statistiques de récupération de place de Python sont activées. Lorsque vous définissez cette valeur sur `True`, cela revient à exécuter la commande suivante : `gc.set_debug(gc.DEBUG_STATS | gc.DEBUG_COLLECTABLE | gc.DEBUG_UNCOLLECTABLE | gc.DEBUG_INSTANCES | gc.DEBUG_OBJECTS )` Pour désactiver KPG_GC_STATS, supprimez cette variable d'environnement. Ne la définissez pas sur `False`. **Remarque :** Ne définissez jamais `KPG_SAVE_ALL=True` dans votre environnement de production officiel. C'est uniquement réservé au mode débogage. Assurez-vous que la mémoire affectée à l'application est suffisante.

Tableau 192. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance de Python sur IBM Cloud (suite)

Nom de la variable	Importance	Valeur	Description
KPG_LOG_LEVEL	Facultative	• DEBUG • ERROR • INFO	• DEBUG : Seules les informations de débogage utiles sont imprimées dans le journal, par exemple, les données collectées, les données envoyées au serveur et la réponse du serveur. • ERROR : Seules les informations concernant les exceptions et les situations imprévues sont imprimées dans le journal. • INFO : Les informations récapitulatives concernant le collecteur de données permettant à l'utilisateur d'être informé de ses activités sont imprimées dans le journal.
KPG_LOG_TOCONSOLE	Facultative	• Y • True • Toute autre valeur qui n'est pas `False`	Le journal est imprimé vers la console et vous pouvez l'afficher en exécutant la commande **`cf logs <nom_app>`**.
KPG_SAVE_ALL	Facultative	True	Tous les objets non référencés sont enregistrés dans `gc.garbage`, et vous devez effacer `gc.garbage` toutes les minutes (le collecteur de données l'efface pour vous). Lorsque la valeur est définie sur `True`, cela revient à exécuter la commande suivante : `gc.set_debug(gc.SAVE_ALL)` Pour désactiver KPG_SAVE_ALL, supprimez cette variable d'environnement. Ne la définissez pas sur `False`. **Remarque :** Ne définissez jamais `KPG_SAVE_ALL=True` dans votre environnement de production officiel. C'est uniquement réservé au mode débogage. Assurez-vous que la mémoire affectée à l'application est suffisante.

Annulation de la configuration du collecteur de données Python pour les applications IBM Cloud

Si vous n'avez pas besoin de surveiller votre environnement Python ou si vous souhaitez mettre à niveau le collecteur de données Python, vous devez d'abord annuler la configuration des paramètres précédents pour le collecteur de données Python.

Procédure

1. Accédez au répertoire de base de votre application Python.
2. Supprimez les lignes suivantes du fichier `requirements.txt` de l'application :

```
--extra-index-url https://<votre_nom_hôte_et_domaine>/python_dc/static/python-dc-repos/
simple/
ibm-python-dc
```

3. Dans le fichier `settings.py`, supprimez la ligne suivante de la section `MIDDLEWARE_CLASSES` :

```
ibm_python_dc.kpg_plugin.ResourceMiddleware
```

4. Exécutez la commande suivante pour renvoyer l'application afin que les modifications soient prises en compte :

```
cf push
```

Résultats

Vous avez correctement annulé la configuration du collecteur de données Python.

Que faire ensuite

Une fois que vous avez configuré le collecteur de données, la console Cloud APM continue d'afficher le collecteur de données dans les applications auxquelles vous l'avez ajouté. La console Cloud APM indique qu'aucune donnée n'est disponible pour l'application et n'indique pas que le collecteur de données est hors ligne. Pour plus d'informations sur la manière de supprimer le collecteur de données d'applications et de groupes de ressources, voir «Suppression de collecteurs de données de la console Cloud APM», à la page 193.

Configuration du collecteur de données Python pour les applications sur site

Pour collecter des informations sur les applications Python exécutées dans votre environnement local, vous devez configurer le collecteur de données Python.

Avant de commencer

1. Assurez-vous que les applications Python que vous voulez surveiller ont des noms uniques. Le collecteur de données Python gère deux applications différentes ayant le même nom comme une seule et même application, ce qui peut entraîner des problèmes d'affichage des données sur la console Cloud APM.
2. Téléchargez le package du collecteur de données à partir du site Web IBM Marketplace. Pour des instructions détaillées, voir «Téléchargement de vos agents et de vos collecteurs de données», à la page 105.

Pourquoi et quand exécuter cette tâche

Le module de collecteur de données est préconfiguré avec un fichier `global.environment` préconfiguré et un `keyfile.p12` qui est copié dans le dossier `etc`. En conséquence, le collecteur de données se connecte automatiquement au serveur Cloud APM.

La procédure suivante configure le collecteur de données dans votre application Python avec les paramètres par défaut. Pour personnaliser la configuration du collecteur de données, utilisez des variables d'environnement dans les fichiers de configuration du collecteur de données. Pour plus d'informations, voir «Personnalisation du collecteur de données Python pour les applications sur site», à la page 696.

Procédure

1. Extrayez les fichiers du package du collecteur de données. Le module `python_datacollector_8.1.4.0.tgz` est inclus dans le répertoire extrait.
2. Procédez à l'extraction des fichiers à partir du module du collecteur de données, par exemple en exécutant la commande suivante :

   ```
   tar -zxf python_datacollector_8.1.4.0.tgz
   ```

3. Depuis le répertoire `python_dc`, exécutez la commande suivante :

   ```
   python server.py
   ```

4. Exécutez la commande suivante :

   ```
   pip install ibm_python_dc --extra-index-url http://nom ou adresse IP de l'hôte:8000/
   python-dc-repos/simple/ --trusted-host nom ou adresse IP de l'hôte
   ```

   où *nom ou adresse IP de l'hôte* est le nom ou l'adresse IP de l'hôte permettant d'exécuter votre référentiel de collecteur de données Python.

   Important : Utilisez le nom ou l'adresse IP pour spécifier l'hôte de l'URL et l'hôte sécurisé dans cette commande. Par exemple, si vous spécifiez l'hôte en utilisant l'adresse IP `9.42.36.180`, la commande est la suivante :

   ```
   pip install ibm_python_dc --extra-index-url http://9.42.36.180:8000/
   python-dc-repos/simple/ --trusted-host 9.42.36.180
   ```

5. Dans le fichier `settings.py` de votre application Python, ajoutez `ibm_python_dc.kpg_plugin.ResourceMiddleware` à la section `MIDDLEWARE_CLASSES` au format utilisé dans l'exemple suivant :

   ```
   MIDDLEWARE_CLASSES = (
       "ibm_python_dc.kpg_plugin.ResourceMiddleware",
       "mezzanine.core.middleware.UpdateCacheMiddleware",
       'django.contrib.sessions.middleware.SessionMiddleware',
       'django.middleware.common.CommonMiddleware',
   ```

Résultats
Le collecteur de données est configuré avec les paramètres par défaut et il est connecté au serveur Cloud APM.

Que faire ensuite
Vous pouvez désormais vous connecter au serveur Cloud APM pour afficher les données de surveillance.

A faire : Après avoir ajouté votre application Python à la console Cloud APM, vous pouvez afficher ses données de surveillance dans le composant nommé application Python Runtime.

Pour obtenir des instructions de démarrage de la serveur Cloud APM, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.

Personnalisation du collecteur de données Python pour les applications sur site
En modifiant des fichiers dans le module de collecteur de données, vous pouvez définir les variables d'environnement de façon à personnaliser la surveillance pour votre application Python.

Deux fichiers sont fournis pour personnaliser les paramètres du collecteur de données, `global.environment` et `config.properties`. Après avoir modifié les paramètres dans ces fichiers, redémarrez l'application Python pour que les modifications soient prises en compte.

En modifiant le fichier `global.environment`, vous pouvez personnaliser la connexion entre le collecteur de données et le serveur Cloud APM. Si vous voulez utiliser un autre serveur Cloud APM au lieu de la valeur par défaut, ou si le fichier de clés ou son mot de passe est changé, modifiez le serveur Cloud APM de façon à reconnecter le collecteur de données au serveur Cloud APM.

En modifiant le fichier `config.properties`, vous pouvez personnaliser le comportement du collecteur de données en fonction de vos besoins, par exemple, activer ou désactiver la trace de méthode.

Le fichier de configuration `global.environment`

Le Tableau 193, à la page 697 indique les variables d'environnement que vous pouvez définir dans le fichier de configuration `global.environment`, ainsi que leur description. Vous pouvez trouver le fichier `global.environment` dans le dossier `etc` dans lequel votre collecteur de données Python est installé, par exemple, dans le répertoire `/root/.pyenv/versions/3.5.2/lib/python3.5/site-packages/ibm_python_dc/etc`.

Tableau 193. Variables d'environnement prises en charge dans le fichier `global.environment`

Nom de la variable	Importance	Valeur	Description
APM_BM_GATEWAY_URL	Facultative	• https://*<IP ou nom d'hôte du serveur>*:443 • http://*<IP ou nom d'hôte du serveur>*:80	L'URL de la passerelle de serveur sur site cible.
APM_KEYFILE_PSWD	Facultative	Mot de passe du fichier de clés	Le mot de passe du fichier de clés qui est apparié avec le fichier de clés. **Remarque :** Définissez cette variable uniquement lorsque vous avez configuré la passerelle pour utiliser HTTPS.
APM_KEYFILE_URL	Facultative	http://*<serveur http hébergé>*:*<port>*/keyfile.p12	L'URL de téléchargement du fichier de clés. **Remarque :** Définissez cette variable uniquement lorsque vous avez configuré la passerelle pour utiliser HTTPS.

Le fichier `config.properties`

Le Tableau 194, à la page 698 indique les variables d'environnement que vous pouvez définir dans le fichier de configuration `config.properties`, ainsi que leur description. Vous pouvez trouver le fichier `config.properties` dans le répertoire d'installation de votre collecteur de données Python, par exemple, dans le répertoire `/root/.pyenv/versions/3.5.2/lib/python3.5/site-packages/ibm_python_dc`.

Tableau 194. Variables d'environnement prises en charge dans le fichier `config.properties`

Nom de la variable	Importance	Valeur	Description
KPG_ENABLE_DEEPDIVE	Facultative	• False • True	• False : La valeur par défaut. Si vous définissez cette variable sur `False`, les données de diagnostic ne seront pas collectées. • True : Si vous définissez cette variable sur `True`, les données de diagnostic seront collectées. La valeur par défaut est `True`. Si vous ne définissez pas cette variable, les données de diagnostic ne seront pas collectées.
KPG_DD_CONFIG_FILE	Facultative	Nom de fichier du fichier de configuration de surveillance des diagnostics.	Nom de fichier du fichier de configuration de surveillance des diagnostics. Le nom de fichier par défaut est `kpg_dd_config.xml`. **Remarque :** Après avoir personnalisé les paramètres dans ce fichier, vous devez le placer dans le répertoire racine de l'application. Si vous ne définissez pas cette variable, le fichier de configuration par défaut `kpg_dd_config.xml` du module de collecteur de données sera utilisé.
KPG_DD_APP_PATH	Facultative	Chemin d'accès de l'application Python.	Le chemin d'accès de l'application Python ou du module pour lequel le collecteur de données collecte des données de diagnostic. Séparez les chemins d'accès des différentes applications et modules Python que vous voulez surveiller à l'aide d'un point-virgule `;`. Si vous ne définissez pas cette variable, le collecteur de données collectera des données pour les demandes et les modules que votre d'application utilise. Les données des demandes dans la lib Python ne seront pas collectées.

Tableau 194. Variables d'environnement prises en charge dans le fichier `config.properties` (suite)

Nom de la variable	Importance	Valeur	Description
KPG_DD_SECURITY_FILTER	Facultative	• True • False	• True : La valeur par défaut. Si vous définissez cette variable sur `True`, les valeurs (telles que les mots de passe) seront masquées dans les instructions SQL et les paramètres ne seront pas affichés dans le widget de groupe **Contexte des demandes**. • False : Si vous définissez cette variable sur `False`, les valeurs (telles que les mots de passe) ne seront pas masquées dans les instructions SQL et les paramètres ne seront pas affichés dans le widget de groupe **Contexte des demandes**. Si vous ne définissez pas cette variable, les valeurs (telles que les mots de passe) seront masquées dans les instructions SQL et les paramètres ne seront pas affichés dans le widget de groupe **Contexte des demandes**.
KPG_GC_STATS	Facultative	True	Toutes les fonctions statistiques de récupération de place de Python sont activées. Lorsque vous définissez cette valeur sur `True`, cela revient à exécuter la commande suivante : `gc.set_debug(gc.DEBUG_STATS | gc.DEBUG_COLLECTABLE | gc.DEBUG_UNCOLLECTABLE | gc.DEBUG_INSTANCES | gc.DEBUG_OBJECTS )` Pour désactiver KPG_GC_STATS, supprimez cette variable d'environnement. Ne la définissez pas sur `False`. La valeur par défaut est `True`. **Remarque :** Ne définissez jamais KPG_GC_STATS=`True` dans votre environnement de produit officiel. C'est uniquement réservé au mode débogage. Et assurez-vous que la mémoire affectée à l'application est suffisante.

Tableau 194. Variables d'environnement prises en charge dans le fichier `config.properties` (suite)

Nom de la variable	Importance	Valeur	Description
KPG_LOG_LEVEL	Facultative	• DEBUG • ERROR • INFO	• DEBUG : Seules les informations de débogage utiles seront imprimées dans le journal, par exemple, les données collectées, les données envoyées au serveur et la réponse du serveur. • ERROR : Seules les informations concernant les exceptions et les situations très imprévues seront imprimées dans le journal. • INFO : Les informations récapitulatives concernant le collecteur de données permettant à l'utilisateur d'être informé de ses activités seront imprimées dans le journal. La valeur par défaut est ERROR.
KPG_LOG_TOCONSOLE	Facultative	• Y • True • Toute autre valeur qui n'est pas `False`	Le journal sera imprimé vers la console et vous pourrez l'afficher en exécutant la commande **`cf logs <nom_app>`**. La valeur par défaut est `True`.
KPG_SAVE_ALL	Facultative	True	Tous les objets non référencés seront enregistrés dans `gc.garbage`, et vous devrez effacer `gc.garbage` toutes les minutes (le collecteur de données l'effacera pour vous). Lorsque la valeur est définie sur `True`, cela revient à exécuter la commande suivante : `gc.set_debug(gc.SAVE_ALL)` Pour désactiver KPG_SAVE_ALL, supprimez cette variable d'environnement. Ne la définissez pas sur `False`. La valeur par défaut est `True`. **Remarque :** Ne définissez jamais `KPG_SAVE_ALL=True` dans votre environnement de produit officiel. C'est uniquement réservé au mode débogage. Et assurez-vous que la mémoire affectée à l'application est suffisante.

Tableau 194. Variables d'environnement prises en charge dans le fichier `config.properties` (suite)			
Nom de la variable	**Importance**	**Valeur**	**Description**
APM_GW_PROXY_CONNECTION	Facultative	http://*<ip ou nom d'hôte du serveur>*:port	Le proxy HTTP ou HTTPS que le collecteur de données Python utilise pour envoyer des données de surveillance.

Annulation de la configuration du collecteur de données Python pour les applications sur site
Si vous n'avez pas besoin de surveiller votre environnement Python ou si vous souhaitez mettre à niveau le collecteur de données Python, vous devez d'abord annuler la configuration des paramètres précédents pour le collecteur de données Python.

Procédure

1. Accédez au répertoire de base de votre application Python.
2. Supprimez les lignes suivantes du fichier `requirements.txt` de l'application :

```
--extra-index-url https://<votre_nom_hôte_et_domaine>/python_dc/static/python-dc-repos/
simple/
ibm-python-dc
```

3. Dans le fichier `settings.py`, supprimez la ligne suivante de la section `MIDDLEWARE_CLASSES` :

```
ibm_python_dc.kpg_plugin.ResourceMiddleware
```

4. Exécutez la commande `pip uninstall ibm_python_dc` pour désinstaller le collecteur de données Python de l'exécution Python.

Résultats
Vous avez correctement annulé la configuration du collecteur de données Python.

Que faire ensuite
Une fois que vous avez configuré le collecteur de données, la console Cloud APM continue d'afficher le collecteur de données dans les applications auxquelles vous l'avez ajouté. La console Cloud APM indique qu'aucune donnée n'est disponible pour l'application et n'indique pas que le collecteur de données est hors ligne. Pour plus d'informations sur la manière de supprimer le collecteur de données d'applications et de groupes de ressources, voir «Suppression de collecteurs de données de la console Cloud APM», à la page 193.

Configuration de la surveillance de RabbitMQ

Monitoring Agent for RabbitMQ surveille l'état de santé et les performances des ressources du cluster RabbitMQ, telles que les noeuds, les files d'attente et les canaux du cluster. Vous devez configurer l'agent RabbitMQ afin qu'il puisse collecter des données RabbitMQ.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel.
- Assurez-vous que l'utilisateur de RabbitMQ qui se connecte au noeud dispose du droit de lecture et que la balise de surveillance, d'administrateur ou de gestion est activée pour cet utilisateur.
- Assurez-vous que le plug-in de gestion de RabbitMQ est activé sur tous les noeuds du cluster, parce qu'en cas d'échec d'un noeud du cluster, l'agent RabbitMQ se connecte à un noeud homologue qui est disponible dans le cluster.

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent RabbitMQ.

Pourquoi et quand exécuter cette tâche

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

L'agent RabbitMQ est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

- Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser la fenêtre IBM Cloud Application Performance Management ou le fichier de réponses silencieux.
- Pour configurer l'agent sur les systèmes Linux, vous pouvez exécuter le script et répondre aux invites, ou utiliser le fichier de réponses silencieux.

Configuration de l'agent sur des systèmes Windows

Pour pouvez utiliser la fenêtre IBM Cloud Application Performance Management pour configurer l'agent sur des systèmes Windows.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Monitoring Agent for RabbitMQ**, puis cliquez sur **Configuration de l'agent**.

   A faire : La première fois que vous configurez l'agent, l'option **Configuration de l'agent** est désactivée. Pour reconfigurer l'agent, cliquez sur **Reconfigurer**.
3. Dans la zone **Entrez un nom d'instance unique**, entrez le nom d'instance de l'agent et cliquez sur **OK**.
4. Dans la fenêtre **Monitoring Agent for RabbitMQ**, indiquez des valeurs pour les paramètres de configuration et cliquez sur **Suivant**.

   Pour plus d'informations sur les paramètres de configuration, voir la rubrique suivante : «Paramètres de configuration de l'agent», à la page 704
5. Cliquez avec le bouton droit de la souris sur l'instance **Monitoring Agent for RabbitMQ**, puis cliquez sur **Démarrer**.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console, voir «Démarrage de la console Cloud APM», à la page 1003.

Pour obtenir de l'aide sur le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration de l'agent sur des systèmes Linux

Pour configurer l'agent sur des systèmes d'exploitation Linux, vous pouvez exécuter le script ou répondre à des invites.

Procédure

1. Dans la ligne de commande, entrez la commande suivante : *rép_install*`/bin/rabbitmq.sh config` *nom_instance* où *nom_instance* est le nom que vous voulez donner à l'instance :

2. Lorsque vous êtes invité à saisir une valeur pour les paramètres suivants, appuyez sur Entrée pour accepter la valeur par défaut ou spécifiez une valeur et appuyez sur Entrée :
   - Adresse IP
   - Nom d'utilisateur
   - Mot de passe
   - Numéro de port
   - Accueil Java
   - Niveau de trace Java

   Pour plus d'informations sur les paramètres de configuration, voir la rubrique suivante : «Paramètres de configuration de l'agent», à la page 704
3. Exécutez la commande suivante pour démarrer l'agent :

```
rép_install/bin/rabbitmq.sh start nom_instance
```

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Pour obtenir de l'aide sur le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'agent RabbitMQ sur les systèmes Linux and Windows. Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

1. Ouvrez le fichier de réponses silencieux disponible à l'emplacement suivant : *rép_install*\samples\rabbitmq_silent_config.txt
2. Dans le fichier rabbitmq_silent_config.txt, spécifiez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.

   Pour plus d'informations sur les paramètres de configuration, voir la rubrique suivante : «Paramètres de configuration de l'agent», à la page 704
3. Sauvegardez le fichier de réponses, puis exécutez la commande suivante :

   Linux AIX *rép_install*/bin/rabbitmq-agent.sh config *rép_install*/samples/rabbitmq_silent_config.txt

   Windows *rép_install*/bin/rabbitmq-agent.bat config *rép_install*/samples/rabbitmq_silent_config.txt
4. Démarrez l'agent :

   Linux AIX Exécutez la commande suivante : *rép_install*\bin\rabbitmq-agent.sh start

   Windows Cliquez avec le bouton droit de la souris sur **Monitoring Agent for RabbitMQ**, puis cliquez sur **Démarrer**.

Que faire ensuite
Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Pour obtenir de l'aide sur le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Paramètres de configuration de l'agent

Lorsque vous configurez l'agent RabbitMQ, vous pouvez modifier les valeurs par défaut des paramètres, comme le nom de l'instance et les certificats de validation SSL.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de l'agent RabbitMQ.

Tableau 195. Noms et descriptions des paramètres de configuration pour l'agent RabbitMQ

Nom de paramètre	Description	Zone obligatoire
Adresse IP	Adresse IP du noeud sur lequel l'application RabbitMQ est installée.	Oui
Nom d'utilisateur	Nom de l'utilisateur RabbitMQ.	Yes
mot de passe	Mot de passe permettant de se connecter à l'interface utilisateur de gestion RabbitMQ.	Yes
Confirmer le mot de passe	Mot de passe que vous avez entré dans la zone **Password**.	Yes
Numéro de port	Numéro de port où le plug-in de gestion RabbitMQ est activé. Utilisez le numéro de port par défaut 15672 ou spécifiez un autre numéro de port.	Non
Répertoire de base Java	Chemin où le plug-in Java est installé. Utilisez le chemin d'accès par défaut `C:\Program Files\IBM\Java50` ou le répertoire où est installé le plug-in Java.	Non
Niveau de trace Java	Niveau de trace du fournisseur Java. Les valeurs de niveau de trace valides sont les suivantes : • OFF • ERROR • WARN • INFO • DEBUG_MAX • ALL	Non

Configuration de la surveillance des temps de réponse

L'agent Response Time Monitoring surveille les transactions HTTP et HTTPS sur votre serveur HTTP. Les transactions réelles des utilisateurs sur le navigateur (temps du navigateur) sont également surveillées.

L'agent Response Time Monitoring peut être utilisé pour visualiser les niveaux suivants d'informations de surveillance :

Surveillance des transactions HTTP et HTTPS
La surveillance des transactions HTTP est automatiquement disponible lorsque vous installez l'agent Response Time Monitoring.

Selon le type de serveur HTTP que vous surveillez, la surveillance des transactions HTTPS peut être disponible automatiquement ou elle peut nécessiter une configuration manuelle. Pour plus d'informations, voir «Response Time Monitoring Composants», à la page 706.

L'agent Response Time Monitoring surveille également les données relatives aux nombres d'utilisateurs, aux nombres de sessions et aux périphériques.

Les données sont présentées sur le tableau de bord Transactions utilisateur final à l'heure locale de l'utilisateur, et elles sont également utilisées dans le widget Demandes et temps de réponse.

Surveillance des transactions réelles des utilisateurs (temps du navigateur)

Selon le type de serveur HTTP que vous surveillez, les temps du navigateur peuvent être disponibles automatiquement ou il peut être nécessaire de les configurer. Pour plus d'informations, voir «Response Time Monitoring Composants», à la page 706.

Les temps du navigateur sont rendus possibles grâce à JavaScript Injection.

JavaScript Injection vous permet d'afficher davantage de widgets et de détails dans les tableaux de bord Transactions utilisateur final. JavaScript Injection veille à ce que le temps de réponse réel de l'utilisateur final soit collecté à partir du navigateur. Il surveille les performances des pages HTTP et des objets imbriqués pour les pages Web servies par le serveur HTTP. Les détails supplémentaires suivants relatifs aux transactions réelles des utilisateurs finaux sont disponibles :

- Le Temps total client dans le widget Demandes et temps de réponse des transactions
- Le Temps de réponse pour les transactions Temps client dans le widget Transactions - 10 premières
- Répartition des temps de rendu

Pour plus d'informations sur la façon de configurer JavaScript injection, voir «Injection JavaScript», à la page 709

Affichage des tableaux de bord de transactions

Affichez les données de transaction dans le Tableau de bord d'Application Performance.

Un certain nombre de widgets sont disponibles dans le Tableau de bord d'Application Performance et fournissent des détails contextuels sur les transactions.

Les *demandes correctes* ont un temps de réponse inférieur à 10 secondes. Les *demandes lentes* ont un temps de réponse supérieur à 10 secondes. La valeur de 10 secondes utilisée pour déterminer si le temps de réponse est correct ou lent n'est pas configurable. Les widgets suivants sont disponibles :

- Widget de groupe Les pires utilisateurs - 5 premiers
- Widget de groupe Les pires appareils - 5 premiers
- Widget de groupe Demandes et temps de réponse
- Widget de groupe Transactions - 10 premières
- Widget de groupe Demandes et temps de réponse des transactions
- Widget de groupe S'exécute sur
- Widget de groupe Sous-transactions
- Widget de groupe Instances de transaction
- Widget de groupe Utilisateurs par emplacement
- Widget de groupe Utilisateurs à l'emplacement sélectionné
- Widget de groupe Sessions utilisateur à l'emplacement sélectionné - 10 premières
- Widget de groupe Demandes et temps de réponse d'utilisateur
- Widget de groupe Sessions utilisateur - 10 premières
- Widget de groupe Demandes et temps de réponse d'unité
- Widget de groupe Session

- Widget de groupe Demandes de session
- Widget de groupe Instances de session
- Widget de groupe Instances de transaction
- Tableau de bord Récapitulatif des transactions de middleware
- Tableau de bord Détails des transactions de middleware
- Seuils d'événement pour la surveillance des transactions
- Données d'agrégation d'interaction
- Données d'agrégation de transactions
- Statut de la transaction WRT

Response Time Monitoring Composants

Les fonctionnalités de base de l'agent Response Time Monitoring sont les suivantes :

- surveillance des transactions HTTP
- surveillance des transactions HTTPS
- Surveillance des temps du navigateur (à l'aide de JavaScript Injection)

Pour voir des descriptions plus détaillées de ces fonctionnalités, voir «Configuration de la surveillance des temps de réponse», à la page 704.

Selon le type de serveur HTTP que vous surveillez, la fonctionnalité de base de l'agent Response Time Monitoring est assurée par l'utilisation de l'un des composants suivants :

module IBM HTTP Server Response Time
Le module IBM HTTP Server Response Time peut surveiller uniquement le contenu http de type : text/html, application/xml ou application/json. (sans injection Javascript)

Actuellement, le module IBM HTTP Server Response Time ne peut pas surveiller les demandes compressées de l'instrument javascript.

Actuellement, le module IBM HTTP Server Response Time d'injection Javascript peut surveiller uniquement le contenu http de type text/html.

Analyseur de paquets
L'Analyseur de paquets peut surveiller uniquement le contenu de type text/html, ainsi que les demandes compressées gzip.

Si vous surveillez un serveur IBM HTTP Server ou Apache HTTP Server sous AIX ou Linux, utilisez le module IBM HTTP Server Response Time. L'Analyseur de paquets peut être utilisé mais cela est déconseillé. Le module IBM HTTP Server Response Time n'est pas pris en charge sous Windows. Utilisez l'Analyseur de paquets dans un environnement Windows.

Si vous surveillez un autre serveur HTTP, utilisez l'Analyseur de paquets. Analyseur de paquets est pris en charge sous Windows, Linux et AIX.

Planification de l'installation

Planifiez votre installation de l'agent Response Time Monitoring en fonction de votre système d'exploitation et du type de serveur HTTP.

La fonctionnalité de base de l'agent Response Time Monitoring peut être assurée par l'utilisation de l'un des composants suivants :

- Analyseur de paquets
- module IBM HTTP Server Response Time

Vous déterminez quel composant utiliser en fonction des considérations suivantes :

- Le type de serveur HTTP sur lequel vous installez l'agent Response Time Monitoring.
- Le système d'exploitation sur lequel le serveur HTTP est installé.

Les éléments à prendre en considération pour l'installation de l'agent Response Time Monitoring avec le Analyseur de paquets sont les suivants :

- Analyseur de paquets est pris en charge sur tous les systèmes d'exploitation (Windows, Linux et AIX).
- Analyseur de paquets surveille les transactions HTTP sur le port 80 pour tous les systèmes d'exploitation.
- La surveillance des transaction HTTPS n'est pas automatique et doit être configurée manuellement. L'agent Response Time Monitoring a besoin d'accéder aux certificats SSL pour pouvoir déchiffrer le trafic SSL provenant des serveurs HTTP. Pour plus d'informations, voir «Surveillance des transactions HTTPS», à la page 726.
- Analyseur de paquets est pris en charge sur tous les serveurs HTTP, mais il est seulement recommandé pour Sun Java System Web Server et Microsoft Internet Information Services.
- AIX Linux Windows Pour installer l'agent Response Time Monitoring de sorte qu'il fonctionne avec l'Analyseur de paquets sur IBM HTTP Server ou Apache HTTP Server, il convient d'arrêter le serveur HTTP. Lorsque vous installez l'agent Response Time Monitoring et que le serveur HTTP est arrêté, Analyseur de paquets est automatiquement activé.
- AIX Linux Windows Bien que l'Analyseur de paquets puisse être configuré pour IBM HTTP Server ou Apache HTTP Server, il n'est pas conseillé de l'utiliser ; l'usage du module IBM HTTP Server Response Time est recommandé.
- Windows WinPcap 4.1.3 est requis préalablement à l'installation de l'agent Response Time Monitoring.
- Windows AIX Linux Si vous installez l'agent Response Time Monitoring sur Sun Java System Web Server ou Microsoft Internet Information Services, l'Analyseur de paquets est configuré automatiquement.

Les éléments à prendre en considération pour l'installation de l'agent Response Time Monitoring avec le module IBM HTTP Server Response Time sont les suivants :

- Le module IBM HTTP Server Response Time est un composant de l'agent HTTP Server. Vous devez installer l'agent HTTP Server soit avant l'agent Response Time Monitoring, soit en même temps. Pour plus d'informations, voir «module IBM HTTP Server Response Time», à la page 715.
- module IBM HTTP Server Response Time est pris en charge sur tous les systèmes d'exploitation (Windows, Linux et AIX). Le module IBM HTTP Server Response Time prend en charge IBM HTTP Server version 7, 8 et 9.
- Installez l'agent Response Time Monitoring et l'agent HTTP Server sur la même machine.
- Le module IBM HTTP Server Response Time surveille les demandes HTTP et HTTPS sur tous les ports sous AIX, Linux et Windows.
- Le module IBM HTTP Server Response Time est seulement pris en charge pour IBM HTTP Server ou Apache HTTP Server.
- Les deux agents démarrent automatiquement, mais vous devez redémarrer le serveur HTTP.

Le tableau suivant décrit les différentes combinaisons pour configurer automatiquement l'agent Response Time Monitoring.

Tableau 196. Scénarios pour la configuration automatique de l'agent Response Time Monitoring

Combinaisons de serveur HTTP et de système d'exploitation	**Analyseur de paquets**	**module IBM HTTP Server Response Time**
Sun Java System Web Server ou Microsoft Internet Information Services sous AIX ou Linux	Automatique	Non pris en charge

Tableau 196. Scénarios pour la configuration automatique de l'agent Response Time Monitoring (suite)		
Combinaisons de serveur HTTP et de système d'exploitation	**Analyseur de paquets**	**module IBM HTTP Server Response Time**
Sun Java System Web Server ou Microsoft Internet Information Services sous Windows	Automatique	Non pris en charge
IBM HTTP Server ou Apache HTTP Server sous AIX, Linux ou Windows	Automatique si le serveur HTTP est arrêté.	Automatique si le serveur HTTP est présent et configuré

Planification de la configuration

La surveillance HTTP est activée automatiquement lorsque vous installez l'agent Response Time Monitoring. Selon votre environnement, il peut être nécessaire de configurer HTTPS et JavaScript Injection manuellement.

Surveillance du protocole HTTP

La surveillance des transactions HTTP est configurée automatiquement pour Analyseur de paquets et pour le module IBM HTTP Server Response Time, si vous suivez les instructions d'installation. Voir «Planification de l'installation », à la page 706.

Surveillance du protocole HTTPS

La surveillance des transactions HTTPS est configurée automatiquement pour le module IBM HTTP Server Response Time si vous suivez les instructions d'installation. Voir «Planification de l'installation », à la page 706.

La surveillance des transactions HTTPS doit être configurée manuellement pour Analyseur de paquets. Pour plus d'informations, voir « Organigramme de l'Analyseur de paquets», à la page 724.

Temps du navigateur (à l'aide de JavaScript Injection)

Les temps du navigateur (à l'aide de JavaScript Injection) sont configurés automatiquement pour le module IBM HTTP Server Response Time.

Les temps du navigateur (à l'aide de JavaScript Injection) doivent être configurés manuellement pour Analyseur de paquets. Pour plus d'informations, voir « Organigramme de l'Analyseur de paquets», à la page 724.

Le tableau suivant décrit la façon dont la fonctionnalité de base est configurée pour chaque composant :

Tableau 197. Configuration de la fonctionnalité de base		
	Analyseur de paquets sur Sun Java System Web Server ou Microsoft Internet Information Services (Windows, Linux ou AIX)	**module IBM HTTP Server Response Time sur IBM HTTP Server ou Apache HTTP Server (Windows, Linux ou AIX)**
Surveillance des transactions HTTP	Activée automatiquement.	Activée automatiquement
Surveillance des transactions HTTPS	Doit être configurée manuellement.	Activée automatiquement
Surveillance des transactions réelles des utilisateurs (temps du navigateur) à l'aide de JavaScript Instrumentation	Doit être configurée manuellement.	Activée automatiquement

Injection JavaScript

Vous pouvez personnaliser les données collectées par l'agent Response Time Monitoring pour l'affichage dans les tableaux de bord Transactions utilisateur final.

Pour assurer un bon acquis utilisateur pour une application Web, vous devez surveiller les performances telles qu'elles sont perçues par les utilisateurs réels. Cela implique une surveillance au niveau du navigateur.

Pour pouvoir surveiller au niveau du navigateur, vous devez injecter du code de surveillance JavaScript dans les pages que vous voulez surveiller. Ce code collecte alors des données pour des temps de navigateur spécifiques.

Cela est possible grâce à l'injection JavaScript dans les pages Web et les objets que vous souhaitez surveiller. Selon le type de serveur HTTP sur lequel vous avez installé votre agent Response Time Monitoring, il existe deux méthodes que vous pouvez utiliser pour collecter des informations sur le temps de réponse moyen des transactions pour l'utilisateur final réel.

- Si vous utilisez un serveur IBM HTTP Server ou Apache HTTP Server, utilisez le module IBM HTTP Server Response Time. Le module IBM HTTP Server Response Time effectue automatiquement l'injection JavaScript. Le module IBM HTTP Server Response Time est un composant de l'agent HTTP Server. Il est installé et configuré en tant qu'élément de l'agent HTTP Server. Pour plus d'informations, voir «module IBM HTTP Server Response Time», à la page 715.
- Si vous utilisez n'importe quel autre serveur HTTP pris en charge, utilisez Analyseur de paquets. Avec Analyseur de paquets, vous devez instrumenter manuellement vos pages Web pour la collecte des temps du navigateur. Pour plus d'informations, voir «Ajout du composant de surveillance JavaScript à votre application», à la page 724.

Le tableau suivant indique les fonctions qui sont disponibles dans le Tableau de bord d'Application Performance si vous configurez votre environnement pour Analyseur de paquets ou pour le module IBM HTTP Server Response Time :

	Analyseur de paquets	**module IBM HTTP Server Response Time**
10 premières transactions	✓	✓
Temps serveur	✓	✓
Répartition des temps de rendu	—	✓
Sous-transactions AJAX	✓	✓
Données de temporisation des ressources dans la table Sous-transactions	—	✓
Instances de transaction (10 premières)	✓	✓
Topologie des instances de transaction	✓	✓
Topologie d'application	✓	✓
Instrumentation automatique de l'injection de JavaScript	N/A	✓

Reconfiguration de la Response Time Monitoring sous Windows

Utilisez la commande de configuration interactive `rt-agent` ou l'utilitaire IBM Cloud Application Performance Management pour configurer ou reconfigurer l'agent.

Avant de commencer

Si vous activez la surveillance des transactions HTTPS, vérifiez que Monitoring Agent for HTTP Server n'est pas installé sur la même machine. Dans le cas contraire, le paramètre HTTPS de l'Analyseur de paquets n'est pas modifié dans la configuration de Response Time Monitoring.

Pourquoi et quand exécuter cette tâche

L'agent de Response Time Monitoring est configuré automatiquement après l'installation. Suivez les instructions d'installation : «Planification de l'installation », à la page 706. Vous pouvez être amené à effectuer une reconfiguration pour pouvoir surveiller un port différent ou les transactions HTTPS, par exemple.

Le répertoire d'installation est *rép_install*. Le chemin d'accès au répertoire d'installation par défaut est : `C:\IBM\APM\`

Outre l'utilisation de la commande de configuration interactive `rt-agent`, vous pouvez configurer l'agent dans l'utilitaire IBM Cloud Application Performance Management. Pour plus d'informations, voir «Utilisation de la fenêtre IBM Cloud Application Performance Management sur les systèmes Windows», à la page 186.

Procédure

Pour personnaliser vos paramètres de données, procédez comme suit :

1. Sur l'ordinateur sur lequel l'agent Response Time Monitoring est installé, arrêtez l'agent :
   rép_install`\BIN\rt-agent.bat stop`
2. Utilisez la configuration silencieuse pour configurer l'agent :

   ```
   rép_install\BIN\rt-agent.bat config rép_install\samples\rt_silent_config.txt
   ```

   Si vous souhaitez activer la surveillance des transactions HTTPS, supprimez la mise en commentaire des lignes suivantes dans le fichier de configuration en mode silencieux. L'exemple de fichier `rt_silent_config.txt` permettant de configurer l'agent Response Time Monitoring de sorte qu'il surveille HTTPS sous Windows doit être similaire à celui-ci :

   ```
   # Monitor HTTPS transactions
   KT5MONITORHTTPSAPP=YES

   # HTTPS keystore (e.g. - /tmp/keys.kdb)
   KT5KEYSTORE=C:\keys\key.kdb

   # HTTPS server certificate map (eg - certAlias,9.48.152.1,443;...)
   KT5SERVERMAP=certalias,9.48.152.1,443

   # Monitor network traffic for the NIC hosts this IP address
   #KT5MONITORIP=9.48.152.1
   ```

3. Redémarrez l'agent Response Time Monitoring pour que les modifications soient prises en compte :
   rép_install`\BIN\rt-agent.bat start`

Résultats

Les données de la nouvelle source sont affichées dans les tableaux de bord associés à Response Time Monitoring.

Reconfiguration de la Response Time Monitoring sur AIX et Linux

Utilisez la commande de configuration `rt-agent` pour configurer ou reconfigurer l'agent de Response Time Monitoring.

Pourquoi et quand exécuter cette tâche

L'agent de Response Time Monitoring est configuré automatiquement après l'installation. Suivez les instructions d'installation : «Planification de l'installation », à la page 706. Il se peut que vous deviez effectuer une reconfiguration,par exemple si vous voulez surveiller un port différent.

Le répertoire d'installation est appelé *rép_install*. Le répertoire d'installation par défaut est : `/opt/ibm/apm/agent`.

Utilisez le même utilisateur root que celui que vous avez utilisé pour démarrer, arrêter et configurer l'agent.

Procédure

Pour effectuer une reconfiguration, procédez comme suit :

1. Sur l'ordinateur sur lequel l'agent Response Time Monitoring est installé, arrêtez l'agent :

   ```
   rép_install/bin/rt-agent.sh stop
   ```

2. Utiliser une configuration en mode silencieux ou interactive :

   a) Configuration interactive :

   ```
   rép_install/bin/rt-agent.sh config
   ```

   b) Configuration en mode silencieux :

   ```
   rép_install/bin/rt-agent.sh config  rép_install/samples/rt_silent_config.txt
   ```

   Si vous souhaitez activer la surveillance des transactions HTTPS, supprimez la mise en commentaire des lignes suivantes dans le fichier de configuration en mode silencieux. L'exemple de fichier `rt_silent_config.txt` permettant de configurer l'agent Response Time Monitoring de sorte qu'il surveille HTTPS sous AIX et Linux doit être similaire à celui-ci :

   ```
   # Monitor HTTPS transactions
   KT5MONITORHTTPSAPP=YES

   # HTTPS keystore (e.g. - /tmp/keys.kdb)
   KT5KEYSTORE=/tmp/keys.kdb

   # HTTPS server certificate map (eg - certAlias,9.48.152.1,443;...)
   KT5SERVERMAP=certalias,9.48.152.1,443

   # Monitor network traffic for the NIC hosts this IP address
   #KT5MONITORIP=9.48.152.1
   ```

3. Redémarrez l'agent Response Time Monitoring pour que les modifications soient prises en compte :
   rép_install`/bin/rt-agent.sh start`

Résultats

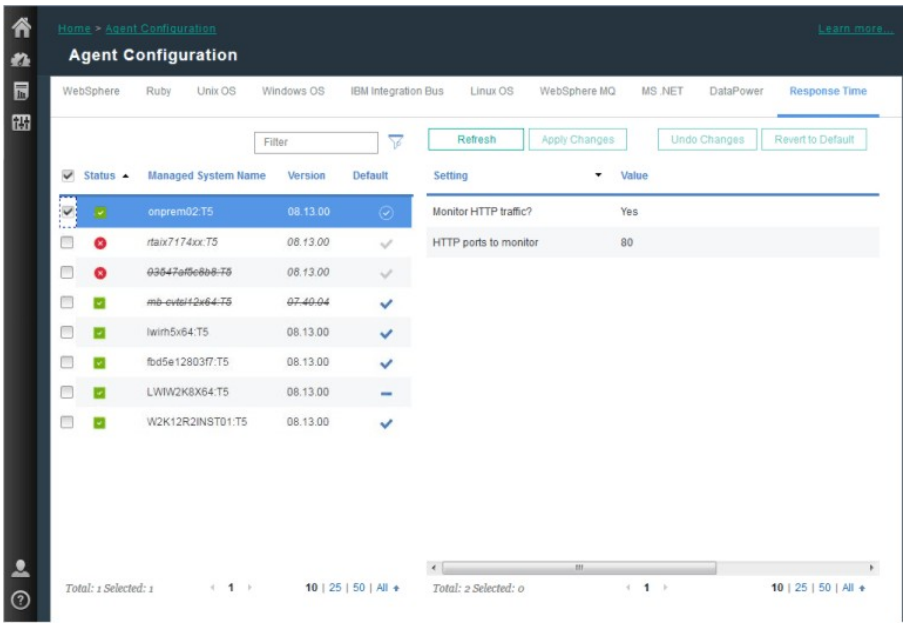
Les données de la nouvelle source sont affichées dans les tableaux de bord associés à Response Time Monitoring.

Configuration à l'aide de la page Configuration d'agent

Vous pouvez utiliser la page **Configuration d'agent** dans la console Cloud APM pour voir quels agents sont installés. Vous pouvez, le cas échéant, désactiver ou activer la surveillance des transactions HTTP et définir les ports surveillés par les agents Response Time Monitoring.

Configuration d'agent

Pour accéder à la page Response Time Monitoring **Configuration d'agent** dans la console Cloud APM, sélectionnez **Configuration du système** > **Configuration d'agent**, puis l'onglet **Temps de réponse**.



La page **Configuration d'agent** répertorie les systèmes de votre environnement sur lesquels Response Time Monitoring est installé.

Pour chaque système où un agent Response Time Monitoring est installé, la page **Configuration d'agent** indique :

- Si le système est en ligne (coche sur fond vert) ou hors ligne (croix sur fond rouge).
- La version de l'agent Response Time Monitoring qui est installée.
- Si la configuration centrale ne parvient pas à déterminer le type de l'agent (c'est-à-dire si l'Analyseur de paquets ou le module IBM HTTP Server Response Time est utilisé pour surveiller des transactions HTTP), seul l'agent est rayé. En général, le type d'agent ne peut pas être déterminé lorsque l'agent n'envoie pas les détails associés via l'activité ASF.
- Si le système utilise les valeurs de configuration par défaut ou si des valeurs personnalisées sont définies.
- Les ports surveillés si l'agent Response Time Monitoring utilise l'Analyseur de paquets pour surveiller des transactions HTTP.

Setting	Value
Monitor HTTP traffic?	Yes
HTTP ports to monitor	80

- Si le module IBM HTTP Server Response Time, associé à l'agent HTTP Server, est utilisé pour surveiller les transactions HTTP.

Setting	Value
Is IBM HTTP Server Response Time module enabled?	Yes

Conseil : Le module IBM HTTP Server Response Time surveille automatiquement les transactions HTTP et HTTPS. Aucune configuration supplémentaire de l'agent Response Time Monitoring n'est obligatoire.

Sélectionnez un système pour afficher ses paramètres de configuration. Pour trouver un système spécifique, entrez son nom partiellement ou en entier dans la zone **Filter**.

Les personnalisations apportées à la page **Configuration d'agent** ont priorité sur les autres personnalisations et sur les valeurs par défaut.

Si vous changez d'avis concernant les paramètres modifiés, cliquez sur **Undo Changes** pour revenir aux paramètres dernièrement enregistrés ou sur **Revert to Default** pour revenir aux valeurs par défaut.

Les nouvelles valeurs de configuration sont envoyées au composant Central Configuration Services et les agents en ligne sont alors automatiquement reconfigurés sans avoir à être redémarrés. Si l'agent est hors ligne, il télécharge les nouveaux paramètres de configuration lorsqu'il devient en ligne. Les données des nouveaux ports sont affichées dans les tableaux de bord associés à Response Time Monitoring lorsque les données sont actualisées.

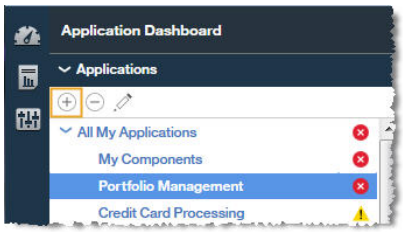
Ajout d'applications

Une fois que vous avez installé l'agent Response Time Monitoring, il se peut que vous deviez ajouter les applications à surveiller au Tableau de bord d'Application Performance .

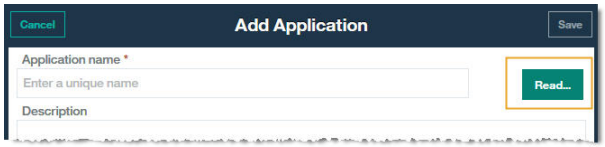
Procédure

Pour ajouter des applications au Tableau de bord d'Application Performance :

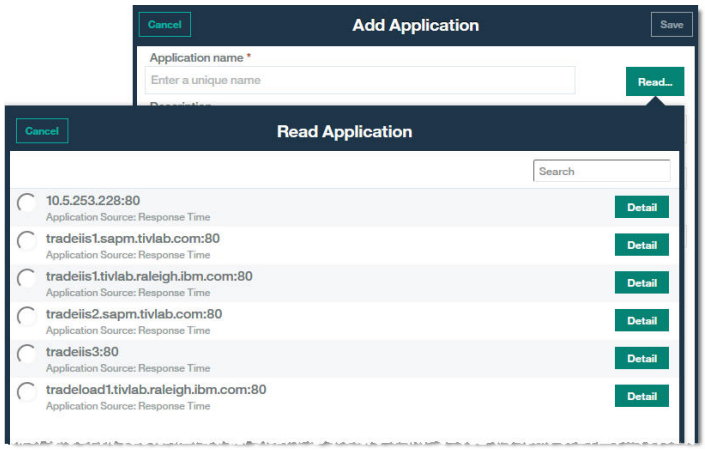
1. Dans le Tableau de bord d'Application Performance , cliquez sur **Ajouter une application**.



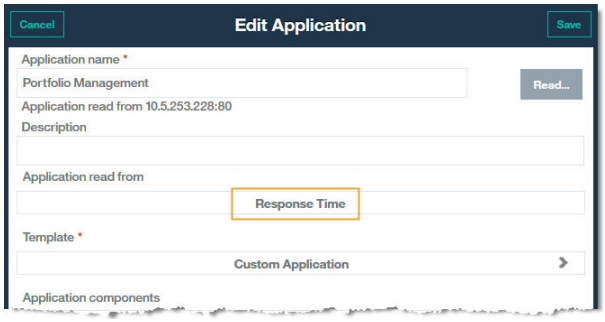
2. Sélectionnez **Lire** pour ouvrir la liste des applications reconnues.



3. Sélectionnez l'application à surveiller.



Temps de réponse s'affiche en tant que référentiel source dans la zone **Application lue dans** et les composants sont répertoriés dans **Composants d'application**.



4. Aucune configuration supplémentaire n'est requise pour afficher les applications surveillées par l'agent Response Time Monitoring dans le Tableau de bord d'Application Performance . Cliquez sur **Sauvegarder** dans la fenêtre **Ajouter une application**.

Résultats

Les applications détectées par l'agent Response Time Monitoring sont répertoriées dans **Toutes mes applications**, dans le Tableau de bord d'Application Performance .

Configuration de l'module IBM HTTP Server Response Time

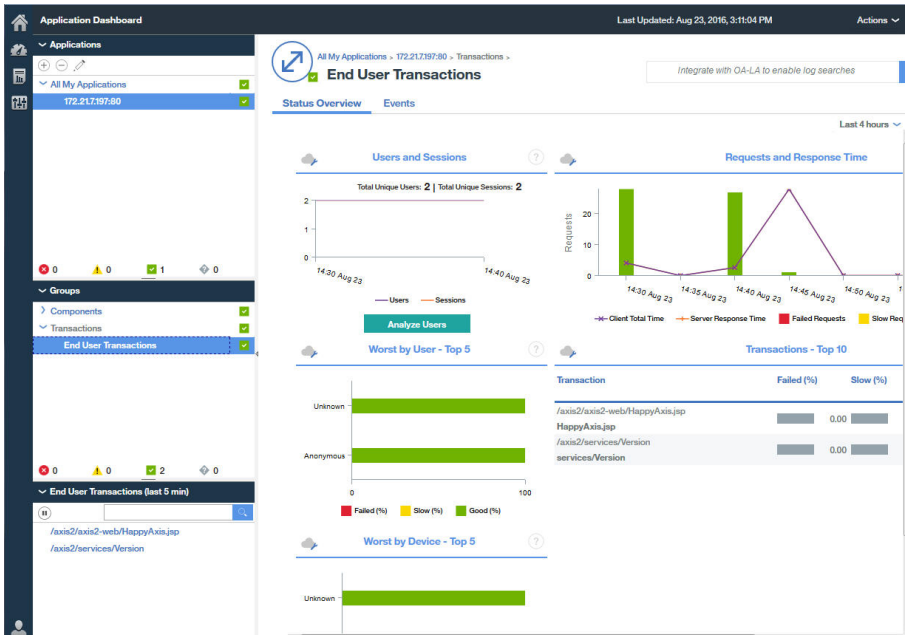
Pour IBM HTTP Server et Apache HTTP Server, utilisez le module IBM HTTP Server Response Time pour afficher les indicateurs réels de surveillance de temps de réponse de l'utilisateur final pour les pages HTTP.

Le module IBM HTTP Server Response Time est installé et configuré en tant qu'élément du agent HTTP Server. Le module IBM HTTP Server Response Time ne fonctionne qu'avec IBM HTTP Server et Apache HTTP Server sous AIX, Linux et Windows. Le module IBM HTTP Server Response Time surveille tous les ports pour les requêtes HTTP et HTTPS.

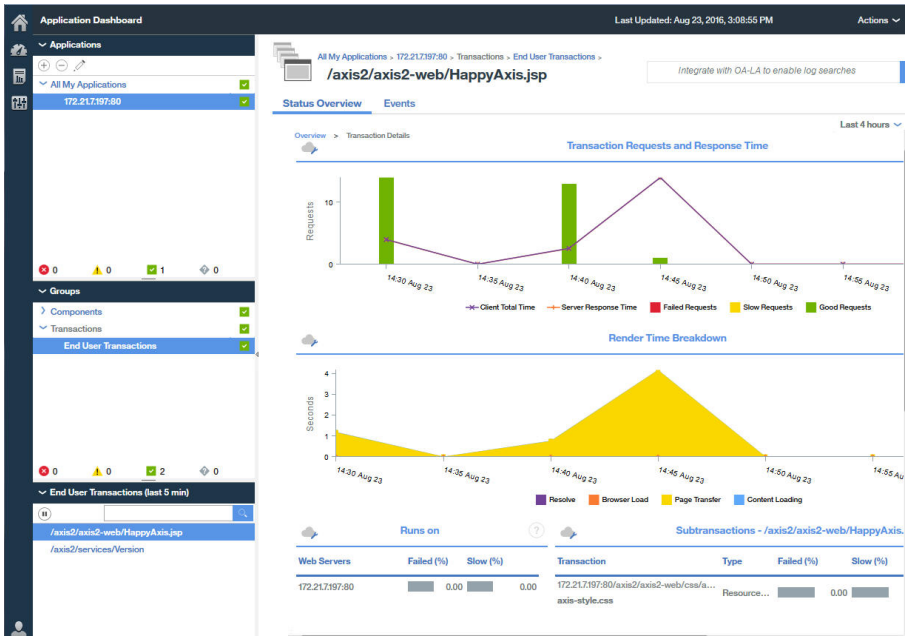
A l'aide de JavaScript, le module IBM HTTP Server Response Time insère un en-tête dans les pages Web transmises par IBM HTTP Server pour que l'agent de Response Time Monitoring puisse surveiller ces pages. Les objets imbriqués chargés par la page sont suivis à l'aide de cookies. Les informations de transaction des pages Web transmises par IBM HTTP Server ou Apache sont ensuite incluses dans les tableaux de bord Transactions utilisateur final.

Par exemple :

Espace de travail Transactions utilisateur final présentant les données collectées à partir du module IBM HTTP Server Response Time dans la section Transactions - 10 premières :



Espace de travail Transactions utilisateur final présentant les données collectées à partir du module IBM HTTP Server Response Time dans le tableau **Sous-transactions**



module IBM HTTP Server Response Time

Le module IBM HTTP Server Response Time fait partie de l'agent HTTP Server. Mais il fonctionne conjointement avec l'agent Response Time Monitoring pour surveiller les transactions d'application sur les serveurs HTTP pris en charge.

Lorsque vous installez l'agent Response Time Monitoring pour qu'il fonctionne avec le module IBM HTTP Server Response Time, il surveille les demandes HTTP et HTTPS sur tous les ports.

Le module IBM HTTP Server Response Time fait partie de l'agent HTTP Server. Vous devez installer l'agent HTTP Server soit avant l'agent Response Time Monitoring, soit en même temps.

L'agent HTTP Server est composé de deux plug-in :

1. `khu_module` - correspond au agent HTTP Server. Ce plug-in est responsable de tous les tableaux de bord associés à l'agent HTTP Server. Pour plus d'informations, voir agent HTTP Server Reference.
2. `wrt_module` - correspond au module IBM HTTP Server Response Time.

Ces deux plug-in sont indiqués dans le fichier de configuration de l'agent HTTP Server. Le fichier de configuration de l'agent HTTP Server est comme suit pour le serveur Apache HTTP Server :

```
khu.usr.local.apache24.conf.httpd.conf
```

Le fichier est comme suit pour le serveur IBM HTTP Server :

```
khu.opt.IBM.HTTPServer.conf.httpd.conf
```

La règle de nommage de ce fichier est : `khu.(chemin d'accès complet du fichier de conf du serveur http, remplacer le / par .).conf`

```
LoadModule khu_module

LoadModule wrt_module
```

Pour que le module IBM HTTP Server Response Time fonctionne, le fichier de configuration du serveur HTTP doit contenir une instructions include faisant référence au fichier de configuration du agent HTTP Server. Par exemple :

```
include /opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf
```

Cette instruction include active les deux plug-in en même temps. Pour plus d'informations, voir «Configuration de la surveillance de HTTP Server», à la page 275.

Installation et configuration du module IBM HTTP Server Response Time
La configuration est automatique du côté de l'agent Response Time Monitoring. Le module IBM HTTP Server Response Time doit être installé et configuré en tant qu'élément de l'agent HTTP Server. L'agent Response Time Monitoring détecte automatiquement le module IBM HTTP Server Response Time et l'active.

Pourquoi et quand exécuter cette tâche

Procédure

1. Installez l'agent HTTP Server qui installe automatiquement le module IBM HTTP Server Response Time.
2. Configurez l'agent HTTP Server. Cette opération active le module IBM HTTP Server Response Time. Pour plus d'informations, voir «Configuration de la surveillance de HTTP Server», à la page 275.
3. Installez l'Agent de surveillance des temps de réponse en tant que `superutilisateur` ou `Administrateur`, en fonction de votre système d'exploitation. Pour des instructions détaillées, voir Chapitre 6, «Installation des agents», à la page 123.
4. Redémarrez IBM HTTP Server. Lorsque le programme d'installation de Response Time Monitoring détecte l'agent HTTP Server, l'agent Response Time Monitoring active le module IBM HTTP Server Response Time automatiquement.

Activation manuelle du module IBM HTTP Server Response Time
Vous pouvez activer le module IBM HTTP Server Response Time manuellement afin de surveiller les performances des pages HTTP et des objets imbriqués des pages Web servies par IBM HTTP Server :

Pourquoi et quand exécuter cette tâche
Le module IBM HTTP Server Response Time est activé automatiquement lorsque l'eagent HTTP Server est installé et configuré. Toutefois, vous souhaiterez sans doute activer le module IBM HTTP Server Response Time manuellement.

Procédure

Pour activer le module IBM HTTP Server Response Time manuellement sous Linux, AIX ou Windows, procédez comme suit :

1. Linux AIX
   Pour activer le module IBM HTTP Server Response Time manuellement sous Linux ou AIX, procédez comme suit :
   a) Arrêtez l'agent Response Time Monitoring.
      Exécutez
      ```
      $AGENT_HOME/bin/rt-agent.sh stop
      ```
      où *$AGENT_HOME* peut correspondre à `/opt/ibm/apm/agent` sur un système Linux, ou à `/opt/ibm/ccm/agent` sur un système AIX.
   b) Exécutez une commande de configuration et utilisez *$AGENT_HOME*`/samples/rt_silent_config_ihs.txt` pour ajouter les modules de chargement au fichier de

configuration de serveur Web et définissez les paramètres de configuration pour le module IBM HTTP Server Response Time.

c) Redémarrez l'agent Response Time Monitoring.

2. Windows

Pour activer le module IBM HTTP Server Response Time manuellement sous Windows, procédez comme suit :

a) Arrêtez l'agent Response Time Monitoring.

Exécutez

```
REP_BASE_AGENT/bin/rt-agent.bat stop
```

où *REP_BASE_AGENT* peut correspondre à `C:\IBM\APM` sur un système Windows.

b) Exécutez une commande de configuration et utilisez *REP_BASE_AGENT*`\samples\rt_silent_config_ihs.txt` pour ajouter les modules de chargement au fichier de configuration de serveur Web et définissez les paramètres de configuration pour le module IBM HTTP Server Response Time.

Par exemple,

```
REP_BASE_AGENT\bin\rt_agent.bat config REP_BASE_AGENT\samples\rt_silent_config_ihs.txt
```

c) Redémarrez l'agent Response Time Monitoring.

Désactivation manuelle du module IBM HTTP Server Response Time

Pour désactiver le module IBM HTTP Server Response Time et réutiliser l'Analyseur de paquets, reconfigurez l'agent et désactivez la surveillance du module IBM HTTP Server Response Time.

Pourquoi et quand exécuter cette tâche

Utilisez les procédures suivantes pour désactiver le module IBM HTTP Server Response Time.

Procédure

Pour reconfigurer l'agent en mode interactif sous Linux, AIX ou Windows, procédez comme suit :

1. Linux AIX

Pour reconfigurer l'agent en mode interactif sous Linux et AIX, procédez comme suit :

a) Exécutez *rép_install*`/bin/rt-agent.sh config`

Où *rép_install* correspond à `/opt/ibm/apm/agent` sous Linux et AIX.

b) Redémarrez l'agent Response Time Monitoring.

Sinon, pour définir les paramètres manuellement :

a) Ouvrez *rép_install*`/config/`*nom_hôte*`_t5.cfg` dans un éditeur de texte.

où *rép_install* correspond à `/opt/ibm/apm/agent` sous Linux et AIX.

b) Définissez les paramètres suivants :

```
KT5DISABLEANALYZER=NO
KT5ENABLEWEBPLUGIN=NO
```

c) Redémarrez l'agent Response Time Monitoring.

2. Windows

Pour reconfigurer l'agent en mode interactif sous Windows, procédez comme suit :

a) Pour définir manuellement les paramètres connexes, ouvrez le fichier *rép_install*`\TMAITM6_x64\`*nomhôte*`_t5.cfg` dans un éditeur de texte.

où *rép_install* correspond à `C:\IBM\APM` sous Windows.

b) Définissez les paramètres suivants :

```
KT5DISABLEANALYZER=NO
KT5ENABLEWEBPLUGIN=NO
```

c) Redémarrez l'agent Response Time Monitoring.

Configuration avancée du module IBM HTTP Server Response Time
Il existe un certain nombre d'options de configuration avancées pour le module IBM HTTP Server Response Time.

Le module IBM HTTP Server Response Time est configuré automatiquement, mais il existe certaines tâches de configuration avancées que vous pouvez effectuer pour affiner les performances et les fonctionnalités.

Désactivation de la surveillance de la temporisation des ressources
La surveillance de la temporisation des ressources est activée pour toutes les instances du module IBM HTTP Server Response Time installées par l'agent HTTP Server.

Pourquoi et quand exécuter cette tâche

Pour réduire le nombre de ressources surveillées par le module IBM HTTP Server Response Time ou pour désactiver la surveillance de la temporisation des ressources afin de réduire la charge de traitement requise pour surveiller une instance spécifique de l'IBM HTTP Server, procédez comme suit :

Procédure

Pour modifier le fichier de configuration de l'agent HTTP Server, procédez comme suit :

1. A la fin du fichier de configuration du serveur HTTP (httpd.conf), ajoutez :

   ```
   WrtMaxPostResourcesSize
   ```

2. Définissez l'une des valeurs suivantes :
   - `WrtMaxPostResourcesSize -1` pour surveiller toutes les ressources.
   - `WrtMaxPostResourcesSize 0` pour désactiver la surveillance des ressources.
   - `WrtMaxPostResourcesSize` *n* pour surveiller un nombre de ressources spécifique, `10` par défaut. Par exemple, définissez `WrtMaxPostResourcesSize 2` pour définir deux ressources au maximum à envoyer au serveur.
3. Redémarrez le serveur HTTP.

Désactivation de la génération de corrélateur ARM
Par défaut, la génération de corrélateur ARM Correlator est activée, ce qui permet au module IBM HTTP Server Response Time de se connecter à tous les serveurs d'arrière-plan de la topologie. Vous pouvez désactiver la génération de corrélateur ARM Correlator si nécessaire.

Pourquoi et quand exécuter cette tâche

Restriction : Si vous désactivez la génération de corrélateur ARM, le module IBM HTTP Server Response Time ne peut pas établir de liaison avec les serveurs d'arrière-plan, comme WebSphere Application Server. Désactivez-la uniquement sur conseil du service de support logiciel IBM.

Procédure

Pour désactiver la génération de corrélateur ARM, procédez comme suit :

1. A la fin du fichier de configuration du serveur HTTP (httpd.conf), ajoutez :

   ```
   WrtDisableArmCorr
   ```

2. Redémarrez le serveur HTTP.

Désactivation de la Surveillance des temps de réponse avec temps client (instrumentation JavaScript)
Dans IBM Application Performance Management, Surveillance des temps de réponse avec temps client (instrumentation JavaScript) est activé pour toutes les installations de la IBM HTTP Server qui s'exécutent sur tous les ordinateurs.

Pourquoi et quand exécuter cette tâche

Procédure

Pour désactiver l'injection JavaScript manuellement, procédez comme suit :

1. Ouvrez le fichier de configuration du serveur HTTP : *racine_HTTP_Server*/conf/httpd.conf
2. Accédez à la ligne ajoutée pour l'agent HTTP Server et ajoutez la ligne suivante après celle-ci :

   ```
   WrtDisableJSI
   ```

   Par exemple,

   ```
   include /opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf
   WrtDisableJSI
   ```

3. Sauvegardez le fichier httpd.conf et recyclez le serveur HTTP.

Contournement du cookie WRTCorrelator
Si l'injection JavaScript est activée pour l'agent Response Time Monitoring sur WebSphere Portal, les cookies tels que le cookie WRTCorrelator risquent d'être à l'origine de problèmes lors de l'utilisation de WebSphere Portal. Pour éviter ces problèmes, vous pouvez définir le cookie WRTCorrelator sur ignore.

Procédure

1. Si nécessaire, démarrez le serveur WebSphere_Portal.
2. Connectez-vous à WebSphere Integrated Solutions Console.
3. Accédez à **Ressources** > **Environnement de ressources** > **Fournisseurs d'environnement de ressources**.
4. Sélectionnez **WP ConfigService**.
5. Sous Propriétés supplémentaires, sélectionnez **Propriétés personnalisées**.
6. Cliquez sur **Nouveau**.
7. Spécifiez le nom de la propriété (le cookie WRTCorrelator dans le cas présent), puis définissez la valeur de cette propriété sur ignore.

   Pour définir le cookie WRTCorrelator sur ignore, entrez ce qui suit :

   ```
   cookie.ignore.regex =
   digest\.ignore.*|LTPAToken|LTPAToken2|JSESSIONID|WASReqURL|WRTCorrelator
   |PD_STATEFUL.*
   ```

8. Cliquez sur **Appliquer** et sauvegardez vos modifications.
9. Déconnectez-vous de WebSphere Integrated Solutions Console.

Résultats
Le cookie WRTCorrelator est défini sur ignore et les problèmes tels que les conditions de fin de boucle sont évités.

Exclusion de pages de la génération de rapports du temps client

Vous pouvez exclure des pages particulières de la génération de rapports du temps client à partir du navigateur.

Pourquoi et quand exécuter cette tâche

Vous pouvez ajouter un paramètre dans le fichier de configuration pour que le module IBM HTTP Server Response Time arrête d'injecter du code JavaScript dans un fichier qui correspond aux modèles que vous spécifiez. Cela arrête la génération de rapports de temps client à partir du navigateur pour ces pages.

Procédure

Pour exclure des pages particulières de la génération de rapports du temps client à partir du navigateur, procédez comme suit :

1. Ouvrez le fichier suivant dans un éditeur de texte :

   Linux AIX *rép_install*/config/*nom_hôte*_t5.cfg où *rép_install* est /opt/ibm/apm/agent

   Windows *rép_install*\TMAITM6_x64*nom_hôte*_t5.cfg où *rép_install* est C:\IBM\APM
2. Dans la section **advconfig**, ajoutez :

   ```
   {KT5WEBPLUGIN_JSI_EXCLUDE_URI_WITH_PATTERNS=URL_path_pattern to_exclude}
   ```

   Par exemple,

   ```
   {KT5WEBPLUGIN_JSI_EXCLUDE_URI_WITH_PATTERNS=*/DoNotJSIMe.jsp,/absolutePath/index.jsp,/
   skipThisDir/*}
   ```

   Le chemin de l'URL est limité à 256 caractères.

   Conseil : Utilisez un astérisque (*) comme préfixe ou suffixe pour correspondre aux modèles. Ajoutez plusieurs valeurs séparées par une virgule au paramètre si nécessaire.
3. Sauvegardez et fermez le fichier *nom_hôte*_t5.cfg.
4. Redémarrez l'agent Response Time Monitoring :

   ```
   rt-agent.sh stop
   rt-agent.sh start
   ```

Utilisation du module IBM HTTP Server Response Time en tant qu'utilisateur non superutilisateur

En prenant un certain nombre de précautions lors de la configuration, vous pouvez utiliser le module IBM HTTP Server Response Time avec un ID utilisateur autre que l'ID superutilisateur (root). Si vous utilisez Network Analyseur de paquets, notez que vous devez utiliser l'ID root.

Pour utiliser un ID utilisateur autre que l'ID root, procédez comme suit :

Pour l'agent Response Time Monitoring

Installez l'agent Response Time Monitoring dans un répertoire doté d'un accès en écriture, à l'aide de l'ID utilisateur avec lequel vous allez l'exécuter.

- Pour cette procédure, l'ID utilisateur de l'agent Response Time Monitoring est *agentuser*. Le répertoire dans lequel l'agent est installé est *$AGENT_HOME*.
- Si vous installez l'agent Response Time Monitoring en tant qu'utilisateur root et que vous exécutez ensuite l'agent à l'aide d'un autre ID utilisateur, vous ne pourrez pas créer de fichiers.

Pour le module IBM HTTP Server Response Time

ServerRoot doit appartenir au même ID utilisateur que celui utilisé pour exécuter apache start|stop.

- Lors de l'exécution de la commande `apache start`, le répertoire de suivi `wrt` est créé sous `ServerRoot`. L'utilisateur doit disposer de droits suffisants pour créer des fichiers et des répertoires sous `ServerRoot`.
- Si l'utilisateur du module IBM HTTP Server Response Time, *ihsuser*, est différent de l'utilisateur *agentuser*, il requiert un accès en écriture dans `$AGENT_HOME/tmp`.

  `$AGENT_HOME/tmp` est créé lors de l'installation d'agents. L'ID utilisateur *ihsuser* doit être autorisé à créer le répertoire `kt5` dans `$AGENT_HOME/tmp`.
- Il peut y avoir plusieurs versions de `ServerRoot`, chacune administrée par des utilisateurs différents.

Pour l'agent Response Time Monitoring et le module IBM HTTP Server Response Time

Les ID utilisateur *agentuser* et *ihsuser* doivent disposer d'un accès en lecture/écriture dans les répertoires suivants :

- `$AGENT_HOME/tmp/kt5`
- `ServerRoot/wrt`

En général, le module IBM HTTP Server Response Time est démarré en premier et les répertoires `wrt` sont créés automatiquement par Response Time Monitoring lors de son premier démarrage avec des droits en lecture/écriture pour tous.

`ServerRoot/wrt` est également utilisé par `camconfig` pour transmettre la configuration. L'utilisateur *ihsuser* crée des fichiers d'ID de file d'attente partagés qui sont sélectionnés par l'utilisateur *agentuser* ; l'utilisateur *agentuser* lit l'ID de file d'attente dans le répertoire et transmet la configuration.

Si `root` est utilisé pour exécuter initialement `apache start` et que *ihsuser* n'est pas `root`, procédez comme suit :

1. Arrêtez l'agent Response Time Monitoring.
2. En tant qu'utilisateur `root`, exécutez `apachectl stop`.
3. Supprimez les répertoires suivants :
   - `$AGENT_HOME/tmp/kt5`
   - `ServerRoot/wrt`
4. En tant qu'utilisateur *ihsuser*, exécutez `apachectl start` pour recréer les répertoires avec les droits appropriés.

Pour réinitialiser les droits du module IBM HTTP Server Response Time dans le répertoire `wrt`

Vous pouvez réinitialiser les droits du répertoire module IBM HTTP Server Response Time `wrt` pour plus de sécurité. La mise à jour implique l'ajout d'un paramètre dans le fichier de configuration pour limiter les droits d'accès au répertoire `wrt` créé par l'utilisateur non root lors de l'installation de IBM HTTP Server.

Effectuez cette procédure sur le système sur lequel le module IBM HTTP Server Response Time est installé pour modifier les droits du répertoire `wrt` pour l'utilisateur non root de 777 en 700 :

1. Ouvrez le fichier `$IHS_HOME$/conf/httpd.conf` dans un éditeur de texte.
2. Ajoutez la propriété **`WrtDisableDirPermNonRoot`** à la fin du fichier :
   - Si cette propriété est activée, seul l'ID utilisateur ayant démarré httpd et correspondant à l'ID utilisateur ayant créé le répertoire est utilisé pour créer le répertoire `wrt` avec les droits 700. L'accès à ce répertoire est refusé à tous les autres utilisateurs.
   - Si cette propriété n'est pas activée, le répertoire `wrt` est créé avec les droits par défaut 777.
3. Redémarrez l'agent Response Time Monitoring :

```
rt-agent.sh stop
rt-agent.sh.start
```

Les données de configuration Response Time Monitoring et certains fichiers persistants sont stockés dans le répertoire `wrt`, qui est utilisé lors du processus de communication, et chaque processus de connexion y crée un fichier de configuration wrt. Une fois que vous avez ajouté **`WrtDisableDirPermNonRoot`** au fichier `httpd.conf`, seuls certains utilisateurs peuvent communiquer avec l'agent de surveillance Response Time Monitoring.

Utilisation des équilibreurs de charge

Si vous utilisez des équilibreurs de charge dans votre environnement, il est nécessaire de les personnaliser.

Procédure

Si vous utilisez un équilibreur de charge, procédez comme suit :

1. Désactivez la réécriture des URL sur l'équilibreur de charge.
2. Installez un agent Response Time Monitoring sur chaque serveur Web que vous souhaitez surveiller.

   N'installez pas Response Time Monitoring sur l'équilibreur de charge.

Que faire ensuite

Si vous exécutez l'agent Response Time Monitoring derrière un équilibreur de charge, vous pouvez configurer ce dernier afin qu'il achemine l'adresse IP du client pour optimiser les performances de surveillance. Utilisez les étapes suivantes comme exemple :

1. Dans l'en-tête HTTP, définissez l'adresse IP du client dans la zone **`X-Forwarded-For`**.
2. Dans le fichier `$AGENT_HOME/config/`*`nom_hôte`*`_t5.cfg`, ajoutez `{KT5WEBPLUGIN_OVERRIDE_SOURCE_ADDR_HEADERS=X-Forwarded-For}` à la section `SECTION=advconfig`.

   Conseil : Ajoutez plusieurs valeurs au paramètre si nécessaire. Par exemple, `{KT5WEBPLUGIN_OVERRIDE_SOURCE_ADDR_HEADERS=x-forwarded-for, iv-remote-address}`
3. Redémarrez l'agent Response Time Monitoring. Exécutez les commandes suivantes :

```
rt-agent.sh stop
rt-agent.sh start
```

Limitation de l'UC utilisée pour surveiller IBM HTTP Server

Dans des environnements saturés, vous pouvez être amené à limiter le pourcentage d'unité centrale utilisé par l'instrumentation IBM HTTP Server.

Pourquoi et quand exécuter cette tâche

Indiquez le pourcentage d'unité centrale que le module IBM HTTP Server Response Time peut utiliser. Le pourcentage d'unité centrale utilisé n'est pas limité par défaut. Configurez le pourcentage d'unité centrale sur le serveur où l'agent est installé.

Procédure

Pour configurer le pourcentage d'unité centrale utilisée, procédez comme suit :

1. Reconfigurez l'agent en mode interactif ou manuellement :
   - Exécutez le script d'agent pour la configuration en mode interactif :

     Linux AIX

```
$AGENT_HOME/bin/rt-agent.sh config
```

Windows

```
rép_install\BIN\rt-agent.bat config
```

- Ouvrez le fichier suivant dans un éditeur de texte :

  Linux AIX

  ```
  /opt/ibm/apm/agent/config/nom_hôte_t5.cfg
  ```

  Windows

  ```
  C:\IBM\APM\TMAITM6_x64\nom_hôte_T5.cfg
  ```

2. Dans la section **advconfig**, ajoutez le paramètre suivant et définissez une valeur comprise entre 0 et 100 :

   ```
   KT5WEBPLUGIN_TARGET_CPU_PERCENTAGE=10
   ```

   Où la valeur que vous indiquez est le pourcentage limite d'utilisation de l'unité centrale. La valeur par défaut *0* signifie que l'utilisation de l'unité centrale n'est pas limitée.
3. Vous pouvez également définir les paramètres suivants :

Option	Description
KT5WEBPLUGINCONFIGPOSTURL	Liste d'URL correspondant à une installation d'IBM HTTP Server. Valeur par défaut : `http://localhost/WrtUpdateConfig.dat`
KT5WEBPLUGIN_MAX_REQUESTS_PER_SECOND	Nombre de demandes par seconde surveillé par chaque installation d'IBM HTTP Server. Si le nombre de demandes dépasse ce chiffre, les demandes ultérieures ne sont pas surveillées. Si la limite est atteinte, l'insertion de JavaScript s'arrête, et aucune donnée n'est renvoyée à l'agent Response Time Monitoring. Valeur par défaut : `0` (aucun maximum)
KT5WEBPLUGIN_CPUMAN_PERIOD_IN_SEC	Période en secondes pendant laquelle l'utilisation de l'unité centrale est vérifiée pour déterminer si la cible a été dépassée. Valeur par défaut : `60` secondes
KT5WEBPLUGIN_CATCHUP_PERIOD_COUNT	Nombre de périodes autorisées dans le même état avant que l'utilisation de l'unité centrale soit réduite. Par exemple, avec la valeur par défaut, si l'utilisation de l'unité centrale est élevée et le reste quatre cycles plus tard, elle est réduite. Valeur par défaut : 3

Résultats
Le pourcentage d'unité centrale à la disposition du module IBM HTTP Server Response Time est défini sur une valeur fixe.

Organigramme de l'Analyseur de paquets

Utilisez l'Analyseur de paquets pour surveiller les transactions HTTP. Vous devrez configurer manuellement la surveillance HTTPS. Vous devrez instrumenter manuellement vos pages Web pour la collecte des temps du navigateur.

Pour déterminer les environnements dans lesquels vous pouvez utiliser l'Analyseur de paquets, consultez «Response Time Monitoring Composants», à la page 706 et «Planification de l'installation », à la page 706.

L'Analyseur de paquets est automatiquement activé lorsque vous installez l'agent de Response Time Monitoring, mais vous devrez peut-être effectuer un certain nombre d'étapes et personnalisations supplémentaires.

1. Vous pouvez personnaliser les paramètres de l'Analyseur de paquets, par exemple, le numéro de port dans la fenêtre Configuration d'agent. Pour plus d'informations, voir «Configuration de Analyseur de paquets à l'aide de la fenêtre Configuration d'agent», à la page 724.
2. Pour surveiller les transactions HTTPS, vous devrez instrumenter manuellement vos pages Web pour la collecte des temps du navigateur. Pour plus d'informations, voir «Surveillance des transactions HTTPS», à la page 726.
3. Pour activer les temps du navigateur, ajoutez le composant d'injection JavaScript et associez le composant de surveillance JavaScript à votre application. Pour plus d'informations, consultez «Ajout du composant de surveillance JavaScript à votre application», à la page 724.
4. Si vous utilisez un environnement où les charges de transactions sont élevées, vous aurez peut-être besoin d'effectuer des étapes d'optimisation avancées. Pour plus d'informations, voir «Configuration avancée de l'Analyseur de paquets», à la page 731.

Configuration de Analyseur de paquets à l'aide de la fenêtre Configuration d'agent

Vous pouvez utiliser la fenêtre Configuration d'agent pour configurer Analyseur de paquets.

Pour surveiller le trafic HTTP d'un système spécifique à l'aide de l'Analyseur de paquets, procédez comme suit :

1. Pour accéder à la page Configuration d'agent, dans l'Interface graphique APM , sélectionnez **Configuration du système** > **Configuration d'agent**, puis l'onglet **Temps de réponse**.
2. Sélectionnez le(s) système(s) que vous souhaitez mettre à jour. Sélectionnez plusieurs systèmes si vous souhaitez utiliser les mêmes paramètres HTTP pour chacun de ces systèmes.

   Si les systèmes que vous sélectionnez ont des valeurs HTTP définies qui sont différentes, `Multiple Values` ou `Multiple Lists` s'affiche à la place des valeurs individuelles. Vous ne pouvez pas mettre à jour simultanément des systèmes avec des valeurs différentes.
3. Dans la zone **Monitor HTTP traffic?**, cliquez deux fois sur la valeur et sélectionnez **Yes** dans la liste.
4. Dans la zone **Ports HTTP à surveiller**, cliquez deux fois sur la valeur et entrez les ports supplémentaires que vous souhaitez surveiller, à l'exception du port par défaut 80 et des autres ports déjà répertoriés.

   Pour arrêter la surveillance d'un port, sélectionnez le port que vous ne souhaitez plus surveiller et cliquez sur **Supprimer**.
5. Cliquez sur **Appliquer les modifications**.

Ajout du composant de surveillance JavaScript à votre application

Pour vous permettre de comprendre les performances de vos pages Web dans un navigateur, ainsi que les erreurs, l'agent Response Time Monitoring doit pouvoir collecter les données de temporisation du navigateur. Pour activer cette fonction, vous devez configurer l'application que vous voulez surveiller.

Pourquoi et quand exécuter cette tâche

Avant de pouvoir surveiller les interactions dans vos pages Web, vous devez ajouter le composant de surveillance JavaScript à chaque page Web pour votre application. Le composant de surveillance JavaScript capture l'état de chaque page Web et de leurs interactions JavaScript associées. Ajoutez le

composant de surveillance JavaScript à l'application que vous voulez surveiller. Le contenu et les actions appropriés sont automatiquement capturés et envoyés au serveur Cloud APM à des fins d'analyse et de corrélation.

Procédure

Pour activer la collecte des données de surveillance utilisateur réelles à partir du navigateur, procédez comme indiqué ci-après. Ces étapes ne doivent être exécutées qu'une seule fois, sauf si la configuration de l'application change.

1. Ajoutez le composant de surveillance JavaScript à l'application. La procédure à utiliser dépend du type d'application :
   a) Pour les applications Java EE, décompressez le fichier *rép_installation*`/clienttime/ClientTime.war` depuis le module d'installation vers un répertoire auquel le serveur HTTP peut accéder.
   b) Pour les applications autres que les applications non Java EE, par exemple Ruby, .NET, Python et Node.js, sauvegardez *rép_install*`/clienttime/wrtInstrumentation.js` depuis le module d'installation dans un répertoire auquel le serveur HTTP peut accéder.

      Décompressez le fichier *rép_install*`/clienttime/ClientTime.war` dans un chemin temporaire. Copiez ensuite le fichier `wrtTimingTarget.dat` extrait à la racine de document. La racine de document (document root) est un paramètre du serveur HTTP (Apache, IIS, etc). Il s'agit d'un répertoire destiné à stocker vos documents. Par défaut, toutes les demandes proviennent de ce répertoire mais des liens symboliques et des alias peuvent être utilisés pour pointer vers d'autres emplacements. Par exemple, la racine de document pour Apache est `/opt/IBM/HTTPServer/htdocs`.

      Le fichier `wrtInstrumentation.js` peut être placé dans n'importe quel répertoire. Veillez à mettre à jour le chemin d'accès à ce fichier dans l'en-tête HTML.
2. Associez le composant de surveillance JavaScript à l'application.

   Normalement, vous pouvez effectuer cette association en modifiant un script d'en-tête d'application. En général, il suffit de modifier un script d'en-tête seulement pour chaque composant ou application à surveiller.

   Pour les applications Java EE et non Java EE, ajoutez le code JavaScript suivant à l'en-tête d'application, avant tout autre code JavaScript :

   ```
   <script language="JavaScript" src="chemin/wrtInstrumentation.js"
   type="text/JavaScript"></script>
   ```

   où *chemin* est le chemin d'accès relatif au composant de surveillance JavaScript.

   Par exemple :

   ```
   <script language="JavaScript" src="/ClientTime/wrtInstrumentation.js"
   type="text/JavaScript"></script>
   ```

Résultats

Les pages qui sont instrumentées avec le composant de surveillance JavaScript sont surveillées, et les données provenant de ces pages sont analysées et affichées dans des tableaux de bord Transactions utilisateur final.

Activation des temps du navigateur

En activant la surveillance de la temporisation des ressources, l'agent Response Time Monitoring traite les données de temporisation des ressources W3C à l'aide de l'Analyseur de paquets. Si cette fonction est

activée, vous pouvez afficher des informations détaillées sur les performances des éléments en avant-plan.

Pourquoi et quand exécuter cette tâche

Pour pouvoir surveiller les données de temporisation des ressources, vous devez ajouter le composant de surveillance de la temporisation des ressources à votre application et l'associer à votre application. Le composant de surveillance de la temporisation des ressources capture automatiquement l'état et les interactions des éléments en avant-plan et envoie les données au serveur Cloud APM pour analyse. Les résultats de cette analyse sont affichés dans le tableau de bord **Sous-transactions**.

Procédure

Effectuez les étapes ci-après pour activer la fonction de surveillance de la temporisation des ressources. N'effectuez ces étapes qu'une seule fois, sauf si la configuration de l'application change.

1. Ajoutez le composant de surveillance de la temporisation des ressources à l'application.
   a) Extrayez le fichier *rép_install*/clienttime/wrtInstrumentation.js du package d'installation.
   b) Ajoutez le fichier wrtInstrumentation.js au répertoire JavaScript de votre application.
2. Ajoutez la ligne suivante à l'en-tête d'application :

```
<script> var wrt_enableResourceTiming=true; </script>
```

   Par exemple,

```
<script language="JavaScript" src="chemin/wrtInstrumentation.js"
type="text/JavaScript"></script>
<script> var wrt_enableResourceTiming=true; </script>
```

Résultats

Les pages sont instrumentées avec le composant de surveillance de la temporisation des ressources. Ce composant est activé par défaut. Les données de temporisation des ressources sur les pages instrumentées avec le composant de surveillance de la temporisation des ressources sont analysées et affichées dans les tableaux de bord **Sous-transactions**.

Que faire ensuite

Si vous souhaitez désactiver le composant de surveillance de la temporisation des ressources, définissez le paramètre **wrt_enableResourceTiming** sur false.

Surveillance des transactions HTTPS

Response Time Monitoring surveille par défaut les transactions HTTPS. Pour surveiller des transactions HTTPS, Response Time Monitoring a besoin d'accéder aux certificats SSL afin de déchiffrer le trafic SSL provenant de vos serveurs Web distants.

Avant de commencer

Identifiez les serveurs Web HTTPS à surveiller, y compris leurs adresses IP et les ports configurés. Par exemple, 192.168.1.23, port 443. Pour chaque serveur Web HTTPS, vérifiez que Response Time Monitoring peut lire ses chiffrements. Response Time Monitoring prend en charge les chiffrements pris en charge par IBM Java et notamment les chiffrements ci-après.

- RSA_WITH_RC4_40_MD5
- RSA_WITH_RC4_128_MD5
- RSA_WITH_RC4_128_SHA
- RSA_WITH_RC4_40_SHA
- RSA_WITH_DES40_CBC_SHA

- RSA_WITH_DESC_CBC_SHA
- RSA_WITH_3DES_EDE_CBC_SHA
- RSA_WITH_AES_128_CBC_SHA
- RSA_WITH_AES_256_CBC_SHA
- RSA_EXPORT1024_WITH_RC4_56_MD5
- RSA_EXPORT1024_WITH_RC2_CBC_56_MD5
- RSA_EXPORT1024_WITH_DES_CBC_SHA
- RSA_EXPORT1024_WITH_RC4_56_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

Restriction : Response Time Monitoring ne peut pas déchiffrer le trafic qui utilise l'échange de clés Diffie-Hellman.

Procédure

Pour activer la surveillance des transactions HTTPS, procédez comme suit :

1. Configurez le magasin de clés. Pour plus d'informations, voir «Configuration du magasin de clés», à la page 728.
2. Configurez l'agent Response Time Monitoring en exécutant l'une des commandes suivantes et en fournissant les valeurs demandées :

   Exemple :

```
Configuring Response Time Monitoring Agent
Edit 'Response Time Monitoring Agent' settings? [1=Yes,2=No](default is: 1): 1

Basic Configuration :   Specify basic monitoring configuration. Note: HTTP is
now configured centrally using the Response Time tab under Agent Configuration.

Specifies if HTTPS transactions should be monitored
Monitor HTTPS transactions [ 1=Yes, 2=No ] (default is:2): 1

This keystore contains the certificates of the HTTPS websites being monitored
HTTPS keystore (e.g. - /tmp/keys.kdb) (default is: ): /tmp/keys.kdb

This table maps HTTPS servers to the appropriate certificates (e.g. cert1,
server ip,server port; cert2,server2 ip,server2 port);...
HTTPS server certificate map (eg - certAlias,9.48.152.1,443;...)(default is: ):
 label1,10.0.0.1,9443;label1,9.185.150.71,443

Advanced Configuration :
Specify advanced monitoring configuration

The NIC card which has the selected IP address will be monitored.
IP address of the NIC to be monitored (default is: ): 10.0.0.1

Data Collection and Analysis Configuration :
Specify Configuration Information on how Data is Analyzed.

Configuration completed successfully.
Agent restart required to apply configuration changes.
```

   où :

   - Le magasin de clés HTTPS est le magasin de clés configuré à l'étape 1
   - Pour la mappe de certificat serveur HTTPS, indiquez :
     - `label 1` : Libellé de clé configuré à l'étape 1
     - `server ip` : Adresse IP du serveur, qui doit correspondre à l'attribut Source/Destination dans l'en-tête IPV4 des paquets
     - `server port` : Numéro de port du serveur, qui doit correspondre à l'attribut Source/Destination port dans l'en-tête TCP des paquets

Ajoutez plusieurs entrées pour plusieurs possibilités de l'IP de serveur du même intitulé de clé.

- adresse IP de la carte d'interface réseau à surveiller, l'interface qui peut voir les paquets et qui est mappée à eth0, en0, etc. Le nom n'a pas besoin de correspondre à l'un des attributs des en-têtes IPV4 ou TCP des paquets. Si `10.0.0.1` correspond à eth0, utilisez `tcpdump -s0 -i eth0 ...` pour afficher tous les paquets que doit analyser l'analyseur de paquets.

3. Redémarrez l'agent Response Time Monitoring.

Configuration du magasin de clés

Pour surveiller des transactions HTTPS, importez des clés dans KT5Keystore pour tous les serveurs Web que vous voulez surveiller.

Pourquoi et quand exécuter cette tâche

Vous pouvez exporter les certificats SSL à partir des serveurs Web que vous surveillez et les importer dans le magasin de clés HTTPS à l'aide d'IBM Key Management (iKeyman) ou spécifier le fichier de dissimulation du serveur Web (`.kdb`) dans le magasin de clés HTTPS. Lorsque vous installez ou configurez Response Time Monitoring, vous êtes invité à entrer l'emplacement du fichier `keys.kdb`.

Si vous ne disposez pas des fichiers de dissimulation de magasin de clés (`.kdb` et `.sth`), vérifiez si le fournisseur CMS est activé dans votre version Java pour que vous puissiez utiliser iKeyman pour définir la base de données de clés :

1. Accédez au répertoire *rép_install*`/ibm-jre/jre/lib/security`. Exemple :
   - Linux `/opt/ibm/apm/agent/JRE/lx8266/lib/security`
   - Windows `C:\Program Files\IBM\APM\ibm-jre\jre\lib\security`
2. Dans le fichier `java.security`, ajoutez l'instruction ci-après à la liste des fournisseurs de sécurité, comme indiqué, où *numéro* est le dernier numéro de séquence dans la liste.

   ```
   security.provider.numéro=com.ibm.security.cmskeystore.CMSProvider
   ```

   La liste des fournisseurs est similaire à celle de l'exemple suivant :

   ```
   ## List of providers and their preference orders #
   security.provider.1=com.ibm.jsse.IBMJSSEProvider
   security.provider.2=com.ibm.crypto.provider.IBMJCE
   security.provider.3=com.ibm.security.jgss.IBMJGSSProvider
   security.provider.4=com.ibm.security.cert.IBMCertPath
   security.provider.5=com.ibm.security.cmskeystore.CMSProvider
   ...
   #
   ```

3. Sauvegardez et fermez le fichier.

Restriction : Response Time Monitoring ne peut pas déchiffrer le trafic à l'aide de l'échange de clés Diffie-Hellman.

Procédure

Pour activer la surveillance des transactions HTTPS, collectez les certificats SSL à partir des serveurs Web à surveiller et importez ces certificats, ainsi que les fichiers de dissimulation du magasin de clés dans le magasin de clés HTTPS, à l'aide d'iKeyMan. L'exemple suivant utilise iKeyman pour exporter les certificats d'un serveur IBM HTTP Server, puis les importer dans le magasin de clés HTTPS :

1. Installez un agent Response Time Monitoring sur chaque serveur Web HTTPS à surveiller.
2. Exécutez **IBM Key Management** (iKeyman) à partir du répertoire `bin` d'IBM Java en exécutant l'une des commandes ci-après, en fonction de votre système d'exploitation.
   - AIX Linux `/opt/ibm/apm/agent/JRE/lx8266/bin/ikeyman`

     Remarque : X-Window doit être installé dans l'environnement pour qu'iKeyMan fonctionne correctement.
   - Windows `c:\IBM\APM\java\java80_x64\jre\bin\ikeyman`

3. Créez une base de données de magasin de clés. Dans la boîte de dialogue **Nouveau**, procédez comme suit :
   a) Dans la liste **Key database type**, sélectionnez **CMS**.

      Si CMS n'est pas disponible dans la liste, le fournisseur CMS n'est peut-être pas activé. Activez le fournisseur CMS dans le fichier de sécurité Java.

   b) Dans la zone **Nom du fichier**, entrez le nom du fichier de clé HTTPS et cliquez sur **OK**.
      Par exemple, `keys.kdb`.
4. Dans la boîte de dialogue **Password Prompt**, procédez comme suit :
   a) Dans les zones **Password** et **Confirm Password**, entrez et confirmez le mot de passe d'accès à `keys.kdb`.

      Ne définissez pas de délai d'expiration sauf si vous souhaitez régulièrement recréer la base de données de clés et redémarrer l'agent Response Time Monitoring.

   b) Sélectionnez **Stash the password to a file?** pour stocker le mot de passe de `keys.kdb` sous forme chiffrée dans un fichier de dissimulation, `keys.sth`.

      Remarque : l'agent Temps de réponse prend en charge le mot de passe secret version 1 uniquement. Après APM 8.1.4, exécutez la commande suivante pour stocker le mot de passe de keys.kdb dans le fichier de dissimulation keys.sth.

      Sous Linux :

      ```
      cp keyfile.sth keyfile.sth.new-format
      ```

      ```
      cd /opt/IBM/ccm/agent/lx8266/gs/bin
      ```

      ```
      #export LD_LIBRARY_PATH=/opt/ibm/apm/agent/lx8266/gs/lib64:$LD_LIBRARY_PATH
      ```

      ```
      ./gsk8capicmd_64 -keydb -stashpw
      -db /opt/IBM/ccm/agent/keyfiles/keyfile.kdb -v1stash
      ```

      Sous Windows :

      ```
      copy server.sth server.sth.backup
      ```

      ```
      set PATH=c:\IBM\APM\GSK8_x64\lib64;%PATH%
      ```

      ```
      C:\IBM\APM\GSK8_x64\bin\gsk8capicmd_64 -keydb
      -stashpw -db .\server.kdb -pw passw0rd -v1stash
      ```
5. Dans la section **Key database content** de la fenêtre iKeyman, procédez comme suit :
   a) Sélectionnez **Personal Certificates**.
   b) Cliquez sur **Import**.
   c) Dans la boîte de dialogue **Import Key**, dans la liste **Keyfile type**, sélectionnez **CMS**.
   d) Parcourez le fichier de clés et cliquez sur **Open**, puis sur **OK**.
   e) Dans la boîte de dialogue **Password Prompt**, entrez le mot de passe du magasin de clés.
   f) Sélectionnez la clé dans la liste et cliquez sur **OK**.
   g) Dans la boîte de dialogue **Change Labels**, sélectionnez le nom de libellé de la clé. Dans la zone **Enter a new label**, indiquez le nom d'hôte du serveur et cliquez sur **Appliquer**.

      Remarque : Cette valeur sera nécessaire lorsque vous configurerez Response Time Monitoring, notez-la.

   h) Cliquez sur **OK**.
6. Sauvegardez le magasin de clés HTTPS.

Importation de clés depuis Internet Information Services

Pour extraire des clés d'Internet Information Services et les importer dans KT5Keystore, procédez comme suit :

1. Installez un agent Response Time Monitoring sur chaque serveur Web HTTPS à surveiller.
2. Exportez un fichier .pfx à partir d'Internet Information Services :
   a. Dans le menu **Démarrer** de Windows, sélectionnez **Outils d'administration** > **Gestionnaire des services Internet (IIS)**.
   b. Sélectionnez le serveur Web et le site dont vous souhaitez exporter la clé privée, puis cliquez avec le bouton droit de la souris et sélectionnez **Propriétés** dans le menu contextuel.
   c. Sélectionnez l'onglet **Sécurité de répertoire**, puis sélectionnez **Certificat du serveur** dans la section **Communications sécurisées**.
   d. Dans **Assistant Certificat d'IIS**, cliquez sur **Suivant**.
   e. Sélectionnez **Exporter le certificat actuel vers un fichier .pfx**, puis cliquez sur **Suivant**.
   f. Entrez le chemin d'accès et le nom de fichier, puis cliquez sur **Suivant**.
   g. Entrez un mot de passe d'exportation pour la clé, puis cliquez sur **Suivant**.
   h. Cliquez sur **Suivant** sur toutes les pages suivantes, puis cliquez sur **Terminer**.
3. Procédez à l'extraction des certificats personnels et de signataires à partir du fichier .pfx :
   a. Exécutez **IBM Key Management** (iKeyman) à partir du répertoire `bin` d'IBM Java à l'aide de la commande `c:\IBM\APM\java\java80_x64\jre\bin\ikeyman`. Vérifiez que la variable d'environnement `JAVA_HOME` est définie.
   b. Dans la base de données de fichiers de clés, sélectionnez **Fichier** > **Ouvrir**.
   c. Dans la liste **Key database type**, sélectionnez **PKCS12**.
   d. Entrez le nom et le chemin d'accès du fichier de .pfx précédemment créé, puis cliquez sur **OK**. A l'invite, entrez le mot de passe, puis cliquez sur **OK**.
   e. Sélectionnez **Key Database Content** > **Personal Certificates**, puis cliquez sur **Export/Import**.
   f. Sélectionnez le type d'action **Exporter la clé** et le type de fichier de clés **PKCS12**. Entrez un nom de fichier et un emplacement pour la clé exportée, puis cliquez sur **OK**. A l'invite, entrez un mot de passe d'exportation puis cliquez à nouveau sur **OK**.
   g. Si le certificat personnel a été signé par une autorité de certification, sélectionnez **Key Database Content** > **Signer Certificates**, puis cliquez sur **Extract**. Sélectionnez le type de fichier par défaut, et entrez un nom de fichier et un emplacement pour le certificat exporté, puis cliquez sur **OK**.
4. Procédez à l'extraction des fichiers de signataire `.cer` (si nécessaire) :
   a. Si un fichier de certificats de signataire a été extrait du fichier .pfx, accédez au répertoire dans lequel il a été sauvegardé et effectuez une nouvelle copie avec l'extension `.cer`. Cliquez deux fois sur la nouvelle copie pour l'ouvrir à l'aide de l'afficheur de certificats Windows.
   b. Dans l'onglet **Chemin d'accès de certification**, vous pouvez afficher la chaîne de certificats de signataire. L'élément le plus bas de la chaîne doit être le certificat personnel. Pour tous les certificats au-dessus, procédez comme suit :
      1) Sélectionnez un certificat et cliquez sur **Afficher le certificat**.
      2) Sélectionnez **Détails** et cliquez sur **Copier dans un fichier**.
      3) Acceptez toutes les valeurs par défaut dans l'assistant d'exportation de certificat et entrez un nom de fichier avec l'extension `.cer`.
5. Créez une base de données de magasin de clés. Dans la boîte de dialogue **Nouveau**, procédez comme suit :
   a. Dans la liste **Key database type**, sélectionnez **CMS**, puis entrez un nom de fichier et un emplacement. A l'invite, entrez un mot de passe pour le nouveau fichier de clés.

      Remarque : Veillez à sélectionner **Stash the password to a file**.

b. Si des certificats de signataire ont été extraits du fichier .pfx, procédez comme suit :
   1) Sélectionnez **Key Database Content** > **Signer Certificates**.
   2) Pour chaque certificat de signataire, cliquez sur **Ajouter** et ajoutez le fichier `.cer`.
c. Sélectionnez **Key Database Content** > **Personal Certificates**, puis cliquez sur **Import**.
d. Sélectionnez le type de fichier de clés **PKCS12**, et le nom et l'emplacement du fichier **.p12**. A l'invite du système, entrez le mot de passe.
e. Sauvegardez le fichier de clés et quittez l'utilitaire de gestion de clés.
f. Copiez les fichiers `.kdb` et `.sth` dans KT5Keystore sur la machine Response Time Monitoring.
g. Placez les fichiers de base de données IBM Key Management (`.kdb`) et de stockage (`.sth`) dans un répertoire sûr, et assurez-vous que seul l'administrateur ou le `superutilisateur` (ou l'ID utilisateur qui a servi à installer l'agent Response Time Monitoring) peut les lire.

Configuration avancée de l'Analyseur de paquets
Il existe un certain nombre d'options de configuration avancées pour l'Analyseur de paquets.

Une fois que vous avez configuré l'Analyseur de paquets, il existe un certain nombre de tâches de configuration avancées que vous pouvez effectuer pour affiner les performances et les fonctionnalités.

Utilisation des équilibreurs de charge
Si vous utilisez des équilibreurs de charge dans votre environnement, il est nécessaire de les personnaliser.

Procédure

Si vous utilisez un équilibreur de charge, procédez comme suit :

1. Désactivez la réécriture des URL sur l'équilibreur de charge.
2. Installez un agent Response Time Monitoring sur chaque serveur Web que vous souhaitez surveiller.
   N'installez pas Response Time Monitoring sur l'équilibreur de charge.
3. Ajoutez le composant de surveillance JavaScript à votre application. Pour plus d'informations, voir «Ajout du composant de surveillance JavaScript à votre application», à la page 724.

Que faire ensuite

Si vous exécutez l'agent Response Time Monitoring derrière un équilibreur de charge, vous pouvez configurer ce dernier afin qu'il achemine l'adresse IP du client pour optimiser les performances de surveillance. Par exemple, reportez-vous à la procédure suivante :

1. Dans l'en-tête HTTP, définissez l'adresse IP du client dans la zone **`X-Forwarded-For`**.
2. Configurez l'agent Response Time Monitoring pour qu'il utilise l'en-tête d'adresse IP du client. Définissez l'en-tête d'adresse IP du client dans la zone **`KFC_OVERRIDE_SOURCE_ADDR_HEADER`**, dans l'un des fichiers suivants, en fonction de votre système d'exploitation :
   - AIX Linux `/opt/ibm/apm/agent/tmaitm6/wrm/kfcmenv`
   - Windows `C:\IBM\ITM\TMAITM6_x64\wrm\Analyzer\kfcmenv`

   Par exemple :

   ```
   KFC_OVERRIDE_SOURCE_ADDR_HEADER=x-forwarded-for
   ```

   ou si vous utilisez WebSEAL :

   ```
   KFC_OVERRIDE_SOURCE_ADDR_HEADER=adresse_éloignée_iv
   ```

Configuration de la limite de surcharge de l'UC
Si vous utilisez un environnement où les charges de transactions sont élevées, vous pouvez limiter les ressources de surveillance utilisées par l'agent Response Time Monitoring.

Pourquoi et quand exécuter cette tâche

Cette fonction limite l'utilisation de l'UC de l'agent Response Time Monitoring en surveillant et en signalant uniquement une partie du trafic Web à l'aide d'échantillons. La `limite de surcharge de l'UC` n'est pas configurée par défaut. Vous devez configurer la `limite de surcharge de l'UC` sur le serveur où l'agent est installé.

Procédure

Pour configurer la `limite de surcharge de l'UC`, procédez comme suit :

1. Ouvrez le fichier suivant dans un éditeur de texte :

   Linux AIX `/opt/ibm/apm/agent/tmaitm6/wrm/kfcmenv`

   Windows `C:\IBM\ITM\TMAITM6_x64\wrm\Analyzer\kfcmenv`

2. Configurez les valeurs des paramètres suivants :

   KFC_MAX_PROTOCOL_PACKETRATE
   Taux de paquets maximal initial. Par exemple, si vous spécifiez **KFC_MAX_PROTOCOL_PACKETRATE=2000**, le taux de paquets maximal est de 2000 paquets par seconde. Ce taux varie de manière dynamique en fonction de la valeur du paramètre **KFC_CPUTHROTTLE_TARGET** et de la quantité d'UC actuellement utilisée.

   KFC_CPUTHROTTLE_TARGET
   Pourcentage de la quantité globale de ressources d'UC qui peut être utilisé par le processus `kfcmserver`. Par exemple, si vous spécifiez **KFC_CPUTHROTTLE_TARGET=10.0**, le processus `kfcmserver` peut utiliser jusqu'à 10 % des ressources d'UC globales.

   Remarque : La valeur du paramètre **KFC_CPUTHROTTLE_TARGET** correspond au pourcentage de ressources d'UC globales disponible pour le processus `kfcmserver`. Par exemple, si vous disposez de 4 noyaux d'unités centrales et si **KFC_CPUTHROTTLE_TARGET** est défini sur 10, le moniteur de ressources de Windows mesure les ressources d'UC sur 400%. Par conséquent, le processus `kfcmserver` peut utiliser jusqu'à 40 % de la quantité totale de ressources d'UC disponibles (400 %).

Résultats
La `limite de surcharge de l'UC` est configurée pour l'agent Response Time Monitoring.

Reconfiguration de l'environnement depuis le module IBM HTTP Server Response Time vers l'Analyseur de paquets

Cette rubrique indique comment passer de l'environnement de surveillance du module IBM HTTP Server Response Time à l'Analyseur de paquets.

Procédure

1. Désinstallez l'agent Serveur HTTP
   a) Modifiez `/etc/httpd/conf/httpd.conf` en mettant en commentaire la ligne du plug-in Response Time. Par exemple :

   ```
   #include /opt/ibm/apm/agent/tmp/khu/khu.etc.httpd.conf.httpd.conf
   ```

   b) Désinstallez l'agent Serveur HTTP. Par exemple :

   ```
   /opt/ibm/apm/agent/bin/http_server-agent.sh uninstall
   ```

c) Ouvrez une nouvelle fenêtre d'invite de commande pour nettoyer le système avant de reconfigurer l'agent Temps de réponse à l'étape suivante.

2. Ouvrez le fichier suivant :

   Linux AIX *rép_install*/config/*nom_hôte*_t5.cfg
   Où *rép_install* est /opt/ibm/apm/agent
   Windows *rép_install*\TMAITM6_x64*nom_hôte*_t5.cfg
   où *rép_install* est C:\IBM\APM

3. Définissez les paramètres comme indiqué ci-après.

```
{ KT5DISABLEANALYZER=NO } { KT5ENABLEWEBPLUGIN=NO }
```

4. Reconfigurez l'agent de la manière suivante :

```
re-agent.bat config  rép_install\samples\rt_silent_config.txt
```

Personnalisation des valeurs de localisation Transaction utilisateur final

Vous pouvez personnaliser les localisations appliquées à des adresses IP ou à des plages d'adresses IP spécifiques dans les tableaux de bord Transaction utilisateur final pour votre environnement.

Avant de commencer

Utilisez l'onglet **Geolocation** sous **Configuration d'agent** pour personnaliser les valeurs de localisation.

Utilisez cette fonction pour définir la localisation des adresses IP affichées comme **inconnues** dans le tableau de bord. Ces adresses peuvent être des adresses internes, comme 192.168.x.x ou 10.x.x.x, ou des adresses IP externes qui ne sont pas résolues. Vous pouvez également utiliser cette fonction pour ignorer les localisations incorrectes des adresses IP. Par exemple, si vous savez que l'adresse IP 9.1.1.1 est située à Los Angeles mais qu'elle apparaît en tant qu'adresse située à San Francisco, ignorez la localisation et associez l'adresse 9.1.1.1 à Los Angeles.

Pourquoi et quand exécuter cette tâche

Personnalisez les valeurs de localisation dans les tableaux de bord Transaction utilisateur final en téléchargeant un fichier CSV contenant les valeurs dont vous avez besoin. Vous trouverez un exemple de fichier CSV dans l'onglet **Geolocation**.

Le fichier CSV doit inclure les valeurs ci-dessous comme en-tête. Les valeurs peuvent être de n'importe quel ordre et les entrées doivent respecter cet ordre.

```
IP_ADDRESS, COUNTRY, REGION, CITY
```

Par exemple,

```
IP_ADDRESS, COUNTRY, REGION, CITY
10.0.5.0/24, Australia, WA, Perth
10.1.0.6, Australia, VIC, Melbourne
```

Vous pouvez indiquer une adresse IPv4 unique ou définir une plage d'adresses. Si vous indiquez une plage, assurez-vous que vous utilisez une valeur valide comprise entre 1 et 32.

Procédure

Pour personnaliser les valeurs de localisation affichées dans les tableaux de bord Transaction utilisateur final, effectuez les opérations suivantes dans le tableau de bord d'Application Performance.

1. Configurez votre fichier ou vos fichiers CSV ; les adresses IP doivent correspondre aux localisations.
2. Téléchargez le fichier CSV.
   a) Accédez à **Configuration d'agent** > **Geolocation**.
   b) Cliquez sur **Upload CSV**, sélectionnez les fichiers à télécharger, puis cliquez sur **Ouvrir**.

- Vérifiez que le fichier CSV répertorie les plages d'adresses IP générales en premier, suivies des adresses IP plus spécifiques.
- Téléchargez plusieurs fichiers si nécessaire.
- Si les valeurs d'un fichier chevauchent celles d'un autre fichier, les valeurs du fichier le plus récent prévalent sur celles de l'autre fichier.

3. Développez **Upload Results** à la recherche d'éventuelles erreurs. Recherchez les problèmes suivants :
   - Substitutions
   - Adresses IP non valides
   - Lignes non valides
   - Valeurs comportant plus de 250 caractères

Résultats

Patientez quelques minutes et affichez vos valeurs personnalisées dans les tableaux de bord Transaction utilisateur final.

Que faire ensuite

Vous pouvez supprimer des valeurs personnalisées si nécessaire. Effectuez l'une des étapes suivantes :

- Pour supprimer certaines valeurs personnalisées, sélectionnez les adresses IP à supprimer, cliquez sur **Clear Selected Entries**, puis sur **OK** pour confirmer la suppression.
- Pour supprimer toutes les valeurs personnalisées, cliquez sur **Clear All Entries**, puis sur **OK** pour confirmer la suppression.

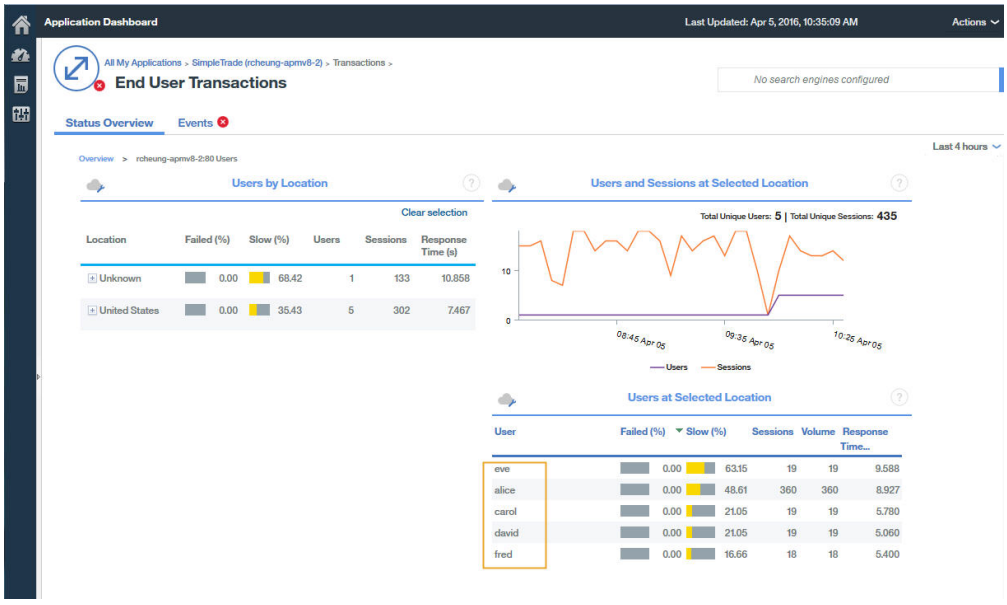
Suivi des applications Web supplémentaires

Pour suivre des applications Web en plus de celles déjà suivies par défaut, vous devez identifier et configurer les méthodes de suivi des utilisateurs et des sessions.

Avant de commencer

Si votre application n'est pas prise en charge par défaut, les tableaux de bord ne contiennent aucun détail d'utilisateur et de session ; le nom d'utilisateur s'affiche comme anonymous ou unknown, et aucune information de session n'est disponible.

Si les méthodes de suivi sont correctement configurées, l'ID utilisateur est extrait puis listé dans le tableau de bord **Transactions utilisateur final** > **User Summary** > **Utilisateurs à l'emplacement sélectionné**.



Remarque : le suivi des utilisateurs est basé sur le suivi de sessions. Vous devez au préalable définir la variable correcte pour les méthodes de suivi des sessions dans les paramètres de configuration de l'agent Temps de réponse, pour les méthodes de suivi des utilisateurs et des sessions.

Pourquoi et quand exécuter cette tâche

Dans IBM Application Performance Management version 8.1.4 et ultérieure, vous pouvez utiliser la page **Configuration d'agent** > **Temps de réponse** pour ajouter les applications que vous souhaitez suivre au moyen de l'Analyseur de paquets ou du module IBM HTTP Server Response Time. Les valeurs définies sur cette page prévalent sur celles du fichier `WRT_Defaults.xml`.

Pour suivre des applications supplémentaires, vous devez d'abord identifier les méthodes et valeurs des ID utilisateur et session pour l'application que vous souhaitez suivre. Par exemple :

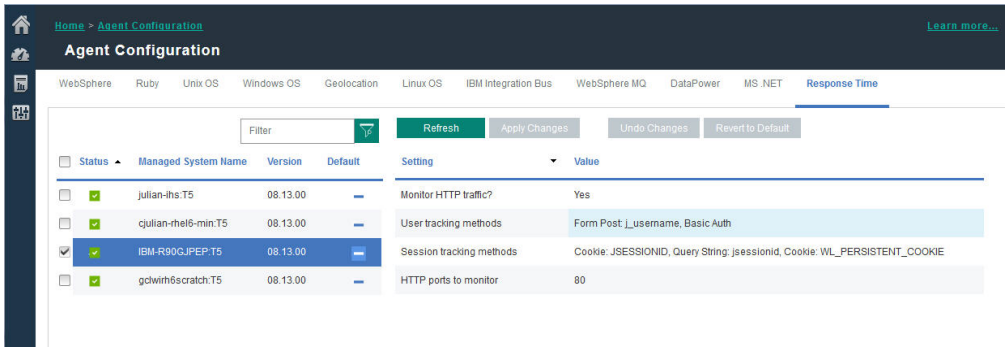
1. Ouvrez l'outil de développement de votre navigateur de sorte à afficher les demandes associées à l'application que vous souhaitez suivre.
2. Sélectionnez la dernière demande dans le journal de réseau du navigateur afin d'identifier facilement votre demande test.
3. Créez une demande test à l'aide de paramètres reconnaissables. Par exemple, connectez-vous à votre site Web en tant qu'`utilisateur test`.
4. Sélectionnez la demande test et vérifiez les `en-têtes`.
5. Identifiez l'ID session dans le journal des demandes. L'ID session est généralement spécifié dans le contenu `cookie`, `POST`, `en-tête de demande/réponse` ou `chaîne de requête`. Si le `cookie` est déjà défini dans le profil par défaut, vous n'avez pas besoin de l'ajouter à l'étape 2.
6. Identifiez l'ID utilisateur dans le journal des demandes. L'ID utilisateur peut être spécifié dans le contenu `cookie`, `en-tête de demande`, `POST` ou `chaîne de requête`. Par exemple, recherchez `utilisateur test` pour obtenir la valeur de l'ID utilisateur.
7. Les variables **Méthodes de suivi des utilisateurs** et **Méthodes de suivi des sessions** doivent être mises à jour avec le nom de session et le nom d'utilisateur en cours corrects dans le code d'application du client. La manière dont le nom de session et le nom d'utilisateur sont identifiés dépend du code de l'application. La valeur par défaut du paramètre Utilisateur/Session dans la version 8.1.4 est la suivante :

```
Session tracking methods=cookie\:JSESSIONID,querystring\:jsessionid,cookie\
       :WL_PERSISTENT_COOKIE
User tracking methods=formpost\:j_username,formpost\:uid,formpost\
       :ctl00%24MainContent%24uid,basicauth\:Authorization\: Basic
```

Procédure

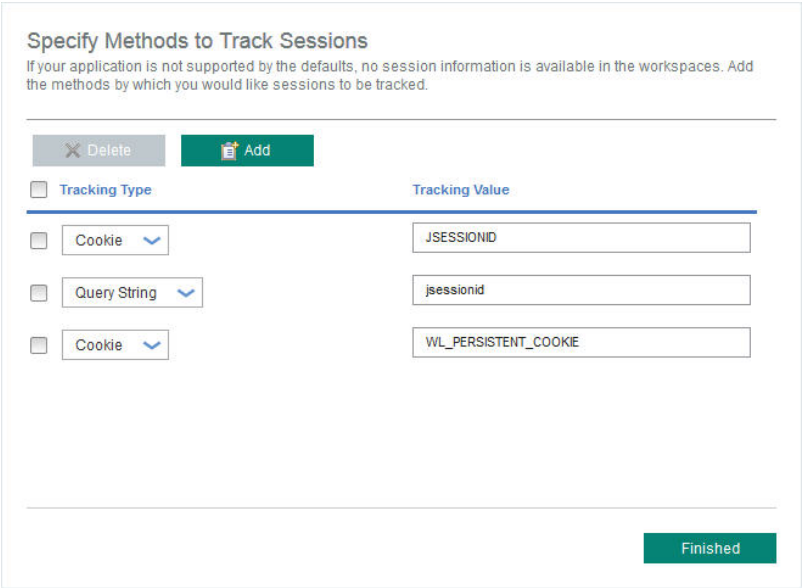
Une fois les méthodes et valeurs de suivi des utilisateurs et des sessions utilisées dans votre application identifiées, procédez comme suit :

1. Accédez à la page de configuration **Configuration d'agent** > **Temps de réponse**.



2. Sélectionnez le système géré que vous souhaitez mettre à jour.
3. Si nécessaire, mettez à jour les méthodes de suivi des sessions :

a) Cliquez sur la valeur dans la zone **Méthodes de suivi des sessions**.



b) Dans la fenêtre **Spécifiez les méthodes de suivi des sessions**, cliquez sur **Ajouter**.

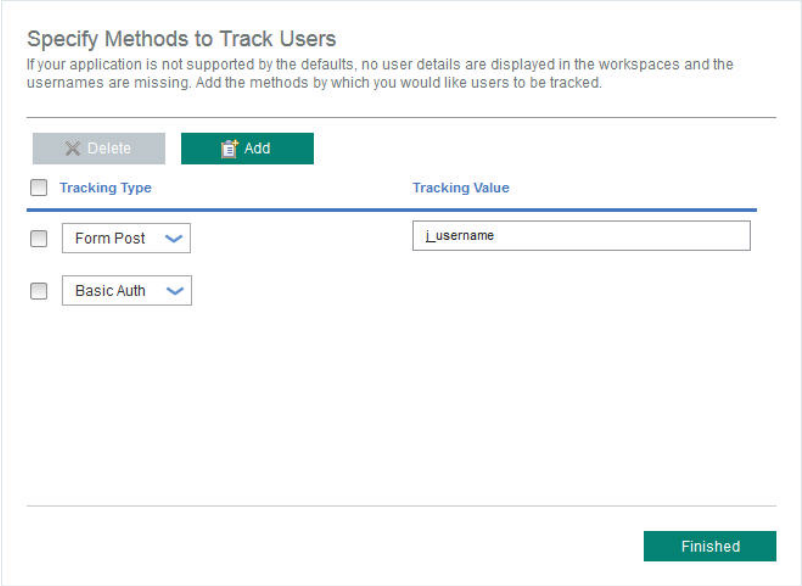
c) Dans la liste **Type de suivi**, sélectionnez le type de suivi. Par exemple, `Cookie`.

d) Dans la zone **Valeur de suivi**, indiquez une valeur. Par exemple, `WL_PERSISTENT_COOKIE`.

e) Cliquez sur **Terminé**.

4. Si nécessaire, mettez à jour les méthodes de suivi des utilisateurs :

a) Cliquez sur la valeur dans la zone **Méthodes de suivi des utilisateurs**.



b) Dans la fenêtre **Spécifiez les méthodes de suivi des utilisateurs**, cliquez sur **Ajouter**.

c) Dans la liste **Type de suivi**, sélectionnez le type de suivi. Par exemple, `En-tête`.

d) Dans la zone **Valeur de suivi**, indiquez une valeur. Par exemple, `nom d'utilisateur`.

e) Cliquez sur **Terminé**.

5. Sur la page Configuration d'agent, cliquez sur **Appliquer les modifications**.

Résultats

Les applications auxquelles les nouvelles méthodes de suivi indiquées sont appliquées figurent dans le Tableau de bord des applications.

Que faire ensuite
Vérifiez que les ID utilisateur et informations de session associés à l'application figurent dans le Tableau de bord des applications.

Spécification d'un nom de système géré unique pour l'Agent de surveillance des temps de réponse

Le nom d'instance de l'Agent de surveillance des temps de réponse affiché sur la console du Cloud APM est également appelé nom de système géré (MSN). Vous pouvez utiliser le paramètre de configuration d'agent afin d'indiquer un MSN unique pour chaque instance d'agent.

Pourquoi et quand exécuter cette tâche
Le nom de système géré de l'Agent de surveillance des temps de réponse est au format suivant :

```
nom_instance:nom_hôte:T5
```

T5 est le code produit de l'Agent de surveillance des temps de réponse.

Procédure

1. Arrêtez toutes les instances d'agent existantes. S'il n'en existe aucune, passez à l'étape suivante. Pour plus d'informations sur l'arrêt des instances d'agent, voir «Utilisation des commandes de l'agent», à la page 181.
2. Linux AIX Modifiez **CTIRA_SUBSYSTEM_ID** dans le fichier `runagent`. En général, toutes les instances d'agent sur un ordinateur utilisent la même valeur de nom d'hôte.
   a) Effectuez une copie de sauvegarde du fichier :

   ```
   Linux AIX rép_install/plateforme/t5/bin/runagent
   ```

   b) Modifiez le fichier. Ajoutez *nouveau_nom_instance* sur les systèmes Linux ou AIX.

   ```
   Linux AIX CTIRA_SUBSYSTEM_ID=nouvel_id_sous_système
   ```

3. Démarrez les instances existantes de l'agent.
4. Démarrez console Cloud APM. Modifiez vos applications en supprimant les instances d'agent sous les anciens MSN et en ajoutant les nouvelles instances d'agent.

Configuration de la surveillance de Ruby

Vous pouvez surveiller à la fois les applications Ruby sur site et IBM Cloud. Pour surveiller les applications Ruby sur site, configurez l'Agent Ruby. Pour surveiller les applications Ruby IBM Cloud, configurez le collecteur de données Ruby.

Pourquoi et quand exécuter cette tâche

Les instructions concernent l'édition la plus récente de l'agent, sauf indication contraire.

La procédure suivante, qui inclut des étapes obligatoires et facultatives, permet de configurer l'Agent Ruby et le collecteur de données Ruby. Effectuez les étapes de configuration en fonction de vos besoins.

Procédure

- Pour surveiller les applications Ruby sur site, effectuez les étapes suivantes pour configurer l'Agent Ruby :
  a) Configurez des instances d'agent pour surveiller les applications Ruby. Voir Configuration de l'Agent Ruby pour surveiller les applications Ruby.

b) Installez le collecteur de données pour surveiller les données à afficher dans la console Cloud APM. Voir Installation du collecteur de données.

c) Facultatif : Si vous êtes un utilisateur Cloud APM, Advanced, vous pouvez procéder comme suit en fonction de vos besoins :

- Pour configurer le collecteur de données afin qu'il collecte des données de diagnostic, voir Configuration du collecteur de données de diagnostic.
- Pour activer la trace de méthode pour les demandes et ajuster la longueur du paramètre de chemin d'accès au fichier qui s'affiche dans le widget Trace de pile des demandes, voir Activation du suivi des méthodes et ajustement de l'affichage de chemin.
- Pour augmenter la taille de segment de mémoire de JVM afin d'éviter l'erreur `out of memory`, voir Augmentation de la taille de segment de mémoire de JVM.
- Pour désactiver les diagnostics, voir Désactivation ou activation des données de diagnostic pour les applications Ruby.

- Pour surveiller les applications Ruby IBM Cloud, effectuez les étapes suivantes afin de configurer le collecteur de données Ruby :

a) Configurez le collecteur de données Ruby pour les applications IBM Cloud. Pour obtenir des instructions, voir «Configuration du collecteur de données Ruby pour les applications IBM Cloud», à la page 745.

b) Facultatif : Pour modifier le comportement du collecteur de données Ruby, voir «Personnalisation du collecteur de données Ruby pour les applications IBM Cloud», à la page 746.

Configuration de l'Agent Ruby

Pour que l'Agent Ruby surveille vos applications, indiquez la durée d'exécution de Ruby. Utilisez ainsi cette durée d'exécution pour regrouper les données issues des applications Ruby et configurer l'agent.

Avant de commencer

Identifiez le serveur que vous allez utiliser pour démarrer les applications Ruby ainsi que le répertoire bin qualifié contenant l'exécutable Ruby ou Rake utilisé par l'agent :

1. Pour déterminer le serveur d'applications que vous allez utiliser, exécutez la commande suivante :

   ```
   ps -ef | grep ruby
   ```

   Le nom du serveur utilisé pour démarrer votre application s'affiche. Les noms de serveur possibles sont répertoriés comme suit :

   - `Passenger`
   - `Unicorn`
   - `Puma`
   - `Thin`

   Si le résultat de la commande n'indique aucun des noms de serveur mentionnés ci-dessus, le serveur que vous utilisez pour démarrer l'application sera peut-être WEBrick.

   Important : Si vous utilisez plusieurs serveurs Web pour démarrer vos applications Ruby, vous devez créer une instance d'agent pour chaque serveur Web d'application : une instance pour PUMA et une pour Unicorn par exemple.

2. Pour déterminer le répertoire bin qualifié contenant l'exécutable Ruby ou Rake utilisé par l'Agent Ruby, exécutez la commande suivante :

   ```
   which ruby
   ```

Pourquoi et quand exécuter cette tâche

Vous pouvez répéter cette tâche pour configurer plusieurs instances d'agent en fonction de vos besoins.

Procédure

1. Pour configurer l'agent, exécutez la commande suivante :
   rép_install/bin/ruby-agent.sh config *nom_instance*
   où *nom_instance* est le nom à attribuer à l'instance, et *rép_install* est le répertoire d'installation de l'Agent Ruby. Le répertoire d'installation par défaut est /opt/ibm/apm/agent.

   Important : N'indiquez pas de nom d'instance long. La longueur totale de votre nom d'hôte et du nom d'instance d'agent ne doit pas dépasser 28 caractères. Si la longueur dépasse la limite, le nom de système géré est tronqué et le code produit de l'Agent Ruby ne s'affiche pas correctement.

   Le nom de système géré inclut le nom d'instance que vous spécifiez, *nom_instance*:*nom_hôte*:*pc* par exemple, où *pc* est le code produit à deux caractères de l'agent. Par exemple, si vous indiquez Ruby2 comme nom d'instance, votre nom de système géré est Ruby2:hostname:KM, où *KM* correspond au code produit à deux caractères de l'Agent Ruby.
2. A l'invite Edit 'Monitoring Agent for Ruby' settings, entrez 1 pour continuer.
3. A l'invite Fully Qualified Rubies Bin Directory, indiquez le répertoire bin. Par exemple, si vous utilisez Ruby Version Manager (RVM), entrez /usr/local/rvm/rubies/ruby-2.0.0-p247/bin.
4. A l'invite Auto Detect Ruby Applications Flag, entrez Y pour continuer. L'agent reçoit les données envoyées par le collecteur de données de l'agent.
5. A l'invite Application Server Process name, appuyez sur Entrée pour accepter la valeur par défaut de ruby, ou spécifiez la valeur du serveur que vous utilisez en vous référant à la liste suivante :
   - Pour les serveurs WEBrick, acceptez la valeur par défaut ou spécifiez ruby ; si le composant Rails est installé par Ruby Stack, spécifiez .ruby.bin.
   - Pour les serveurs Passenger, spécifiez passenger.
   - Pour les serveurs Unicorn, spécifiez unicorn.
   - Pour les serveurs Puma, spécifiez puma.
   - Pour les serveurs Thin, si les applications sont démarrées en exécutant la commande thin start, acceptez la valeur par défaut pour utiliser ruby ; si les applications sont démarrées en utilisant la commande thin start -d, spécifiez thin ; si le composant Rails est installé par Ruby Stack et que les applications sont démarrées en exécutant la commande thin start, spécifiez .ruby.bin.
6. A l'invite Socket Data Source, appuyez sur Entrée pour accepter la valeur par défaut 0 permettant d'utiliser le port temporaire.
7. A l'invite Edit 'Application' settings, entrez 5 pour quitter.
8. Pour démarrer l'agent, exécutez la commande suivante :
   rép_install/bin/ruby-agent.sh start *nom_instance*

Que faire ensuite
Installez le collecteur de données pour que l'Agent Ruby fonctionne correctement et pour que les données s'affichent dans l'interface utilisateur de Cloud APM. Pour plus d'informations, voir Installation du collecteur de données

Installation du collecteur de données
Vous devez installer le collecteur de données pour que l'agent fonctionne correctement. Après avoir installé le collecteur de données, les données de surveillance s'affichent dans le Tableau de bord d'Application Performance.

Avant de commencer
Si vous avez installé une application Ruby on Rails sur un système Linux en utilisant un compte utilisateur non superutilisateur et que vous prévoyez de collecter des données de diagnostic, l'utilisateur non superutilisateur doit avoir accès au répertoire de base du collecteur de données de diagnostic. Vérifiez que l'utilisateur non superutilisateur dispose d'un accès en lecture et en écriture au répertoire *rép_install*/install-images/kkm, où *rép_install* correspond au répertoire d'installation de l'Agent

Ruby. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`. Entrez si nécessaire les droits d'accès en lecture et en écriture à l'aide de la commande `chmod 777`.

Procédure

1. Arrêtez votre application Ruby on Rails.
2. Facultatif : Si vous mettez à niveau le collecteur de données Ruby to a new version, vers une nouvelle version, vous devez au préalable désinstaller l'ancienne version du collecteur de données en exécutant la commande suivante :

   ```
   gem uninstall stacktracer
   ```

3. Installez le collecteur de données de diagnostic. Entrez `gem install --local` *`rép_install`*`/lx8266/km/bin/stacktracer-`*`version`*`.gem`, où *version* est le numéro de version et *rép_install* est le répertoire d'installation de l'Agent Ruby. Le numéro de version du fichier `stacktracer-`*`version`*`.gem` dans le répertoire d'installation indique le numéro de version dont vous avez besoin pour entrer ici. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.

   Important : Installez le collecteur de données avec le même ID utilisateur que vous avez utilisé pour installer et exécuter l'application Ruby on Rails.
4. Accédez au répertoire de base de votre application, ouvrez le fichier `Gemfile` et ajoutez la ligne suivante à la fin du fichier : `gem 'stacktracer', '`*`version`*`'`
   où *version* est le numéro de version du collecteur de données. Le numéro de version se trouve dans le nom du fichier `stacktracer-`*`version`*`.gem` qui se trouve dans *rép_install* de l'Agent Ruby.
   Par exemple, si vous installez le collecteur de données Ruby Version 1.0 Fix Pack 8, le fichier `stacktracer-01.00.08.00.gem` se trouve dans le répertoire d'installation de l'agent. Ensuite, ajoutez la ligne `gem 'stacktracer', '01.00.08.00'` à votre application pour installer le collecteur de données.

   Remarque : S'il n'existe qu'une seule version de `stacktracer` dans l'environnement, ajoutez la ligne `gem 'stacktracer'` à la fin du fichier. Ne spécifiez pas le numéro de version dans la ligne.
5. Dans le répertoire de base de votre application, entrez `bundle install`.
6. Redémarrez l'application Ruby on Rails.

Résultats

Le collecteur des données est installé et configuré, et l'application Ruby on Rails est démarrée.

Que faire ensuite

- Si vous n'êtes pas connecté, suivez les instructions figurant dans «Démarrage de la console Cloud APM», à la page 1003. Sélectionnez **Performance** > **Tableau de bord d'Application Performance** pour ouvrir le tableau de bord **Toutes mes applications**, puis explorez en aval les tableaux de bord de diagnostic et de surveillance des ressources des applications Ruby pour observer les applications Ruby on Rails du récapitulatif des statuts jusqu'aux instances de demande individuelles.
- Pour afficher et modifier les paramètres du collecteur des données diagnostics, passez à la rubrique suivante, «Configuration du collecteur de données de diagnostic», à la page 741.
- Pour afficher les données de trace de méthode pour les demandes dans l'interface utilisateur de Cloud APM, voir Activation du suivi des méthodes et ajustement de l'affichage de chemin.
- Lorsque la trace de méthode est activée ou que le nombre de demandes de données est élevé, vous risquez de recevoir des erreurs `out of memory`. Vous pouvez augmenter la taille de segment de mémoire de JVM afin d'éviter ces erreurs. Voir Augmentation de la taille de segment de mémoire de JVM.
- Vous pouvez désactiver ou activer à tout moment la collecte des données de diagnostic pour une ou plusieurs applications Ruby on Rails gérées via la console Cloud APM. Voir «Désactivation ou activation des données de diagnostic pour les applications Ruby», à la page 745 . Cette fonction n'est pas disponible pour la surveillance des ressources.

Configuration du collecteur de données de diagnostic
Si vous êtes un utilisateur de Cloud APM, Advanced, vous pouvez continuer à configurer le collecteur de données pour les données de diagnostic. La collecte des données de diagnostic est désactivée par défaut dans le fichier de configuration du collecteur de données.

Avant de commencer
Vous devez avoir installé le collecteur de données de diagnostic et configuré la prise en charge de la collecte des données de diagnostic, comme indiqué dans «Installation du collecteur de données», à la page 739.

Pourquoi et quand exécuter cette tâche
Le fichier de configuration `instrumenter_settings.rb` apparaît une fois que l'agent a enregistré l'existence d'un application Ruby on Rails en configurant correctement le fichier `Gemfile`. Ce fichier de configuration peut être modifié pendant que l'agent Ruby est actif, et les modifications sont appliquées automatiquement. Vous pouvez également appliquer les modifications à toutes les applications Ruby on Rails surveillées, ce qui implique d'arrêter les applications pendant que vous modifiez le fichier de configuration.

Procédure

- Pour modifier les paramètres du collecteur de données pour une application spécifique en cours d'exécution :
  1. Accédez au répertoire *rép_install*`/install-images/kkm/dchome/`*appClassName*`/config`, où *appClassName* est le nom de classe d'application Ruby, et *rép_install* est le répertoire d'installation de l'Agent Ruby. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.
  2. Ouvrez `instrumenter_settings.rb` dans un éditeur de texte.
  3. Modifiez les paramètres du collecteur de données :

     :instrumentation_enabled
     Pour activer le support de la collecte des données de diagnostic, définissez `:instrumentation_enabled => true`.

     Pour désactiver le support de la collecte des données de diagnostic, définissez `:instrumentation_enabled => false`.

     :sample_frequency
     Pour modifier la fréquence d'échantillonnage de demandes, entrez le nombre de demandes entre les échantillonnages.

     Le collecteur de données ne rassemble les données de diagnostic que pour les demandes échantillonnées. Si vous définissez la propriété `:sample_frequency => 10`, par exemple, les données sont collectées pour 1 demande sur 10.

     :max_methods_to_instrument
     Pour désactiver ou activer la collecte des données de trace des méthodes et limiter le nombre de méthodes à suivre, définissez la valeur zéro ou entrez le nombre maximal de méthodes à suivre.

     Pour désactiver la collecte des données de trace des méthodes, définissez `:max_methods_to_instrument => 0`.

     Pour l'activer, définissez `:max_methods_to_instrument => 10000`. Cette valeur peut être plus élevée, mais pas trop afin d'éviter une baisse des performances. Lorsque les données des méthodes sont collectées, les appels aux méthodes sont inclus dans le widget Trace des méthodes du tableau de bord Traces des demandes, ce qui permet d'afficher toutes les instances de demande et leurs demandes imbriquées.

     :min_wallclock_to_include_in_trace
     Pour modifier le seuil qui détermine si la demande ou la méthode doit être tracée, définissez le temps minimum de réponse. Si vous définissez `:min_wallclock_to_include_in_trace`

`=> 0.001`, par exemple, seules les demandes et les méthodes dont les temps de réponse dépassent 1 milliseconde sont suivis.

A faire : Dans le tableau de bord des diagnostics **Trace des demandes**, vous pouvez explorer en aval vers une instance de demande depuis le widget de groupe Trace de pile de demande. Les totaux des temps de réponse de l'instance peuvent être incorrects du fait des filtres définis pour `:min_wallclock_to_include_in_trace` et `:min_wallclock_to_include_stacks`, qui peuvent exclure des données.

:min_wallclock_to_include_stacks
Pour modifier le seuil qui détermine si les informations de trace de pile doivent être collectées pour une demande ou une méthode, définissez le temps de réponse minimum.

Si vous définissez `:min_wallclock_to_include_stacks => 0.1`, par exemple, les informations de trace de pile sont collectées pour toutes les demandes et méthodes dont le temps de réponse est supérieur à 100 millisecondes.

:include_subclasses_of_these_modules
Le tableau de bord des diagnostics Trace des demandes permet d'identifier la séquence des appels aux demandes imbriquées et aux méthodes d'une instance de demande. Le collecteur des données filtre à l'avance les méthodes des classes qui ne sont pas incluses dans la liste de filtres. Si des opérations à suivre ne sont pas incluses dans les traces de pile des méthodes, vous pouvez les ajouter ici.

Pour définir les méthodes à suivre, ajoutez leurs noms de classe.

Supposons que vous vouliez tracer les API Moped dans le type de code Ruby suivant :

```
session = Moped::Session.new(['ip:27017'])
session.use(:HR)
session[:profiles].insert({......})
session[:profiles].find({...}).remove
```

Ajoutez les noms de module de ces API Moped à la propriété :

```
:include_subclasses_of_these_modules => {"
ActionController" => true,
                     "ERB" => true,
                     "erb" => true,
                     "Arel" => true,
                     "Mongoid" => true,
                     "Moped" => true
                    },
```

Restriction : Les traces de méthode n'incluent pas les méthodes de classe et les méthodes privées (méthodes définies dans une classe, qui ont des spécificateurs d'accès "privé" implicite ou explicite).

:include_sql_text
Pour collecter les données de contexte pour les méthodes, affectez à cette propriété la valeur `true`.

:num_samples_per_file
Pour modifier le nombre maximal de demandes suivies à stocker dans chaque fichier, entrez une valeur, telle que `:num_samples_per_file => 1000`. Lorsque la limite définie ici est atteinte, un nouveau fichier est créé.

Envisagez d'affecter au paramètre `:num_samples_per_file` une valeur inférieure si vous ajustez la configuration de manière à ce que davantage de données soient collectées. Par exemple, la définition de `:include_subclasses_of_these_modules` pour effectuer le suivi d'un nombre plus élevé de classes et de méthodes peut augmenter la collecte de données. L'affectation d'une valeur inférieure à l'une des propriétés suivantes peut également augmenter la collecte de données : `:sample_frequency`, `:min_wallclock_to_include_in_trace` et `:min_wallclock_to_include_stacks`.

:verbose_request_instrumentation
:verbose_class_instrumentation
:verbose_method_instrumentation
Pour augmenter le niveau de consignation du collecteur des données de diagnostic, affectez à ces propriétés la valeur `true`.

Conseil : Si les opérations que vous voulez tracer ne sont pas incluses dans les traces de pile des méthodes, définissez `:verbose_class_instrumentation => true` et vérifiez le journal pour déterminer si la classe à suivre est instrumentée. Si tel n'est pas le cas, ajoutez le nom de classe du nom du module de la classe à la propriété `:include_subclasses_of_these_modules` property.

4. Si vous avez modifié des propriétés, redémarrez l'application Ruby on Rails correspondante pour appliquer les modifications :

```
:include_subclasses_of_these_modules
:max_methods_to_instrument
```

Le redémarrage est nécessaire, car ces propriétés sont utilisées uniquement lorsqu'une application est lancée pour déterminer la classe ou la méthode que le collecteur des données Ruby doit instrumenter.

- Pour modifier les paramètres du collecteur de données de toutes les applications, procédez comme suit :
  1. Arrêtez les applications Ruby on Rails en cours d'exécution.
  2. Retirez le fichier `instrumer_settings.rb` du répertoire *rép_install*`/install-images/kkm/dchome/`*nom_application*`/config`.
  3. Modifiez les paramètres du collecteur de données dans le fichier *rép_Gem*`/gems/stacktracer-`*version*`/config/instrumenter_settings_template.rb` où *version* correspond au numéro de version, comme 01.00.05.00, et *rép_Gem* au répertoire d'installation de `stacktracer-version.gem`, tel que `/usr/local/rvm/gems/ruby-2.1.4/`. Pour plus d'informations, voir l'étape «3», à la page 741 dans la procédure de modification des paramètres du collecteur de données pour une application spécifique.
  4. Redémarrez les applications Ruby on Rails en cours d'exécution.

Résultats
La configuration du collecteur de données de diagnostic a été modifiée pour l'application en cours d'exécution que vous avez spécifiée ou pour toutes les applications.

Activation du suivi des méthodes et ajustement de l'affichage de chemin
IBM Cloud Application Performance Management, Advanced avec données de diagnostic permet aux utilisateurs de disposer d'un tableau de bord **Traces de demande**. Si les données des méthodes sont collectées, les appels aux méthodes sont affichés. Le widget **Trace des méthodes** affiche les instances de demande et leurs demandes imbriquées. Vous pouvez activer la trace des méthodes pour inclure les appels aux méthodes dans les demandes imbriquées. Vous pouvez également ajuster la configuration du widget **Trace de pile de demande** pour afficher plus de 50 caractères par défaut pour chaque chemin de fichier.

Pourquoi et quand exécuter cette tâche
Le suivi des méthodes est activé par défaut. Exécutez la première procédure pour activer le suivi des méthodes afin de l'afficher dans le tableau **Traces des demandes**. Vous pouvez activer le suivi des méthodes en changeant un paramètre dans le fichier de configuration.

Exécutez la seconde procédure pour ajuster le nombre de caractères indiqué dans le chemin de fichier dans le widget **Trace de pile de demande**.

Procédure

- Pour activer le suivi des méthodes, modifiez les paramètres `instrumenter_settings.rb` :

a) Recherchez le fichier `instrumenter_settings.rb` dans l'installation de l'Agent Ruby, par exemple, *rép_install*`/install-images/kkm/dchome/`*appClassName*`/config` où *appClassName* est le nom de classe d'application Ruby, et *rép_install* est le répertoire d'installation de l'Agent Ruby. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.

b) Ouvrez `instrumenter_settings.rb` dans un éditeur de texte.

c) Affectez la valeur 10000 à la propriété suivante.

```
max_method_to_instrument
```

Cette valeur peut être plus élevée, mais pas trop afin d'éviter une baisse des performances. (Voir aussi «Augmentation de la taille de segment de mémoire de JVM», à la page 744.)

d) Redémarrez les applications Ruby on Rails pour lancer la collecte des données des méthodes.

Pour plus d'informations sur toutes les propriétés `instrumenter_settings.rb`, voir «Configuration du collecteur de données de diagnostic», à la page 741.

- Pour ajuster la taille d'affichage du chemin de fichier dans le widget **Trace de pile de demande**, modifiez le fichier `dfe.properties` :

a) Recherchez le fichier `dfe.properties` dans l'installation de l'Agent Ruby, par exemple, *rép_install*`/lx8266/km/bin/dfe.properties`
où *rép_install* correspond au répertoire d'installation de l'Agent Ruby. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.

b) Ouvrez `dfe.properties` dans un éditeur de texte.

c) Changez la taille maximum du chemin de fichier à afficher dans chaque élément de la trace de pile en ajustant la valeur de la propriété suivante :

```
dfe.stacktrace.filepath.maxsize
```

d) Redémarrez l'Agent Ruby.

Augmentation de la taille de segment de mémoire de JVM

Lorsque la trace des méthodes est activée pour le tableau de bord **Traces des demandes** des diagnostics Ruby, ou que les demandes sont très grandes, vous pouvez augmenter la taille du segment de mémoire pour éviter les erreurs de manque de mémoire.

Pourquoi et quand exécuter cette tâche

L'Agent Ruby est un agent Java et la taille de segment de mémoire de JVM par défaut est de 384 Mo. Pour augmenter la taille de segment et réduire ainsi les risques de saturation de la mémoire, procédez comme suit. L'erreur de saturation de mémoire peut se produire lorsque les demandes de données de grande taille sont fréquentes et que la trace de méthode est activée.

Procédure

1. Recherchez le paramètre de taille de segment JVM dans le répertoire d'installation de l'Agent Ruby, comme *rép_install*`/lx8266/km/bin/runDeepDiveClient.sh`
Où *rép_install* correspond au répertoire d'installation de l'Agent Ruby. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.

   La valeur par défaut est `-Xmx384m`.
2. Augmentez cette valeur jusqu'à 1024 Mo par exemple, comme dans `-Xmx1024m` :
```
export JAVA_OPT="-Djlog.common.dir=$CANDLEHOME/logs -DCONFIG_DIR=
$DC_RUNTIME_DIR -Dkqe.cache.interval=60 -Xmx1024m -Dkqe.timespan=900 -
Djlog.propertyFileDir.CYN=$CANDLEHOME/$ITM_BINARCH/$PRODUCT_CODE/bin"
```
3. Redémarrez l'Agent Ruby.

Désactivation ou activation des données de diagnostic pour les applications Ruby

Si vous disposez d'IBM Cloud Application Performance Management, Advanced, vous pouvez utiliser la page **Configuration d'agent** dans la console Cloud APM pour désactiver ou activer la collecte des données de diagnostic à tout moment pour un ou plusieurs systèmes gérés.

Avant de commencer

- Vous devez disposer de l'outil Cloud APM, Advanced dans votre environnement.
- Vous devez installer et configurer Monitoring Agent for Ruby sur une machine virtuelle, comme indiqué dans «Installation d'agents», à la page 128 sur des systèmes AIX ou «Installation d'agents», à la page 137 sur des systèmes Linux et dans «Configuration de la surveillance de Ruby», à la page 737.
- Vous devez installer le collecteur de données des diagnostic et configurer la prise en charge de la collecte des données de diagnostic, comme indiqué dans «Installation du collecteur de données», à la page 739.

Pourquoi et quand exécuter cette tâche

Une fois que vous avez configuré la prise en charge des données de diagnostic dans la configuration du collecteur de données, la collecte des données de diagnostic est désactivée par défaut pour chaque système géré. Pour afficher des données dans les tableaux de bord de diagnostic, vous devez activer la collecte de diagnostic pour chaque système géré que vous surveillez.

Exécutez les étapes suivantes pour activer et désactiver la collecte de données de diagnostic pour chaque système géré :

Procédure

1. Dans la barre de navigation, sélectionnez **Configuration du système->Configuration d'agent**.
   La page **Configuration d'agent** s'affiche.
2. Cliquez sur l'onglet **Ruby**.
3. Cochez la case des systèmes gérés pour lesquels vous voulez désactiver ou activer la collecte des diagnostics.
4. Dans la liste **Actions**, sélectionnez l'une des options suivantes pour désactiver ou activer la collecte des diagnostics des systèmes gérés sélectionnés :
   - Sélectionnez **`Désactiver la collecte des données`**. Le statut indiqué dans la colonne `Collecte de données activée` est mis à jour et devient `Non` pour chacun des systèmes gérés sélectionnés.
   - Sélectionnez **`Activer la collecte des données`**. Le statut indiqué dans la colonne `Collecte de données activée` est mis à jour et devient `Oui` pour chacun des systèmes gérés sélectionnés.

Résultats

Vous avez configuré la collecte des données de diagnostic pour chacun des systèmes gérés sélectionnés.

Configuration du collecteur de données Ruby pour les applications IBM Cloud

Pour collecter des informations sur les applications Ruby sur IBM Cloud, vous devez configurer le collecteur de données Ruby.

Avant de commencer

1. Téléchargez le package du collecteur de données à partir du site Web IBM Marketplace. Pour des instructions détaillées, voir «Téléchargement de vos agents et de vos collecteurs de données», à la page 105.

Procédure

1. Extrayez les fichiers du package du collecteur de données. Le module `ruby_datacollector_8.1.4.0.tgz` est inclus dans le répertoire extrait.
2. Procédez à l'extraction des fichiers dans `ruby_datacollector_8.1.4.0.tgz` en exécutant la commande suivante :

   ```
   tar -zxf ruby_datacollector_8.1.4.0.tgz
   ```

   Vous obtenez un dossier `ibm_ruby_dc`.
3. Copiez l'intégralité du dossier `etc` dans `ibm_ruby_dc` dans le dossier principal de votre application Ruby en exécutant la commande suivante :

   ```
   cp –r répertoire du dossier etc  répertoire de base de votre application Ruby
   ```

   La commande suivante extrait le collecteur de données dans le répertoire `/opt/ibm/ccm/ibm_ruby_dc/etc` et le répertoire de base de votre application Ruby est `/root/ruby_app/` :

   ```
   cp –r /opt/ibm/ccm/ibm_ruby_dc/etc /root/ruby_app/
   ```
4. Ajoutez la section suivante au fichier `Gemfile` dans le dossier de base de votre application Ruby :

   ```
   gem 'logger',  '>= 1.2.8'
   source 'https://maagemserver.ng.bluemix.net/' do
     gem 'ibm_resource_monitor'
     gem 'stacktracer'
   end
   ```
5. Exécutez la commande `bundle lock` pour régénérer le fichier `Gemfile.lock`.
6. A partir du répertoire qui contient le fichier `manifest.yml` de votre application Ruby, exécutez la commande suivante :

   ```
   cf push
   ```

   Conseil : Pour un fichier `manifest.yml` exemple, voir «Exemple de fichier manifest.yml», à la page 193.

Résultats
Le collecteur de données est configuré et il est connecté au serveur Cloud APM.

Que faire ensuite

Vous pouvez vérifier que les données de surveillance de votre application IBM Cloud sont affichées dans la console Cloud APM. Pour obtenir des instructions de démarrage de la console Cloud APM, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.

Personnalisation du collecteur de données Ruby pour les applications IBM Cloud
Vous pouvez ajouter des variables d'environnement dans l'interface utilisateur IBM Cloud pour personnaliser la surveillance de votre application IBM Cloud. Utilisez les informations suivantes pour ajouter des variables en fonction de vos besoins.

Variables d'environnement définies par l'utilisateur pour le collecteur de données Ruby

Vous pouvez utiliser les informations du tableau suivant pour personnaliser la surveillance de Ruby sur IBM Cloud.

Tableau 198. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance de Ruby sur IBM Cloud

Nom de la variable	Importance	Valeur	Description
APM_BM_GATEWAY_URL	Facultative	• https://*<IP ou nom d'hôte du serveur>*:443 • http://*<IP ou nom d'hôte du serveur>*:80	L'URL de la passerelle de serveur sur site cible.
APM_KEYFILE_PSWD	Facultative	Mot de passe chiffré du fichier de clés	Le mot de passe chiffré du fichier de clés qui est apparié avec le fichier de clés. Si vous êtes un utilisateur Linux, vous pouvez utiliser la commande `echo -n <mot de passe du fichier de clés> | base64` pour chiffrer votre mot de passe. **Remarque :** Définissez cette variable uniquement lorsque vous avez configuré la passerelle pour utiliser HTTPS.
APM_KEYFILE_URL	Facultative	http://*<serveur http hébergé>*:*<port>*/keyfile.p12	L'URL de téléchargement du fichier de clés. **Remarque :** Définissez cette variable uniquement lorsque vous configurez la passerelle pour utiliser HTTPS.
kkm_instrumentation_enabled	Facultative	• true • false	Active ou désactive la collecte des données de diagnostic. true : si vous définissez la valeur sur `true`, les données de diagnostic sont collectées. false : si vous définissez la valeur sur `false`, les données de diagnostic ne sont pas collectées. La valeur par défaut est `true`.

Tableau 198. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance de Ruby sur IBM Cloud (suite)

Nom de la variable	Importance	Valeur	Description
kkm_max_methods_to_instrument	Facultative	Nombre maximal de méthodes tracées	Nombre maximal de méthodes tracées. Vous pouvez désactiver la trace de méthode en définissant la valeur sur `0`. Par défaut, la valeur est `10000` et la trace de méthode est activée. **Remarque :** Il est recommandé de ne pas définir une valeur supérieure à 10000. Une valeur très supérieure à 10000 peut altérer l'efficacité de l'exécution de l'application.
kkm_sample_frequency	Facultative	Fréquence des demandes par échantillonnage	Le nombre de demandes à partir duquel une demande d'échantillon est effectuée, par exemple, si vous définissez la valeur sur `10`, les données de surveillance sont collectées pour une demande sur 10. La valeur par défaut est `10`.
kkm_min_wallclock_to_include_in_trace	Facultative	Seuil de temps de réponse pour collecter la trace de méthode, en secondes	Si le temps de réponse d'une instance de demande dépasse la valeur de cette variable, le collecteur de données collecte sa trace de méthode. Si vous définissez cette variable sur 0,001, par exemple, les demandes et les méthodes dont le temps de réponse est supérieur à 1 milliseconde sont tracés. La valeur par défaut est `0`, ce qui signifie que la trace de méthode est activée pour toutes les demandes et méthodes.

Tableau 198. Variables d'environnement définies par l'utilisateur prises en charge pour la surveillance de Ruby sur IBM Cloud (suite)

Nom de la variable	Importance	Valeur	Description
kkm_min_wallclock_to_include_stacks	Facultative	Seuil de temps de réponse pour collecter la trace de pile, en secondes	Si le temps de réponse d'une instance de demande dépasse la valeur de cette variable, le collecteur de données collecte sa trace de pile. Si vous définissez cette variable sur 0,001, par exemple, les demandes et les méthodes dont le temps de réponse est supérieur à 1 milliseconde sont tracés. La valeur par défaut est `0`, ce qui signifie que la trace de pile est activée pour toutes les demandes et méthodes.

Annulation de la configuration du collecteur de données Ruby pour les applications IBM Cloud
Si vous n'avez pas besoin de surveiller votre environnement Ruby ou si vous souhaitez mettre à niveau le collecteur de données Ruby, vous devez d'abord annuler la configuration des paramètres précédents pour le collecteur de données Ruby.

Procédure

1. Accédez au dossier principal de l'application.
2. Supprimez les lignes suivantes de `Gemfile` dans le dossier de base de votre application Ruby :

```
gem 'logger',  '>= 1.2.8'
source 'https://maagemserver.ng.bluemix.net/' do
  gem 'ibm_resource_monitor'
  gem 'stacktracer'
end
```

3. Exécutez la commande `bundle lock`.
4. A partir du répertoire de base de l'application, exécutez la commande suivante pour renvoyer l'application par push à IBM Cloud afin que les modifications soient prises en compte.

```
cf push
```

Résultats
Vous avez correctement annulé la configuration du collecteur de données Ruby.

Que faire ensuite
Une fois que vous avez configuré le collecteur de données, la console Cloud APM continue d'afficher le collecteur de données dans les applications auxquelles vous l'avez ajouté. La console Cloud APM indique qu'aucune donnée n'est disponible pour l'application et n'indique pas que le collecteur de données est hors ligne. Pour plus d'informations sur la manière de supprimer le collecteur de données d'applications et de groupes de ressources, voir «Suppression de collecteurs de données de la console Cloud APM», à la page 193.

Configuration de la surveillance de SAP

Pour surveiller un système SAP, Monitoring Agent for SAP Applications doit se connecter à un serveur d'applications sur le système à surveiller afin que l'agent puisse accéder au code Advanced Business Application Programming (ABAP) fourni avec le produit.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel en consultant Software Product Compatibility Reports for SAP agent
- L'agent SAP ne prend pas en charge les systèmes SAP non Unicode.

Pourquoi et quand exécuter cette tâche

L'Agent SAP est un agent d'instance multiple. Vous devez créer la première instance et démarrer l'agent manuellement.

- Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser la fenêtre **IBM Performance Management** ou le fichier de réponses silencieux.
  - «Configuration de l'agent sur des systèmes Windows», à la page 751
  - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 753
- Pour configurer l'agent sur des systèmes d'exploitation Linux ou AIX, vous pouvez exécuter le script et répondre aux invites ou utiliser le fichier de réponses silencieux.
  - «Configuration de l'agent sur des systèmes Linux ou AIX», à la page 752
  - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 753

Une fois que vous avez installé l'agent SAP, vous pouvez importer le transport ABAP (Advanced Business Application Programming) sur le système SAP pour prendre en charge la collecte des données sur le système SAP. Pour plus d'informations, voir «Importation du transport ABAP dans le système SAP», à la page 758.

Une fois que vous avez configuré l'agent SAP, vous devez vérifier sa configuration. Pour plus d'informations, voir «Vérification de la configuration de l'agent», à la page 765.

Après avoir configuré l'agent SAP, vous pouvez ajouter le numéro de port de communication de la base de données qui est requis pour la conformité avec OSLC (Open Source Lifecycle Collaboration). Pour plus d'informations, voir «Ajout du numéro de port de communication de base de données», à la page 769.

Pour supprimer le transport ABAP du système SAP, vous devez importer le transport DELETE dans le système SAP. Pour plus d'informations, voir «Suppression du transport ABAP du système SAP», à la page 764.

La nouvelle conception CCMS est activée par défaut. Une entrée est présente dans la table de base de données /IBMMON/ITM_CNGF pour le paramètre isnewccmsdesign dont la valeur est définie sur YES.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'Agent SAP sur des systèmes Windows à l'aide de la fenêtre **IBM Performance Management** afin que l'agent puisse collecter des données à partir du serveur d'applications SAP surveillé.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Modèle** dans la colonne **Tâche/sous-système**, puis sélectionnez **Configurer avec les valeurs par défaut**.

   La fenêtre **Monitoring Agent for SAP Applications** s'affiche.
3. Dans la zone **Enter a unique instance name**, entrez le nom d'instance de l'agent et cliquez sur **OK**.

   Important : Le nom d'instance de l'agent doit correspondre à l'identificateur système (SID) à 3 chiffres du serveur d'applications SAP géré. Par exemple, si l'identificateur système (SID) du serveur d'applications SAP géré est PS1, entrez PS1 comme nom d'instance.
4. Configurez l'Agent SAP en mode Serveur d'applications ou Groupe de connexions.
   - Procédez comme suit pour configurer l'Agent SAP en mode Serveur d'applications :
     a. Dans la zone **Mode de connexion**, sélectionnez **Mode Serveur d'applications** et cliquez sur **Suivant**.
     b. Dans la section **Specify Application Server Information**, indiquez des valeurs pour des paramètres de configuration et cliquez sur **Suivant**.
     c. Dans la zone **Specify Logon Information to the SAP System**, indiquez des valeurs pour les paramètres de configuration et cliquez sur **OK**.

     Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 753
   - Procédez comme suit pour configurer l'Agent SAP en mode Groupe de connexions :
     a. Dans la zone **Mode de connexion**, sélectionnez **Mode Groupe de connexions** et cliquez sur **Suivant**.
     b. Dans la section **Specify Logon Group Information**, indiquez des valeurs pour les paramètres de configuration et cliquez sur **Suivant**.
     c. Dans la zone **Specify Logon Information to the SAP System**, indiquez des valeurs pour les paramètres de configuration et cliquez sur **OK**.

     Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 753

   Important : Pour le mode Serveur d'applications, il est obligatoire de configurer l'instance de boîte de dialogue dont le répartiteur se trouve sur le système SAP où le serveur de messages ou ASCS est configuré. Pour le mode Groupe de connexions, il n'est pas obligatoire de configurer l'instance de boîte de dialogue dont le répartiteur se trouve sur le système SAP où le serveur de messages ou ASCS est configuré.
5. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis cliquez sur **Démarrer**.

   Important : Si vous souhaitez créer une autre instance de l'Agent SAP, répétez les étapes 1 à 6. Utilisez un identificateur système unique pour chaque instance d'Agent SAP que vous souhaitez créer.

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

- Vous devez modifier les situations R3_Alert_Crit et R3_Alert_Warn prédéfinies pour attribuer à la condition de l'attribut Alert Status la valeur `Alert Status!= DONE` pour éviter que ces situations soient déclenchées pour les alertes CCMS fermées.

Configuration de l'agent sur des systèmes Linux ou AIX

Vous pouvez configurer l'Agent SAP sur des systèmes Linux ou AIX pour que l'agent puisse collecter des données du serveur d'applications SAP surveillé.

Procédure

1. Dans la ligne de commande, modifiez le chemin d'accès au répertoire d'installation de l'agent. Exemple : `/opt/ibm/apm/agent/bin`
2. Exécutez la commande suivante, où nom_instance est le nom que vous souhaitez donner à l'instance :

   `./sap-agent.sh config` *`nom_instance`*

   Important : Le nom d'instance de l'agent doit correspondre à l'identificateur système (SID) à 3 chiffres du serveur d'applications SAP géré. Par exemple, si l'identificateur système (SID) du serveur d'applications SAP géré est PS1, entrez PS1 comme nom d'instance.
3. Lorsque la ligne de commande affiche le message suivant, entrez 1 et appuyez sur Entrée : `Edit 'Monitoring Agent for SAP Applications' setting? [1=Yes, 2=No]`
4. Configurez l'Agent SAP à l'aide du mode Serveur d'applications ou du mode Groupe de connexions.
   - Procédez comme suit pour configurer l'Agent SAP en mode Serveur d'applications :
     a. Lorsque la ligne de commande affiche le message suivant, entrez 1 et appuyez sur Entrée : `Connection Mode [ 1=Application Server Mode, 2=Logon Group Mode ]`
     b. Indiquez les valeurs des paramètres de configuration.

     Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 753
   - Procédez comme suit pour configurer l'Agent SAP en mode Groupe de connexions :
     a. Lorsque la ligne de commande affiche le message suivant, entrez 2 et appuyez sur Entrée : `Connection Mode [ 1=Application Server Mode, 2=Logon Group Mode ]`
     b. Indiquez les valeurs des paramètres de configuration.

     Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 753

   Important : Pour le mode Serveur d'applications, il est obligatoire de configurer l'instance de boîte de dialogue dont le répartiteur se trouve sur le système SAP où le serveur de messages ou ASCS est configuré. Pour le mode Groupe de connexions, il n'est pas obligatoire de configurer l'instance de boîte de dialogue dont le répartiteur se trouve sur le système SAP où le serveur de messages ou ASCS est configuré.
5. Exécutez la commande suivante pour démarrer l'Agent SAP :

   `./sap-agent.sh start` *`nom_instance`*

   Important : Si vous souhaitez créer une autre instance de l'Agent SAP, répétez les étapes 1 à 5. Utilisez un identificateur système unique pour chaque instance d'Agent SAP que vous créez.

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.
- Vous devez modifier les situations R3_Alert_Crit et R3_Alert_Warn prédéfinies pour attribuer à la condition de l'attribut Alert Status la valeur `Alert Status!= DONE` pour éviter que ces situations soient déclenchées pour les alertes CCMS fermées.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Vous pouvez configurer l'Agent SAP sur des systèmes Windows, Linux ou AIX à l'aide du fichier de réponses silencieux.

Procédure

1. Dans un éditeur de texte, ouvrez le fichier `sap_silent_config.txt` disponible dans le chemin d'accès *rép_install*`\samples` et indiquez les valeurs pour tous les paramètres de configuration.

   Windows `C:\IBM\APM\samples`

   Linux AIX `/opt/ibm/apm/agent/samples`

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 753
2. Sur la ligne de commande, accédez au répertoire bin :

   Windows *rép_install*`\BIN`

   Linux AIX *rép_install*`\bin`
3. Exécutez la commande suivante :

   Windows `sap-agent.bat config` *nom_instance rép_install*`\samples \sap_silent_config.txt`

   Linux AIX `sap-agent.sh config` *nom_instance rép_install*`\samples \sap_silent_config.txt`

   Important : Le nom d'instance de l'agent doit correspondre à l'identificateur système (SID) à 3 chiffres du serveur d'applications SAP géré. Par exemple, si l'identificateur système (SID) du serveur d'applications SAP géré est PS1, entrez PS1 comme nom d'instance.
4. Démarrez l'agent.

   Windows Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis sur **Démarrer**.

   Linux AIX Exécutez la commande suivante : `./sap-agent.sh start` *nom_instance*

   Important : Si vous souhaitez créer une autre instance de l'Agent SAP, répétez les étapes 1 à 4. Utilisez un identificateur système unique pour chaque instance d'Agent SAP que vous créez.

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.
- Vous devez modifier les situations `R3_Alert_Crit` et `R3_Alert_Warn` prédéfinies pour attribuer à la condition de l'attribut Alert Status la valeur `Alert Status!= DONE` pour éviter que ces situations soient déclenchées pour les alertes CCMS fermées.

Paramètres de configuration de l'agent

Lorsque vous configurez l'Agent SAP, vous pouvez modifier la valeur par défaut des paramètres, comme le nom d'hôte SAP et le numéro de système SAP.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de l'Agent SAP.

Tableau 199. Noms et descriptions des paramètres de configuration de l'Agent SAP

Nom du paramètre	Description	Zone obligatoire	Exemples
SAP Hostname (Primary)	Nom d'hôte du serveur d'applications SAP auquel cet agent se connecte. Si vos serveurs SAP dialoguent à travers un réseau local privé, les ordinateurs hébergeant les serveurs comportent au moins deux cartes de réseau. Pour le nom d'hôte, entrez un nom permettant d'atteindre le serveur d'applications à partir de systèmes externes tels que la connexion SAPGUI. N'utilisez pas le nom d'hôte du réseau LAN privé. Le nom d'hôte par défaut est celui sur lequel l'agent est installé.	Oui	`saphost.domain.com`
SAP System Number (Primary)	Numéro de système SAP ou numéro d'instance à deux chiffres utilisé pour la connexion à un serveur hôte SAP. La valeur par défaut est 00.	Oui	
SAP Hostname (Alternate 1)	(facultatif) Deuxième choix pour le nom d'hôte si l'hôte principal est indisponible.	Non	
SAP System Number (Alternate 1)	Premier numéro de système de remplacement pour le nom d'hôte.	Non	
SAP Hostname (Alternate 2)	Troisième choix pour le nom d'hôte si le nom d'hôte SAP (Principal) et le nom d'hôte SAP de remplacement (Remplacement 1) sont indisponibles.	Non	
SAP System Number (Alternate 2)	Second numéro de système de remplacement pour le nom d'hôte.	Non	
SAP Client Number	Numéro de client SAP pour la connexion RFC à SAP. La valeur par défaut est 000. Si l'utilisateur IBMMON_AGENT généré par ABAP est utilisé, entrez le numéro de client qui a été spécifié dans l'importation de transport. Ce numéro est le même que le numéro de client nnn sous le profil.	Oui	
SAP User Id	Identificateur utilisateur SAP pour la connexion RFC à SAP. La valeur par défaut est IBMMON_AGENT, c'est-à-dire l'ID utilisateur prédéfini qui est créé lors de l'importation.	Oui	
SAP User Password	Utilisez le mot de passe par défaut ou indiquez un mot de passe différent.	Oui	
Confirm SAP User Password	Mot de passe indiqué dans la zone **SAP User Password**.	Oui	

Tableau 199. Noms et descriptions des paramètres de configuration de l'Agent SAP (suite)

Nom du paramètre	Description	Zone obligatoire	Exemples
SAP Language Code	Code de langue qui indique la langue que l'agent utilise lors la connexion au système SAP. La langue indiquée détermine celle dans laquelle s'affichent les informations SAP, comme les messages d'alerte, les messages syslog et les messages du journal des travaux. Tous les systèmes SAP sont fournis en anglais et en allemand. Si vous avez besoin d'une langue différente, vérifiez auprès de votre administrateur SAP que cette langue est installée sur le système SAP. Si vous indiquez une langue qui n'est pas prise en charge, l'agent ne peut pas se connecter au système SAP. Les langues et codes suivants sont pris en charge : • CS - tchèque • EN - anglais • FR - français • DE - allemand • HU - hongrois • IT - italien • ES - espagnol • JA - japonais • KO - coréen • PL - polonais • PT - portugais • RU - russe • ZH - chinois • ZF - chinois traditionnel	Oui	
RFC Trace	Paramètre de trace RFC (Remote Function Call) pour la variable *SAPTRACE*. Lorsque vous cochez cette case, vous activez la fonction de trace RFC et la valeur par défaut est aucun traçage RFC. Pour la ligne de commande, 2 = pas de trace et 1 = trace. Dans la mesure où la fonction de trace RFC génère des informations de diagnostics étendues, utilisez-la soigneusement. Pour plus d'informations sur la fonction de trace RFC, contactez le support IBM.	Non	
SAP Logon Group	Nom du groupe relatif aux connexions de serveur SAP.	Oui	
SAP Message Server Name	Nom d'hôte du serveur de messages SAP.	Oui	

Tableau 199. Noms et descriptions des paramètres de configuration de l'Agent SAP (suite)

Nom du paramètre	Description	Zone obligatoire	Exemples
SAP Message Service	Nom du service où se trouve le serveur de messages SAP. Vous devez inclure les noms de service dans les fichiers de services du système d'exploitation suivants : • `/etc/services` • `\windows\system32\drivers\etc \services`	Oui	Vous pouvez utiliser le nom de service de messages sapmsTV1, ou le numéro de port du service de messages complet 3601.
SAP Route String	Si vous devez accéder au serveur SAP qui utilise un routeur SAP, vous devez indiquer la chaîne du routeur SAP.	Non	La chaîne de routeur `/H/host/H/` doit être au format suivant : `/H/ beagle/H/ brittany/H/` ou `/H/ amsaix11.tivlab. raleigh.ibm.com/W / tivoli/H/amsaix25`
SNC	Indiquez si vous souhaitez activer ou désactiver SNC (Secure Network Communications). La valeur par défaut est Disabled (désactivé).	Oui	**sap_conn.sap_snc_ mode** =`true` ou `false`
SNC Security Level	Niveau de sécurité de SNC.	Oui	**sap_snc_mode1.sap _snc _qop**=*valeur_QOP*. La valeur par défaut est 8.
Client or Agent SNC Name	Nom SNC du client ou de l'agent.	Oui	**sap_snc_mode1.sap _snc _client**= *nom_SNC_client*
Partner or SAP Server SNC Name	Nom SNC du partenaire ou du serveur SAP.	Oui	**sap_snc_mode1.sap _snc _server**= *nom_SNC_serveur*
SAP Cryptolibrary Path	Chemin de la bibliothèque cryptographique SAP.	Oui	**sap_snc_mode1.sap _snc _library**= *Chemin_bibliothèque_cr yptographique*

Le nom d'hôte SAP est tronqué pour respecter les restrictions de longueur de nom du système géré

Le nom du système géré d'une ressource publiée sur la console APM est limité à 32 caractères. L'Agent SAP prend en charge la troncature du nom de domaine afin que le nom du système géré respecte la limite de longueur définie.

Scénario 1

Le nom du système géré du sous-noeud de type **Sys** est au format suivant :

SID-DBHOST:**Sys**
Où :

- *SID* correspond à l'ID du système SAP.
- *DBHOST* correspond au nom d'hôte du système SAP.

Exemple :
Etant donné que *SID* est **P27** et que *DBHOST* est **VPT02F90.mycorporation.co.in**, le nom de domaine complet (FQDN) associé au nom du système géré formé est **P27-VPT02F90.mycorporation.co.in:Sys**.

Lorsque le nom du système géré comporte plus de 32 caractères, l'Agent SAP tronque le nom de domaine, pour que celui-ci devienne **P27-VPT02F90:Sys**. Le nom du système géré tronqué du sous-noeud est alors publié sur la console APM.

Remarque : Si le nom du système géré, nom de domaine compris, a une longueur inférieure ou égale à 32 caractères, le nom de domaine complet n'est pas tronqué. Le nom de domaine complet du nom du système géré est publié sur la console APM.
La troncature du nom de domaine, permettant de respecter la limite de longueur du nom du système géré, s'applique à tous les types de sous-noeud publiés par l'Agent SAP.

Scénario 2

Le nom du système géré pour le sous-noeud de l'instance d'agent **mySAP** est au format suivant :

$SAPSYSTEMNAME-$dbhost:*$CTIRA_HOSTNAME*:**mySAP**
Où :

- *$SAPSYSTEMNAME* est le nom de l'instance d'agent indiqué au cours de la configuration.
- *$dbhost* est le nom d'hôte du système SAP.
- *$CTIRA_HOSTNAME* est le nom d'hôte de la machine de l'agent.

Exemple :
Etant donné que *$SAPSYSTEMNAME* est **SA2**, *$dbhost* est **VPT02F90. mycorporation.co** et que *$CTIRA_HOSTNAME* est **mysap1-v27.mycorp.co**, le nom de domaine complet associé au nom du système géré est **SA2-VPT02F90.mycorporation.co.in: mysap1-v27:mySAP**.

Remarque : Le nom de domaine par défaut du nom d'hôte de la machine de l'agent est tronqué et correspond à **mysap1-v27**.

Le nom du système géré comporte plus de 32 caractères. L'Agent SAP tronque d'abord le nom du domaine associé au nom d'hôte du système SAP pour former **SA2-VPT02F90:mysap1-v27:mySAP**.
Si le nom du système géré obtenu dépasse toujours la limite des 32 caractères, l'Agent SAP tronque les caractères de fin du nom d'hôte de la machine de l'agent. Le nom du système géré du sous-noeud est publié sur la console APM.

Importation du transport ABAP dans le système SAP

Vous pouvez installer un agent Agent SAP pour chaque système SAP sur lequel vous importez la demande de transport ABAP (Advanced Business Application Programming) pour prendre en charge la collecte des données sur le système SAP.

Avant de commencer

Avant d'importer le transport ABAP sur le système SAP, assurez-vous que les prérequis suivants sont respectés :

- Pour importer la demande de transport de produit, R3trans Version 01.07.04 ou ultérieure est requis car les tables Dynpro et Exportation et Importation sont incompatibles. Le fonctionnement de base de l'agent n'est pas affecté par les problèmes d'incompatibilité Dynpro ou Exportation et Importation ; seules les fenêtres de configuration SAP sont affectées.
- Pour surveiller le système Solution Manager, veillez à bien importer le transport Agent SAP version 7.1.1 sur le client où la configuration MAI est disponible. Pour afficher les fonctions du système PI, importez le transport Agent SAP version 7.1.1 sur le système PI sur un client où la configuration PI est disponible.
- Pour afficher les données dans les widgets de groupe qui se trouvent sous le sous-noeud SLM, vous devez effectuer les configurations MAI de PI et Solution Manager. Vous devez également configurer la surveillance des processus métier afin de pouvoir afficher les données dans le widget de groupe Alertes BPM. Pour afficher les données du widget de groupe Dernières alertes critiques et de priorité élevée, procédez aux configurations suivantes :
  - Dans Solution Manager 7.1, exécutez la transaction SOLMAN_SETUP et sélectionnez **System Monitoring**, activez le composant tiers et ajoutez **Implementation: BADI Definition for Alert Reactions** et le connecteur tiers.
  - Définissez le filtre de portée à la valeur **All Alerts and Metrics**.
  - Vérifiez que l'état d'implémentation est **Actif**.

  Pour plus d'informations, reportez-vous aux notes d'OSS (Online Service System) suivantes, qui incluent une liste des niveaux de Service Pack SAP requis :
  - OSS Note 454321
  - OSS Note 330267
  - OSS Note 743155
- Pour surveiller les systèmes SAP, l'Agent SAP a besoin des données statistiques SAP. Sur les systèmes SAP 7.0, vous devez définir le fuseau horaire du système SAP afin qu'il corresponde au fuseau horaire du système d'exploitation, afin que les statistiques SAP soient collectées avec les horodatages adéquats. De même, mettez à jour le fuseau horaire du système SAP pour l'Agent SAP de sorte que ce dernier puisse collecter les données. Pour plus d'informations concernant ce sujet, consultez la note SAP 926290.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur l'importation du transport SAP, voir «Importation du transport SAP», à la page 760.

Prérequis relatifs aux alertes MAI pour l'importation du transport ABAP

Vous devez vérifier les prérequis relatifs aux alertes MAI avant d'importer le transport ABAP.

Paramètres de configuration dans le fichier `transport.prop`

Lorsque vous utilisez le nouveau mécanisme d'extraction des alertes MAI qui permet d'extraire les alertes MAI sans avoir à configurer les paramètres de notification par e-mail et sans implémentation BAdi, vous devez modifier le paramètre de configuration suivant dans le fichier `transport.prop`.

Ajoutez la ligne SPLEVEL=X, où X correspond au niveau de module de support (SP) du système Solution Manager.

Par exemple, si l'ID système est S10 et que le niveau de module de support est 13, ajoutez SPLEVEL=13.

Important : Pour un système SAP avec un niveau SP 10 ou ultérieur, la valeur de l'attribut Technical Name (MEA) n'est pas renseignée dans le widget de groupe Latest MAI Alerts with Rating 'Red' du tableau de bord SAP Solution Manager lorsque les alertes MAI sont extraites sans configurer les notifications par e-mail dans SAP Solution Manager et sans implémentation BAdi. La valeur de l'attribut Technical Name (MEA) est renseignée dans le widget de groupe Latest MAI Alerts with Rating 'Red' du tableau de bord SAP Solution Manager lorsque les alertes MAI sont extraites en configurant les notifications par e-mail dans SAP Solution Manager et l'implémentation BAdi.

Détermination des anciens et des nouveaux mécanismes d'extraction des alertes MAI en fonction du niveau de module de support (SP) Solution Manager

Ancien mécanisme d'extraction des alertes MAI
Ce mécanisme se base sur la configuration des paramètres de notification par e-mail et sur l'implémentation BAdi /IBMMON/ITM_IMPL_ALRTINBX avec l'interface IF_ALERT_DYN_COFIGURATION pour collecter les alertes MAI et les envoyer à l'Agent SAP.

Nouveau mécanisme d'extraction des alertes MAI
Ce mécanisme se base sur l'extraction des alertes MAI sans avoir à configurer les paramètres de notification par e-mail et sans implémentation BAdi /IBMMON/ITM_IMPL_ALRTINBX avec l'interface IF_ALERT_DYN_COFIGURATION.

Vous pouvez utiliser le tableau ci-dessous pour comprendre l'utilisation du fichier `transport.prop` et sa dépendance à la configuration des paramètres de notification par e-mail.

Tableau 200. Utilisation du fichier transport.prop et ses dépendances

Niveau SP du système SAP	Paramètres transport.prop		Configuration des paramètres de notification par e-mail	Mécanisme d'extraction des alertes MAI à utiliser
	MAI_ CONFIGURED	Niveau SP de Solution Manager		
Tous	No ou file does not exist	Non applicable	Configurés ou non	Le sous-noeud SOL apparaît à la place du sous-noeud SLM.
SP 6 à 9	Yes	Mentionné	Configurés	Ancien mécanisme
SP 6 à 9	Yes	Non mentionné	Configurés	Ancien mécanisme
SP 6 à 9	Yes	Non mentionné	Non configurés	L'ancien mécanisme ne fonctionne pas car la configuration des paramètres de notification par e-mail est obligatoire.
SP 6 à 9	Yes	Mentionné	Non configurés	L'ancien mécanisme ne fonctionne pas car la configuration des paramètres de notification par e-mail est obligatoire.
SP 10 ou ultérieur	Yes	Mentionné	Configurés	Nouveau mécanisme

Tableau 200. Utilisation du fichier transport.prop et ses dépendances (suite)				
Niveau SP du système SAP	**Paramètres transport.prop**		**Configuration des paramètres de notification par e-mail**	**Mécanisme d'extraction des alertes MAI à utiliser**
	MAI_ CONFIGURED	**Niveau SP de Solution Manager**		
SP 10 ou ultérieur	Yes	Mentionné	Non configurés	Nouveau mécanisme
SP 10 ou ultérieur	Yes	Non mentionné	Configurés	Ancien mécanisme
SP 10 ou ultérieur	Yes	Non mentionné	Non configurés	L'ancien mécanisme ne fonctionne pas car la configuration des paramètres de notification par e-mail est obligatoire.

Importation du transport SAP
L'Agent SAP fournit un ensemble de routines ABAP (Advanced Business Application Programming) pour prendre en charge la collecte des données dans le système SAP. Ce code ABAP est distribué comme transport SAP qui doit être installé sur chaque système SAP à surveiller. Votre administrateur SAP installe le transport.

Pourquoi et quand exécuter cette tâche

Le profil d'autorisation **ZITM_610AUTH** et le rôle d'autorisation **ZITM_610AUT** ne sont valides que jusqu'à la version 6.1. A partir de la version 6.2 ou d'une version ultérieure, le profil d'autorisation **/ IBMMON/AUTH** est utilisé. Pour se protéger contre une utilisation par une personne non autorisée, le code ABAP qui est installé sur le système SAP n'est pas visible de l'intérieur du système SAP. En outre, ce code ne peut être ni modifié, ni généré. Vous devez obtenir le support de ce code à partir du site Web de support des logiciels IBM.

En plus d'installer le code ABAP, le transport installe également les éléments de texte traduits dans le cadre de la prise en charge multiculturelle des éléments de texte du transport SAP.

Important : Avant d'importer le transport dans le système SAP, vous ne devez pas démarrer l'instance Agent SAP configurée pour surveiller le système SAP.

Lorsque vous importez le transport SAP, les utilisateurs sont définis de manière implicite dans le système SAP.

Procédez comme suit pour importer le transport SAP dans le système SAP.

Procédure

1. Copiez le fichier de transport IBM Tivoli Monitoring à partir des chemins ci-après, sur l'ordinateur où l'agent est installé.
   - Pour les systèmes d'exploitation Windows : *rép_install*\TMAITM6_x64\ABAP
   - Pour les systèmes d'exploitation non Windows : *rép_install*/*intrp*/sa/ABAP, où *intrp* doit être **1x8266** ou **aix526**.
2. Copiez les fichiers de transport suivants des chemins mentionnés à l'étape 1 dans l'environnement SAP :
   - K711_00xxxU.ITM et R711_00xxxU.ITM

Ces fichiers sont des versions Unicode du transfert. Ils contiennent le code ABAP de l'Agent SAP, ainsi que la prise en charge Unicode des chaînes de texte pour les pages de codes latins et les pages de codes sur deux octets.

- K711_00xxx_DELETE.ITM et R711_00xxx_DELETE.ITM

  Ces fichiers suppriment le code ABAP. Il n'est pas nécessaire d'importer le transport DELETE, à moins que vous n'arrêtiez d'utiliser intégralement le produit et que vous souhaitiez supprimer les transports des systèmes SAP. Voir «Suppression du transport ABAP du système SAP», à la page 764.

3. Copiez vos fichiers de transport dans le répertoire de données du système de transport SAP comme indiqué ci-dessous, sans modifier le nom du fichier de transport :

   Transport Unicode

   a. Copiez le fichier K711_00xxxU.ITM dans le répertoire cofiles.
   b. Copiez le fichier R711_00xxxU.ITM dans le répertoire data.

4. Pour installer l'unique fichier de transport IBM Tivoli Monitoring sur le système SAP, sélectionnez l'une des options d'importation de fichier suivantes :

   - Pour le système SAP qui correspond à un niveau Solution Manager 7.1 Service Pack 6 ou ultérieur et pour lequel MAI est configuré, vous devez créer le fichier transport.prop dans le répertoire de travail usr/sap/SID/DVEBMGS*numéro_instance*/work du système SAP. Si le système SAP est un système réparti avec ASCS (ABAP SAP Central Services), créez le fichier transport.prop dans le répertoire usr/sap/SID de l'instance centrale. Ajoutez ensuite l'entrée MAI_CONFIGURED = YES dans ce fichier. Cette entrée crée une entrée MAI_CONFIGURED = YES dans la table /IBMMON/ITM_CNFG. Vous pouvez maintenant importer l'unique fichier de transport IBM Tivoli Monitoring sur le système SAP.

     Remarque : Avant d'importer ce fichier de transport IBM Tivoli Monitoring, vous devez créer le fichier transport.prop dans le répertoire de travail usr/sap/SID/DVEBMGS*numéro_instance*/work du système SAP et ajouter l'entrée MAI_CONFIGURED = YES dans ce fichier. Vous ne devez pas éditer l'entrée dans la table /IBMMON/ITM_CNFG.

   - Pour tous les autres systèmes SAP dont la version de base correspond à la version 7.0 ou une version ultérieure et qui disposent de Solution Manager version 7.1 sans configuration MAI, vous devez importer directement l'unique fichier de transport IBM Tivoli Monitoring.

5. Exécutez la commande suivante pour importer le transport SAP :

   ```
   tp addtobuffer ITMK711_00xxxU SID
   pf=\usr\sap\trans\bin\NOM_PROFIL
   ```

   où :

   SID
   Correspond à l'ID du système SAP cible.

   NOM_PROFIL
   Correspond au nom du fichier de profil tp. Vérifiez que le fichier de paramètres tp actuel est spécifié lorsque vous importez les fichiers de transport d'agent à partir de la ligne de commande. Le fichier de paramètres tp est généralement nommé TP_DOMAIN_*SID*.PFL. Ce nom de fichier est sensible à la casse sous UNIX.

   nnn
   Numéro du client cible sur lequel l'agent est exécuté et pour lequel l'ID utilisateur, IBMMON_AGENT, le profil d'autorisation et /IBMMON/AUTH sont définis.

   Vous pouvez également utiliser la transaction STMS de SAP pour importer les demandes de transport ITMK711_00xxxU.ITM. Vérifiez que les options ci-après sont sélectionnées dans l'onglet **Import Options** de la fenêtre **Import Transport Request**.

   - **Leave Transport Request in Queue for Later Import**
   - **Import Transport Request Again**

- **Overwrite Originals**
- **Overwrite Objects in Unconfirmed Repairs**

  Pour la version de base de SAP, si l'option **Ignore Invalid Component Version** est activée, vérifiez qu'elle est sélectionnée.

Résultats
En fonction du niveau de votre version SAP, lorsque vous exécutez la commande **`tp import`**, vous risquez de recevoir le code retour 4, qui n'indique pas de problème. L'affichage du code retour 4 est le résultat attendu après l'exécution de la commande **`import`**.

Utilisateurs et autorisations nécessaires pour l'Agent SAP
Si vous souhaitez vous protéger contre l'accès non autorisé au système SAP, vous pouvez affecter des autorisations à l'utilisateur qui se connecte à celui-ci. Ces autorisations définissent les niveaux d'accès de l'utilisateur dans le système SAP.

Après l'importation du transport ABAP, l'agent SAP crée l'ID utilisateur par défaut IBMMON_AGENT dans le système SAP ainsi que le mot de passe par défaut ITMMYSAP. Cet utilisateur est un utilisateur système auquel est associé le profil d'autorisation /IBMMON/AUTH. Le profil /IBMMON/AUTH et l'utilisateur IBMMON_AGENT sont créés à l'issue de l'importation du transport ABAP. Avec le profil /IBMMON/AUTH, l'utilisateur IBMMON_AGENT peut accéder aux transactions qui sont nécessaires pour lire les données de performances depuis le système SAP. Voici ci-dessous quelques exemples des transactions utilisées :

- Alertes et administration CDSM
- Autorisation de surveillance des messages PI/XI
- Autorisations Solution Manager

Vous pouvez créer un autre utilisateur de type système pour l'agent. L'utilisateur doit être associé au profil /IBMMON/AUTH.

Pour visualiser les données des composants SAP et y accéder, assurez-vous que l'utilisateur créé pour l'agent dispose de toutes les autorisations mentionnées dans le tableau suivant :

Tableau 201. Liste des autorisations

Composants	Objets d'autorisation	Description de l'autorisation
Autorisations système générales comprenant les composants suivants : • Instance SAP • Système SAP	S_ADMI_FCD	Permet d'accéder au système SAP
	S_BDS_DS -BC-SRV-KPR-BDS	Permet d'accéder à l'ensemble de documents
	S_BTCH_JOB	Permet d'exécuter des opérations sur des travaux en arrière-plan
	S_CCM_RECV	Permet de transférer les données de référentiel du système central
	S_C_FUNCT	Permet d'effectuer des appels aux fonctions de noyau C dans les programmes ABAP
	S_DATASET	Permet d'accéder aux fichiers
	S_RFC	Permet de vérifier l'accès RFC. L'objet d'autorisation S_RFC contient les deux sous-autorisations suivantes : • RFC1 : pour fournir les autorisations pour le groupe de fonctions RFC1. • SDIFRUNTIME : pour fournir les autorisations pour le groupe de fonctions SDIFRUNTIME.
	S_RFCACL	Permet de vérifier l'autorisation des utilisateurs de RFC
	S_RZL_ADM	Permet d'accéder au système CCMS (Computing Center Management System) pour l'administration de R/3 System
	S_TCODE	Permet de vérifier les autorisations de démarrage des transactions qui sont définies pour une application
	S_TOOLS_EX	Permet d'afficher les enregistrements de statistiques externes dans des outils de surveillance
Autorisations pour PI comprenant l'intégration des processus SAP	S_XMB_MONI	Permet d'accéder à XI Message Monitoring

Tableau 201. Liste des autorisations (suite)		
Composants	**Objets d'autorisation**	**Description de l'autorisation**
Autorisations pour MAI comprenant SAP Solution Manager	AI_DIAGE2E	Permet de restreindre les fonctions de diagnostics d'E2E
	AI_LMDB_OB	Permet d'accéder aux objets LMDB (Landscape Management Database)
	SM_MOAL_TC	Permet de contrôler l'accès aux fonctionnalités d'alerte et de surveillance de SAP Solution Manager
	SM_WC_VIEW	Permet de restreindre l'accès aux éléments d'interface utilisateur spécifiques dans les centres de charge de Solution Manager
	S_RFC_ADM	Permet de contrôler les droits d'administration des destinations RFC
	S_RS_AUTH	Permet de spécifier les autorisations d'analyse au sein d'un rôle
	SM_APPTYPE	Permet d'accéder au type d'application Solution Manager
	SM_APP_ID	Permet d'accéder aux applications fournies dans les centres de charge

Suppression du transport ABAP du système SAP

Si vous choisissez de supprimer l'Agent SAP de votre système, vous devez importer le transport DELETE sur le système SAP. Ce transport supprime les objets dictionnaire et modules de fonction de l'Agent SAP.

Avant de commencer

Avant de supprimer le transport du système SAP, vous devez arrêter l'instance Agent SAP configurée pour surveiller le système SAP.

Si le système SAP est de version 7.20 ou ultérieure, avant d'importer le transport DELETE, vous devez ajouter le paramètre de profil de transport **tadirdeletions=true** dans votre profil de transport. Ce paramètre est disponible sur tp version 375.57.68 et également dans R3trans version 6.14 édition 700 ou suivante. Pour plus d'informations sur la suppression de demandes de transport du système SAP, voir Suppression de demandes de transport.

Procédure

1. Accédez au chemin suivant :
   - Pour les systèmes d'exploitation Windows : *rép_install*\TMAITM6_x64\ABAP
   - Pour les systèmes d'exploitation non Windows : *rép_install*/*intrp*/sa/ABAP, où *intrp* doit être **lx8266** ou **aix526**.
2. Copiez les fichiers de transfert dans l'environnement SAP.
3. Copiez les fichiers K711_00xxx_DELETE et R711_00xxx_DELETE dans le répertoire de données du système de transfert SAP, comme suit :

a) Copiez le fichier K711_00xxx_DELETE dans le répertoire cofiles.

b) Copiez le fichier R711_00xxx_DELETE dans le répertoire data.

4. Exécutez les commandes suivantes pour importer le transport DELETE :

a) **tp addtobuffer ITMK711_00xxx_DELETE SID pf=\usr\sap\trans\bin***NOM_PROFIL*

b) **tp import ITMK711_00xxx_DELETE SID client=nnn U16 pf=\usr\sap\trans\bin** *NOM_PROFIL*, où :

SID
Correspond à l'ID du système SAP cible.

NOM_PROFIL
Correspond au nom du fichier de profil tp.

nnn
Correspond au numéro du client cible où l'agent doit être exécuté.

Vérification de la configuration de l'agent

Une fois que vous avez installé l'Agent SAP, vous devez vérifier sa configuration en téléchargeant, en copiant et en vérifiant la bibliothèque NetWeaver RFC SDK V7.20. Vous devez également vérifier la configuration de Solution Manager version 7.1 avec la surveillance MAI, les alertes MAI et le paramètre de configuration spécifique au composant tiers.

Vérifiez la configuration de l'agent à l'aide des procédures suivantes :

- «Téléchargement de la bibliothèque NetWeaver RFC SDK V7.20», à la page 765
- «Copie de la bibliothèque NetWeaver RFC SDK V7.20 dans la configuration de l'agent SAP», à la page 766
- «Vérification de la bibliothèque NetWeaver RFC SDK V7.20», à la page 766
- «Vérification de la configuration de Solution Manager version 7.1 avec la surveillance MAI», à la page 767
- «Vérification des alertes MAI», à la page 768
- «Vérification des paramètres de configuration spécifiques au composant tiers», à la page 768

Téléchargement de la bibliothèque NetWeaver RFC SDK V7.20

Téléchargez la bibliothèque NetWeaver RFC SDK V7.20 une fois l'installation de l'agent SAP terminée. Tous les fichiers liés à la bibliothèque NetWeaver RFC SDK V7.20 peuvent être téléchargés à partir du site Web de SAP.

Procédure

1. Connectez-vous à SAP Marketplace avec l'adresse URL suivante : http://service.sap.com
2. Cliquez sur **SAP Support Portal**.
3. Entrez votre nom d'utilisateur et votre mot de passe Service Marketplace.
4. Cliquez sur **Software Downloads** et développez le lien **Support Packages and Patches**.
5. Cliquez sur **Browse our Download Catalog**, puis cliquez sur **Additional Components**.
6. Cliquez sur **SAP NetWeaver RFC SDK**, puis cliquez sur **SAP NetWeaver RFC SDK 7.20**.
7. Sélectionnez le système d'exploitation sur lequel se trouve l'agent SAP.
8. Téléchargez le fichier *.SAR sur votre ordinateur.
9. Pour extraire le fichier SAP Netweaver RFC SDK *.SAR avec l'utilitaire SAPCAR mis à disposition par SAP, exécutez la commande suivante :
   sapcar -xvf *nom du fichier SAP NetWeaver RFC SDK*.SAR

   Remarque : Vous pouvez télécharger l'utilitaire SAPCAR depuis le site Web SAP.
10. Accédez au dossier lib dans le dossier extrait.

Que faire ensuite

Copiez la bibliothèque NetWeaver RFC SDK V7.20 dans la configuration de l'agent SAP.

Copie de la bibliothèque NetWeaver RFC SDK V7.20 dans la configuration de l'agent SAP
La bibliothèque NetWeaver RFC SDK V7.20 contient des fichiers que vous devez copier manuellement à l'emplacement de la configuration de l'agent SAP.

Procédure

1. Accédez au répertoire dans lequel vous avez téléchargé la bibliothèque NetWeaver RFC SDK V7.20.
2. Copiez les fichiers à l'emplacement de la configuration de l'agent SAP.
   - Pour les systèmes d'exploitation Windows 64 bits, vous devez copier les fichiers suivants :
     - `icuin34.dll`
     - `libicudecnumber.dll`
     - `libsapucum.dll`
     - `icudt34.dll`
     - `icuuc34.dll`
     - `sapnwrfc.dll`

     Vous devez copier les fichiers à l'emplacement `rép_install\TMAITM6_x64`.
   - Pour les systèmes d'exploitation autres que Windows, vous devez copier les fichiers dans `rép_install/`*`intrp`*`/sa/lib`, où *intrp* est le code du système d'exploitation (aix526, li6263, sol606). Vous devez copier les fichiers suivants :
     - `libsapnwrfc.so`
     - `ibicudecnumber.so`
     - `ibicuuc34.a`
     - `libicui18n34.a`
     - `libicudata34.a`
     - `libsapucum.so`

Que faire ensuite

Vérifiez la version de la bibliothèque NetWeaver RFC SDK V7.20 téléchargée.

Vérification de la bibliothèque NetWeaver RFC SDK V7.20
Vous devez vérifier la version du fichier après avoir copié le fichier extrait.

Procédure

- Windows Pour vérifier la version du fichier, procédez comme suit :
  a) Cliquez avec le bouton droit de la souris sur `sapnwrfc.dll`, puis cliquez sur **Propriétés**.
  b) Cliquez sur l'onglet **Version**.
  c) Dans la section **Version du produit**, vérifiez que la version est la suivante : 720, patch 514, changelist 1448293 (ou qu'il s'agit d'une version ultérieure).
- Linux AIX Pour vérifier la version du fichier, procédez comme suit :
  a) Accédez au dossier `lib` dans le fichier `*.SAR` extrait.
  b) Exécutez la commande suivante : **`strings libsapnwrfc.so | grep SAPFileVersion`**
  c) Le message suivant doit s'afficher : `[root@IBMSAP2V6 lib]# strings libsapnwrfc.so | grep SAPFileVersion GetSAPFileVersion #[%]SAPFileVersion: 7200, 514, 22, 6206 .GetSAPFileVersion`

Remarque : Le message indique que la version de cette bibliothèque est la version 720 correctif 514 (ou une version ultérieure).

Vérification de la configuration de Solution Manager version 7.1 avec la surveillance MAI

Afin de recevoir des données pour les alertes MAI, vous devez vérifier que Solution Manager version 7.1 est configuré correctement.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser Solution Manager version 7.1 avec MAI (Monitoring and Alerting Infrastructure) pour surveiller les systèmes gérés. Solution Manager version 7.1 se surveille lui-même ainsi que les systèmes satellites. Chaque système satellite possède un plug-in et des agents de diagnostic. Les agents de diagnostic extraient les données de niveau hôte ou système d'exploitation. Chaque hôte peut posséder plusieurs agents de diagnostic pour différentes instances de Solution Manager surveillant l'hôte. Vous trouverez ci-après les mots clés qui sont utilisés dans la surveillance MAI de Solution Manager :

- Mesures : données provenant des systèmes satellites.
- Alertes : notifications reposant sur des dépassements de valeurs de seuil pouvant être configurées.
- Incident : alertes converties en tickets et affectées à un utilisateur.

Pour vérifier la configuration de Solution Manager version 7.1 avec la surveillance MAI, vous devez vérifier les paramètres de base, les paramètres de niveau global et les paramètres au niveau du modèle.

Procédure

1. Pour vérifier les paramètres de base, entrez le code de transaction SOLMAN_SETUP et appuyez sur **Entrée**.

   Vérifiez que tous les voyants sont verts dans les onglets suivants :

   - Overview
   - Basic Configuration
   - Managed System Configuration

   Remarque : Il existe différentes catégories de systèmes gérés : systèmes techniques, scénarios techniques, hôte, base de données, instance, domaine PI, composant technique et connexion. Vous devez configurer ces systèmes gérés en fonction des besoins métier. Les alertes MAI reposent sur les systèmes gérés que vous avez configurés.
2. Entrez le code de transaction SE38 et appuyez sur **Entrée**.
3. Indiquez le nom de programme RTCCTOOL et exécutez le rapport.

   Vérifiez que tous les voyants sont verts dans la sortie.
4. Pour vérifier les paramètres globaux, entrez le code de transaction : SOLMAN_WORKCENTER et cliquez sur **Entrée**.

   Vérifiez que tous les voyants sont verts dans les onglets suivants :

   - Overview
   - Configure Infrastructure
   - Pre-requisites
   - Configurer
5. Vérifiez si **Global Settings** pour le statut **Notification** est **Active**.
6. Pour vérifier les paramètres au niveau du modèle, entrez le code de transaction SOLMAN_SETUP et cliquez sur **Entrée**.

   Dans **Technical Settings**, dans la liste **Auto-Notifications**, vérifiez que **Active** est sélectionné.

   Remarque : Pour un traitement initial des incidents, vérifiez que les notifications par courrier électronique sont actives.

7. Pour la surveillance de système MAI, vérifiez la configuration d'End-User Experience Monitoring (EEM) en procédant comme suit :
   a) Entrez le code de transaction SE37 et appuyez sur **Entrée**.
   b) Entrez **AI_EEM_LIST_ALL_SCENARIOS** dans la zone **Function Module name** et appuyez sur F8.
      Une entrée pour End-User Experience Monitoring (EEM) doit exister.

Vérification des alertes MAI
Pour vous assurer que l'infrastructure MAI de Solution Manager est configurée correctement pour la surveillance de la boîte de réception des alertes MAI dans Technical Monitoring, vous devez vérifier que vous recevez les alertes MAI dans la sortie.

Procédure

1. Entrez le code de transaction SOLMAN_WORKCENTER et appuyez sur **Entrée**. Vérifiez si vous pouvez afficher les alertes MAI dans la boîte de réception des alertes MAI de Solution Manager, sous Technical Monitoring.
2. Recherchez l'implémentation BADI en procédant comme suit :
   a) Entrez le code de transaction SE19 et appuyez sur **Entrée**.
   b) Entrez /IBMMON/ITM_IMPL_ALRTINBX dans la zone **Enhancement Implementation**.
   c) Cliquez sur **Display** et vérifiez si l'implémentation BADI est active dans la section **Runtime Behavior**.
3. Vérifiez si la base de données /IBMMON/ITM_ALIX contient des alertes MAI, à l'aide des étapes suivantes :
   a) Entrez le code de transaction SE16 et appuyez sur **Entrée**.
   b) Dans la zone **Table Name**, entrez /IBMMON/ITM_ALIX et exécutez cette commande. Vérifiez que vous recevez les alertes MAI dans la table.
4. Entrez le code de transaction SE37 et appuyez sur **Entrée**.
5. Dans la zone **Function Module Name**, entrez /IBMMON/ITM_MAIALRT_INX et appuyez sur F8.
   Vous devez voir les alertes MAI dans la sortie.

Que faire ensuite
Si vous ne parvenez pas à voir les alertes MAI dans la base de données /IBMMON/ITM_ALIX, vous devez vérifier les paramètres dans le composant tiers.

Vérification des paramètres de configuration spécifiques au composant tiers
Si vous ne parvenez pas à voir les alertes MAI, vous devez vérifier les paramètres dans le composant tiers.

Procédure

1. Vérifiez que le composant tiers est actif.
2. Vérifiez que **Alert Reaction** est disponible dans **OS Adapter**, sous **BAdi Implementation**. Si tel n'est pas le cas, supprimez les paramètres par défaut et sélectionnez **BAdi implementation - Alert Reaction**.
3. Vérifiez les paramètres du modèle en procédant comme suit :
   a) Vérifiez les paramètres utilisés pour transférer des alertes spécifiques sur le système tiers, tel que SAP ABAP 7.0.0.
   b) Sélectionnez **Expert Mode**, sélectionnez **Alerts**, puis cliquez sur **Third Party Component**.
      Vérifiez que le nom Alert Reaction BAdi s'affiche.

      Remarque : Vérifiez que les notes SAP les plus récentes sont implémentées. Pour Solution Manager version 7.1 Service Pack 8, vérifiez que les notes suivantes sont implémentées :

      - https://service.sap.com/sap/support/notes/1959978
      - https://service.sap.com/sap/support/notes/1820727

4. Si vous ne parvenez pas à voir les alertes MAI dans la base de données /IBMMON/ITM_MAIALRT_INX, vous devez exécuter les étapes de configuration de Solution Manager MAI pour le composant tiers.
   a) Entrez le code de transaction SOLMAN_SETUP et appuyez sur **Entrée**.
   b) Dans **Technical Monitoring**, sélectionnez **System Monitoring**.
   c) Cliquez sur l'onglet **Configure Infrastructure**, puis sur l'onglet **Default Settings**.
   d) Cliquez sur l'onglet **Third Party Components**, puis cliquez sur **Edit**.
   e) Sélectionnez **Active** dans la liste.
   f) Vérifiez que le filtre de portée a pour valeur **All alerts, Events and Metrics (with Internal Events)** pour le connecteur sélectionné.

      Remarque : L'adaptateur de commande de système d'exploitation est également l'une des méthodes permettant d'envoyer des données au connecteur tiers. Pour le configurer, reportez-vous aux paramètres détaillés de la configuration dans le guide d'utilisation de l'adaptateur de commande de système d'exploitation.

Ajout du numéro de port de communication de base de données

Un numéro de port de communication de base de données est essentiel pour identifier de manière unique l'entité de base de données dans les scénarios intégrés. Pour assurer la collaboration inter-composant, les composants de SCM AI comprennent OSLC (Open Source Lifecycle Collaboration). Pour la conformité OSLC, il est essentiel d'identifier les composants de collaboration de manière unique. C'est la raison pour laquelle le numéro de port de communication de base de données est important.

Pourquoi et quand exécuter cette tâche

Lorsque vous importez le transport IBM Tivoli Monitoring approprié dans le système SAP, la table de base de données /IBMMON/ITM_PORT est créée automatiquement. Cette dernière contient les zones de base de données suivantes :

- ID système
- Nom d'hôte du système
- Numéro de port de communication de base de données

Procédure

Pour ajouter le numéro de port de communication de base de données pour l'Agent SAP qui est requis pour la conformité OSLC, procédez comme suit :

1. Accédez au code de transaction SE16 et appuyez sur la touche Entrée.
2. Dans la zone **Nom de table de base de données**, entrez /IBMMON/ITM_PORT et appuyez sur la touche F7.
3. Lorsque l'écran de sélection de la table de base de données **/IBMMON/ITM_PORT** apparaît, appuyez sur la touche F8.

   La table de base de données **/IBMMON/ITM_PORT** contient les trois zones de base de données suivantes :

   - ID système
   - Nom d'hôte du système
   - Numéro de port de communication de base de données

   Remarque : Les systèmes SAP qui apparaissent dans la table de base de données /IBMMON/ITM_PORT sont destinés à la fois aux architectures Java et ABAP.
4. Dans la zone **Numéro de port de communication de base de données**, entrez le numéro de port de communication de base de données SAP approprié pour l'ID système SAP et le nom d'hôte système SAP respectif et sauvegardez les modifications.

   Remarque : Si vous n'entrez pas de valeur dans la zone **Numéro de port de communication de base de données** dans la table de base de données /IBMMON/ITM_PORT, celui-ci a la valeur par défaut 0.

Installation et configuration avancées de l'agent SAP

La présente section décrit l'installation et la configuration avancées spécifiques à l'Agent SAP.

Les rubriques d'installation et de configuration suivantes y sont traitées :

- «Module de fonction SAP», à la page 770
- «ID utilisateur SAP», à la page 771
- Utilitaires de l'Agent SAP
- «Connexions RFC SAP», à la page 771
- «Fonction de test de connexion», à la page 782
- «Configuration avancée facultative dans SAP», à la page 774
- «Génération d'états du CCMS CEN», à la page 780
- «Désinstallation du transport ABAP (Advanced Business Application Programming) sur le système SAP», à la page 782

Remarque : La section traitant de l'installation et de la configuration avancées de l'Agent SAP contient des références à IBM Tivoli Monitoring afin que la documentation soit compatible avec l'interface utilisateur du code de transaction personnalisé pour le transport ABAP.

Module de fonction SAP

Lorsque le volume de données est élevé sur le serveur SAP, il est possible que vous rencontriez des problèmes avec certains widgets provoquant un temps de réponse lent du serveur. Si les widgets ne sont pas critiques, vous pouvez désactiver le module de fonction SAP associé.

Par défaut, les modules de fonction de l'Agent SAP sont activés. Cependant, les modules de fonction suivants sont désactivés par défaut :

- Services HTTP sous le sous-noeud SYS (`/IBMMON/ITM_HTTP_SRVS`)
- Messages XML sous le sous-noeud PI/XI (`/IBMMON/ITM_SXMB_MONI_NEW`)
- Communication synchrone/asynchrone sous le sous-noeud PI/XI (`/IBMMON/ITM_SYN_ASYN_COMM`)
- Détails de la file d'attente entrante qRFC sous le sous-noeud Sys (`/IBMMON/ITM_QIN_QDETAILS`)

Après avoir désactivé le module de fonction SAP, si vous sélectionnez un widget, les données ne s'affichent pas sur le tableau de bord IBM Application Performance Management. Par conséquent, vous évitez tous les problèmes relatifs aux performances.

Activation du module de fonction de l'agent SAP

Si vous avez déjà désactivé le module de fonction de l'Agent SAP pour résoudre les problèmes de performances, vous pouvez également activer le module de fonction.

Procédure

1. Connectez-vous au système SAP.
2. Exécutez le code de transaction SE16.
3. Entrez le nom de table `/IBMMON/ITM_CNFG`.
4. Sélectionnez la ligne à supprimer et appuyez sur **Maj + F2** pour supprimer l'entrée.
5. Cliquez sur **Sauvegarder**.

Désactivation du module de fonction SAP

Certains widgets peuvent provoquer une réponse lente depuis le serveur SAP. Vous pouvez ainsi désactiver le module de fonction SAP pour améliorer les performances du serveur.

Procédure

1. Connectez-vous au système SAP.
2. Exécutez le code de transaction SE16.

3. Entrez le nom de table /IBMMON/ITM_CNFG.
4. Appuyez sur **F5** pour créer une entrée.
5. Entrez le nom du module de fonction SAP dans la zone **PARM NAME**.
6. Entrez No dans la zone **VALUE CHAR**.
7. Cliquez sur **Sauvegarder**.

ID utilisateur SAP
La présente section fournit des informations sur les ID utilisateur et les droits SAP requis par l'Agent SAP.

Les ID utilisateur sont utilisés aux fins suivantes :

- «Connexions RFC SAP», à la page 771
- «Surveillance de l'agent de base», à la page 771

Connexions RFC SAP
L'Agent SAP utilise les connexions Remote Function Calls (RFC) pour l'interrogation interne de CCMS et la collecte des données d'alerte CCMS. Ce comportement est particulier à l'architecture RFC SAP.

L'Agent SAP ouvre une connexion RFC dédiée vers le système SAP qui est surveillée par l'agent. Le système SAP ouvre alors une connexion interne par serveur d'applications pour la collecte de données à l'aide des programmes et modules de fonction. Si des alertes du CCMS sont en cours de collecte par l'agent, le système SAP ouvre une connexion RFC supplémentaire (interne au système) pour chaque serveur d'applications de cette unité d'exécution de collecte. Ainsi, lorsque la collecte de données démarre, une connexion RFC pour l'agent est ouverte. Ainsi, un nombre de connexions représentant jusqu'à deux fois le nombre de serveurs d'applications SAP pour des connexions RFC supplémentaires du système interne est ouvert.

Vous devez veiller à ce que l'instance réalisant la surveillance puisse recevoir les sessions RFC supplémentaires, notamment sur de gros systèmes à 10 instances ou plus. Si la charge RFC prévue pour la surveillance risque de nuire aux performances et tolérances du système, ajustez le paramètre de profil SAP comme il convient. Consultez votre administrateur SAP et les documents SAP suivants :

- Sessions de terminal (valeur implicite : 200) 22099
- Paramètres de communication/passerelle/conversation 887909 316877 384971

Surveillance de l'agent de base
L'Agent SAP crée un IBMMON_AGENT dans le système SAP lorsque le transfert d'agent est importé.

Cet ID utilisateur est IBMMON_AGENT avec le mot de passe par défaut ITMMYSAP. Il est préconfiguré pour un utilisateur de type communication uniquement et pour utiliser le profil d'autorisation /IBMMON/AUTH. Ce profil, qui est créé lors de l'importation du transfert, contient l'ensemble de droits minimum pour exécuter le code ABAP d'agent. De plus, ce profil accepte un ensemble d'actions limitées sur votre système SAP.

Si ce nom d'ID utilisateur n'est pas admissible, par exemple s'il viole les conventions de dénomination de votre installation, vous pouvez créer un ID utilisateur différent. L'ID utilisateur peut être tout ID utilisateur SAP autorisé, mais il nécessite l'ensemble complet des droits dans le profil /IBMMON/AUTH. L'ID utilisateur exige un accès utilisateur de type communication uniquement.

L'ID utilisateur par défaut offre uniquement des droits d'accès suffisants pour les buts suivants :

- Surveillance et collecte de données
- Fermeture des alertes de Computing Center Management System (CCMS)
- Activation, désactivation et réinitialisation des statistiques de la passerelle
- Réinitialisation des statistiques de la base de données Oracle

Si vous choisissez de limiter les fonctionnalités d'action de l'agent, vous pouvez supprimer certains droits d'action tels que la fermeture des alertes du CCMS.

Pour accéder aux données de certains composants sur le portail de l'interface utilisateur IBM Application Performance Management, assurez-vous de disposer des autorisations appropriées. Le tableau ci-

dessous répertorie les autorisations requises pour accéder aux données à partir de différents sous-noeuds :

Tableau 202. Liste des autorisations

Sous-noeuds	Objets d'autorisation	Description de l'autorisation
Autorisations système générales incluant les sous-noeuds suivants : • Ins • Sys	S_ADMI_FCD	Permet d'accéder au système
	S_BDS_DS -BC-SRV-KPR-BDS	Permet d'accéder à l'ensemble de documents
	S_BTCH_JOB	Permet d'exécuter des opérations sur des travaux en arrière-plan
	S_CCM_RECV	Permet de transférer les données du référentiel système central
	S_C_FUNCT	Permet d'effectuer des appels C dans les programmes ABAP
	S_DATASET	Permet d'accéder aux fichiers
	S_RFC	Permet de vérifier l'accès RFC. L'objet d'autorisation S_RFC contient les deux sous-autorisations suivantes : • RFC1 : pour fournir les autorisations pour le groupe de fonctions RFC1. • SDIFRUNTIME : pour fournir les autorisations pour le groupe de fonctions SDIFRUNTIME.
	S_RFCACL	Pour l'utilisateur RFC
	S_RZL_ADM	Permet d'accéder à CCMS (Computing Center Management System) : Administration de système
	S_TCODE	Permet de vérifier le code de transaction au démarrage de la transaction
	S_TOOLS_EX	Permet d'accéder à Tools Performance Monitor

Tableau 202. Liste des autorisations (suite)

Sous-noeuds	Objets d'autorisation	Description de l'autorisation
Autorisations pour Solution Manager incluant les sous-noeuds suivants : • Lds • Sol	D_MD_DATA -DMD	Permet d'afficher le contenu de données de données maître
	D_SOLMANBU	Permet d'accéder à un type de session de Solution Manager
	D_SOLM_ACT	Permet d'accéder à une solution dans Solution Manager
	D_SOL_VSBL	Permet d'afficher une solution dans Solution Manager
	S_CTS_SADM	Permet d'afficher l'administration propre au système (transport)
	S_TABU_RFC	Permet d'afficher la copie et la comparaison de client : exportation des données avec RFC
Autorisations pour PI incluant le sous-noeud PI	S_XMB_MONI	Permet d'accéder à XI Message Monitoring
Autorisations pour MAI incluant le sous-noeud Slm	AI_DIAGE2E	Permet d'accéder à l'analyse de bout en bout Solution Diagnostics
	AI_LMDB_OB	Permet d'accéder aux objets LMDB (Landscape Management Database)
	SM_MOAL_TC	Permet d'accéder à Monitoring and Alerting
	SM_WC_VIEW	Permet d'accéder aux éléments d'interface utilisateur du centre de travail
	S_RFC_ADM	Permet d'accéder aux options d'administration pour la destination RFC
	S_RS_AUTH	Permet d'accéder à l'analyse BI dans le rôle
	SM_APPTYPE	Permet d'accéder au type d'application Solution Manager
	SM_APP_ID	Permet d'accéder aux applications fournies dans le centre de travail

Utilisation de Central User Administration (CUA)
Central User Administration (CUA) permet de surveiller un système SAP.

Procédure

Si vous voulez utiliser l'ID utilisateur et le rôle d'autorisation prédéfinis pour surveiller un système SAP configuré avec la gestion centrale des utilisateurs, exécutez l'une des étapes suivantes :

- Installez le transfert dans le client de système logique père de la gestion centrale des utilisateurs.

- Créez manuellement l'ID utilisateur ou rôle dans le client sur lequel vous voulez installer le transfert. L'ID utilisateur ou rôle est dans le client où le transfert est installé (importé).
- Créez manuellement l'ID utilisateur ou rôle dans le client de système logique parent de la gestion centrale des utilisateurs. Distribuez ensuite l'ID utilisateur ou le rôle au client sur lequel l'agent s'exécute.
- Créez manuellement l'ID utilisateur ou rôle dans le client de système logique père de la gestion centrale des utilisateurs et exécutez l'agent dans ce client.

Configuration avancée facultative dans SAP
Vous pouvez configurer l'Agent SAP à l'aide des fonctions SAP standard ou fournies par l'agent.

Utilisez les transactions fournies par l'agent de SAP pour personnaliser un certain nombre de comportements d'agent. Après l'exécution de la transaction `/n/IBMMON/ITM_CONFIG` pour accéder au menu de configuration principal dans SAP, sélectionnez l'une des options de configuration suivantes :

- «Fonction et transactions de copie, sauvegarde et restauration», à la page 774
- «Copie, sauvegarde et restauration des données à l'aide de transactions», à la page 775
- «Utilitaire de ligne de commande», à la page 776
- «Exécution de l'utilitaire de ligne de commande dans un environnement Windows», à la page 776
- «Exécution de l'utilitaire de ligne de commande dans un environnement non Windows», à la page 777
- «Maintenance des alertes», à la page 777
- «Sélection des ensembles de surveillance et des transactions de surveillance», à la page 778
- «Configuration du seuil de réponse d'étape de boîte de dialogue dans le système SAP», à la page 779

Remarque : Toutes les transactions `/IBMMON/ITM*` doivent être précédées de `/n`.

Les modifications de configuration effectuées dans ces transactions sont immédiatement utilisées par l'Agent SAP, à l'exception des modifications effectuées pour la mise à jour des groupes gérés. Lorsque la configuration du groupe géré a été modifiée, les modifications sont découvertes par l'Agent SAP à la prochaine pulsation.

Utilisez les fonctions SAP standard pour effectuer la configuration suivante : «Configuration du seuil de réponse d'étape de boîte de dialogue dans le système SAP», à la page 779

Fonction et transactions de copie, sauvegarde et restauration
Les fonctions de copie, sauvegarde et restauration sont disponibles une fois que vous vous êtes connecté au serveur SAP et que vous avez exécuté la transaction suivante : `/n/IBMMON/ITM_CONFIG`.

Les opérations de copie, sauvegarde et restauration vous permettent de copier, sauvegarder et restaurer les données de configuration d'IBM Tivoli Monitoring.

Utilisez cette fonction pour sélectionner et pour sauvegarder les données de configuration IBM Tivoli Monitoring :

- **Copier**

  Utilisez cette fonction pour copier les paramètres de configuration IBM Tivoli Monitoring à partir d'un serveur SAP vers un autre serveur SAP. Par exemple, il est possible que vous vouliez copier les paramètres de configuration IBM Tivoli Monitoring à partir de l'agent **a1** vers SAP server instance SAP2. Cet agent s'exécute sur le système **m1** et est configuré pour l'instance de serveur SAP SAP 1. Tous les paramètres de configuration IBM Tivoli Monitoring, sauf les paramètres de surveillance de l'instance du serveur SAP, sont copiés dans le système SAP cible. Vous implémentez la fonction de copie à l'aide de l'utilitaire de ligne de commande ou de l'interface utilisateur SAP.

- **Sauvegarder**

  Vous pouvez stocker les configurations spécifiques à l'agent que vous avez terminées sur le serveur SAP en procédant à une sauvegarde du système. Utilisez cette fonction pour sauvegarder les paramètres de configuration spécifiques à IBM Tivoli Monitoring sur le système SAP. Utilisez la transaction `/IBMMON/ITM_CONFIG` pour saisir les paramètres. Le fichier de sauvegarde est stocké dans le répertoire de travail sur le serveur SAP au chemin suivant : `/usr/sap//DVEBMGS/work`.

- **Restaurer**

  Utilisez cette fonction pour restaurer les données de configuration IBM Tivoli Monitoring sur le serveur SAP à partir du répertoire de travail. Vous pouvez restaurer les données de configuration d'IBM Tivoli Monitoring sur le même serveur SAP que celui sur lequel vous avez effectué la procédure de sauvegarde de ces données de configuration ou sur un autre serveur SAP. Vous pouvez restaurer les données de configuration d'IBM Tivoli Monitoring vers un serveur SAP spécifique et des tables IBM Tivoli Monitoring. Les fichiers de configuration sont stockés avec une date et une heure, vous pouvez donc sélectionner le point à partir duquel vous souhaitez restaurer vos fichiers.

Les configurations spécifiques à l'agent comprennent des paramètres de configuration dans la transaction `/IBMMON/ITM_CONFIG` dans SAP. Vous pouvez effectuer les procédures de configuration suivantes :

- Echantillonnage de la fréquence pour les alertes.
- Activation d'alertes spécifiques.
- Stockage des noms de fichier journal.
- Gestion des définitions de groupe.
- Sélection des ensembles de surveillance et des surveillances.
- Sélection des instances SAP à des fins de surveillance.

Copie, sauvegarde et restauration des données à l'aide de transactions
Dans l'interface utilisateur SAP, vous pouvez copier, sauvegarder et restaurer des données à l'aide de la transaction n`/IBMMON/ITM_CONFIG` .

Avant de commencer
Utilisez les procédures de copie, sauvegarde et restauration pour copier les paramètres de configuration d'IBM Tivoli Monitoring d'un serveur SAP vers un autre serveur SAP. Tous les paramètres de configuration IBM Tivoli Monitoring, à l'exception des paramètres de surveillance de l'instance du serveur SAP sont copiés sur le système SAP cible.

Procédure

Exécutez la procédure suivante pour copier, sauvegarder et restaurer vos données sur SAP :

- **Copier**
  a. Entrez l'ID du système SAP cible et le nom du fichier existant au format `source system id__<filenam>date_time`.

     La transaction `/IBMMON/ITM_COPY` crée un fichier de configuration IBM Tivoli Monitoring dans le répertoire de travail sous le nom SAP `target SAP system id__<filename>_date_time`.
  b. Cliquez sur **Exécuter** pour copier les données de configuration IBM Tivoli Monitoring dans le fichier.
  c. Cliquez sur **Précédent** ou sur **Annuler** pour revenir à l'écran de configuration d'IBM Tivoli Monitoring précédent.

     Les paramètres d'entrée attendus qui doivent être copiés sont **`Target System id`** et **`filename`**.
- **Sauvegarder**
  a. Connectez-vous au serveur SAP et démarrez la transaction `/IBMMON/ITM_CONFIG`.
  b. Sélectionnez **Sauvegarder**.
  c. Entrez le nom du fichier de sauvegarde.

     Le nom du fichier est stocké au format `sys_id_<filename>_date_time`.
  d. Cliquez sur **Exécuter** pour effectuer la sauvegarde et stocker le fichier sur le serveur d'applications.

     Remarque : Le fichier de sauvegarde est stocké dans le répertoire de travail du serveur d'applications.

e. Cliquez sur **Précédent** ou sur **Annuler** pour revenir à l'écran de configuration d'IBM Tivoli Monitoring précédent.

- **Restaurer**

a. Connectez-vous au serveur SAP et démarrez la transaction `/IBMMON/ITM_CONFIG`.

b. Sélectionnez **Restaurer**.

c. Entrez le nom du fichier à restaurer au format `sys_id_<filename>_date_time`.

d. Cliquez sur **Exécuter** pour restaurer les données de configuration IBM Tivoli Monitoring.

e. Cliquez sur **Précédent** ou sur **Annuler** pour revenir à l'écran de configuration d'IBM Tivoli Monitoring précédent.

Utilitaire de ligne de commande

Vous pouvez utiliser l'utilitaire de ligne de commande pour copier, sauvegarder et restaurer les données de configuration IBM Tivoli Monitoring sur le serveur SAP.

Vous pouvez exécuter l'utilitaire de ligne de commande dans un environnement Windows et non Windows. Voir «Exécution de l'utilitaire de ligne de commande dans un environnement Windows», à la page 776 et «Exécution de l'utilitaire de ligne de commande dans un environnement non Windows», à la page 777.

- **Copier**

  Exécutez la commande **backup** pour copier le fichier de configuration IBM Tivoli Monitoring de l'instance du serveur SAP du répertoire de l'agent sap1 vers sap2. Entrez le nom du fichier et sap1 comme système source à partir du répertoire de l'agent sap1. La fonction ABAP est ensuite appelée et copie les paramètres IBM Tivoli Monitoring de ce fichier vers le fichier de configuration IBM Tivoli Monitoring pour Sap2. Sélectionnez à présent **`Copier`** à partir de l'utilitaire du répertoire de l'agent sap1 et entrez un nom de fichier et sap2 comme système SAP cible.

- **Sauvegarder**

  Après avoir exécuté l'utilitaire de ligne de commande, sélectionnez l'option **Sauvegarder**. Vous devez ensuite entrer le nom du fichier et l'ID du système SAP. L'outil appelle le module de fonction SAP `/IBMMON/ITM_BACKUP`. Le module de fonction lit les paramètres de configuration IBM Tivoli Monitoring spécifiques stockés dans des tableaux et les stocke avec un séparateur de ligne et de colonne. L'utilitaire de ligne de commande lit ensuite la chaîne et écrit les données dans un fichier. Le nom du fichier qui est généré a le format suivant : ID>_<filename>-<date&time>. Ce fichier est stocké dans le répertoire dans lequel le programme utilitaire est stocké.

- **Restaurer**

  Après avoir exécuté l'utilitaire de ligne de commande, entrez le nom du fichier à restaurer et le système SAP cible sur lequel vous voulez restaurer le fichier. L'utilitaire de ligne de commande lit le fichier à partir du répertoire de l'agent et appelle le module de fonction SAP `/IBMMON/ITM_RESTORE`. L'utilitaire transmet ensuite les configurations IBM Tivoli Monitoring sous forme de chaîne. Le module de fonction SAP met à jour les tables IBM Tivoli Monitoring spécifiques et restaure les configurations IBM Tivoli Monitoring correspondantes.

Exécution de l'utilitaire de ligne de commande dans un environnement Windows

Vous pouvez exécuter l'utilitaire de ligne de commande dans un environnement Windows pour effectuer des procédures de copie, de sauvegarde et de restauration.

Procédure

1. En fonction de votre système d'exploitation, exécutez l'une des actions suivantes :
   - Pour un système d'exploitation 64 bits, définissez le chemin CANDLEHOME à l'aide de la commande **`set CANDLE_HOME = C:\IBM\APM`** et exécutez la commande **`ksacopybackuprestore.bat`** à partir du chemin suivant : `%candle_home%\ TMAITM6x64`.
2. Pour créer un fichier de sauvegarde, procédez comme suit :
   a) Sélectionnez **Sauvegarder** et entrez le nom du fichier et le nom du système SAP source.

b) Le fichier de sauvegarde est créé avec le format suivant : SYS ID>_<filename>_<date&time>.

3. Pour restaurer le fichier, procédez comme suit :
   a) Sélectionnez **Restaurer** et entrez le nom du système SAP cible.
   b) Entrez le nom du fichier.
4. Pour copier le fichier, procédez comme suit :
   a) A partir de l'agent source, sélectionnez **Sauvegarder** et créez un fichier de sauvegarde.
   b) Copiez le fichier de sauvegarde deu répertoire de l'agent source vers le répertoire de l'agent cible.
   c) A partir du répertoire source, exécutez l'utilitaire de ligne de commande et sélectionnez **Copier**.
   d) Entrez le nom du fichier et le système SAP cible.

Exécution de l'utilitaire de ligne de commande dans un environnement non Windows
Vous pouvez exécuter l'utilitaire de ligne de commande dans un environnement non Windows pour effectuer des procédures de copie, de sauvegarde et de restauration.

Procédure

1. Exécutez la commande **ksacopybackuprestore.sh** à partir du chemin suivant : `/candle_home/<arch>/sa/shell`.
2. Pour créer un fichier de sauvegarde, procédez comme suit :
   a) Sélectionnez **Sauvegarder** et entrez le nom du fichier et le nom du système SAP source.
   b) Le fichier de sauvegarde est créé avec le format suivant : SYS ID>_<filename>_<date&time>.
   Le fichier de sauvegarde est enregistré à cet emplacement : `%candlehome% / arch /sa/bin`.
3. Pour restaurer le fichier, procédez comme suit :
   a) Sélectionnez **Restaurer** et entrez le nom du système SAP cible.
   b) Entrez le nom du fichier.
4. Pour copier le fichier, procédez comme suit :
   a) A partir de l'agent source, sélectionnez **Sauvegarder** et créez un fichier de sauvegarde.
   b) Copiez le fichier de sauvegarde deu répertoire de l'agent source vers le répertoire de l'agent cible.
   c) A partir du répertoire source, exécutez l'utilitaire de ligne de commande et sélectionnez **Copier**.
   d) Entrez le nom du fichier et le système SAP cible.

Maintenance des alertes
Vous pouvez modifier les alertes qui sont générées par Tivoli Monitoring en modifiant leur statut et leurs seuils.

Cette transaction est utilisée pour activer ou désactiver les alertes générées par Tivoli Monitoring et pour définir des seuils d'avertissement et des seuils critiques. Toutes les alertes générées par Tivoli Monitoring sont affichées avec leur état en cours et les valeurs de seuil.

Lorsque vous modifiez les états et seuils d'alerte, les valeurs modifiées sont utilisées au cours de la prochaine heure d'échantillonnage.

Maintenance de la période d'échantillonnage par défaut

La période d'échantillonnage par défaut fournit des informations sur la génération de rapports en temps réel pour certains groupes d'attributs.

Certains groupes d'attributs ont une date et une heure implicites pour chaque enregistrement du groupe. Par exemple, le groupe d'attributs R/3_Abap_Dumps établit un rapport sur l'heure de création du vidage et le groupe d'attributs R/3_System_Log attribute établit un rapport sur l'heure de création de l'entrée de journal. Ces enregistrements ont une zone de date et d'heure. Vous pouvez obtenir un rapport pour un bref historique de la table et non pas seulement les informations les plus récentes. Cet intervalle de temps est la période de collecte de données et est utilisé comme intervalle en temps réel lors de la collecte des données. La transaction /IBMMON/ITM_PERIOD définit une période d'échantillon par défaut

(période pour le rapport en temps réel) pour chacun de ces groupes d'attributs. La période d'échantillonnage identifie la durée de la période d'échantillonnage des données qui commence à l'heure actuelle et remonte dans le temps.

Maintenance des noms de fichier journal

Les fichiers journaux spécifiques qui correspondent uniquement aux instances sont inclus dans les rapports IBM Tivoli Monitoring avec des informations du fichier journal.

Cette transaction permet d'identifier quels sont les fichiers journaux à inclure dans les rapports IBM Tivoli Monitoring contenant les informations de fichiers journaux. Tous les fichiers journaux dont le nom correspond aux modèles de nom spécifiés sur les instances spécifiées sont inclus dans le rapport à l'intervalle suivant de collecte de données.

Maintenance des groupes gérés

La transaction nommée Groupes gérés surveille et traite les transactions spécifiques dans le système SAP.

Utilisez cette transaction pour gérer les définitions de Groupe géré IBM Tivoli Monitoring. Tous les noms de groupes gérés sont transférés vers le portail de l'interface utilisateur d'IBM Application Performance Management et affichés dans les listes de sélection de système géré. Lors de la collecte des données, seules les données remplissant les conditions de sélection des attributs sont envoyées à l'agent SAP. Ces données sont affichées dans des rapports ou utilisées à des fins d'évaluation dans des situations ou des règles.

Vous pouvez utiliser les groupes gérés pour surveiller des sous-ensembles d'informations dans le système SAP. Vous pouvez ainsi vous concentrer sur les parties du système SAP qui vous intéressent et ignorer celles qui ne vous concernent pas. Par exemple, si vous êtes uniquement intéressé par le temps de réponse des transactions faisant partie de l'application financière, vous pouvez créer un groupe géré que vous appellerez Etats financiers. Vous n'inclurez que les codes de transactions financières dedans. Lorsque le groupe géré Etats financiers est traité par Tivoli Enterprise Portal, seules les informations contenant les codes de transaction spécifiés sont prises en compte lors de l'affichage d'un rapport ou de l'évaluation d'une situation ou des règles d'administration.

Sélection des ensembles de surveillance et des transactions de surveillance
Utilisez la sélection des ensembles de surveillance et de transaction de surveillance pour éditer la configuration des alertes du CCMS. Par exemple, vous pouvez désactiver complètement la collecte des alertes du CCMS.

Cette transaction est utilisée pour sélectionner les surveillances du CCMS dont IBM Tivoli Monitoring extrait les alertes. Par défaut, c'est la surveillance Système complet qui est sélectionnée la première fois que cette fenêtre s'affiche. Vous pouvez modifier l'ensemble de surveillances, la surveillance ou à la fois l'ensemble de surveillances et la surveillance, puis sauvegarder la configuration. Vous pouvez sélectionner un maximum de trois surveillances pour lesquelles les alertes du CCMS devront être collectées.

Pour désactiver complètement la collecte des alertes du CCMS, décochez les cases de toutes les surveillances et sauvegardez cette configuration.

L'agent qui est déjà exécuté lit cette configuration et collecte les alertes du CCMS pour les surveillances que vous avez sélectionnées. Cependant, les alertes du CCMS qui ont déjà été collectées par l'agent avant la modification de la configuration des alertes du CCMS restent avec l'agent et IBM Tivoli Monitoring.

Cette transaction n'est pas seulement utilisée pour la sélection des surveillances et ensembles de surveillances, mais aussi pour définir le nombre d'occurrences d'un type d'alerte qui doivent être extraites. Elle vous permet également de déterminer automatiquement si les occurrences plus anciennes des alertes doivent être extraites.

Configuration du seuil de réponse d'étape de boîte de dialogue dans le système SAP
Vous pouvez configurer un seuil de réponse d'étape de boîte de dialogue pour toute transaction en exécutant la transaction SE16.

Procédure

1. Dans la zone **Nom de table**, saisissez /IBMMON/ITM_TRSH puis sélectionnez **Contenu de la table (F7)** pour accéder à la table.
2. Pour afficher les paramètres de seuil actuels, sélectionnez **Exécuter (F8)**. Les noms de transaction sont affichés sous la colonne **CHARGE DE TRAVAIL** ; les valeurs de seuil sont affichées sous la colonne **SEUIL**.
3. Pour ajouter un nouveau paramètre de seuil, sélectionnez **Créer (F5)**. Saisissez le nom de la transaction dans la zone **CHARGE DE TRAVAIL**. Les caractères génériques suivants sont acceptés pour la valeur **CHARGE DE TRAVAIL** :
   - * correspond à plusieurs caractères
   - + correspond à un caractère unique
4. Saisissez la valeur de seuil, en millisecondes, dans la zone **SEUIL**. Sélectionnez **Sauvegarder** pour sauvegarder ce paramètre. De nouvelles valeurs de seuil et des valeurs de seuil modifiées ne prennent pas effet immédiatement, mais uniquement si l'une des conditions suivantes est respectée :
   - L'agent est redémarré.
   - L'agent rouvre sa connexion RFC sur le système SAP. Cela se produit toutes les 12 pulsations, ce qui, par défaut, correspond à 2 heures et 10 minutes.

Résultats
La valeur entrée dans la colonne **Seuil** est renvoyée dans l'attribut Seuil de réponse d'étape de boîte de dialogue du groupe d'attributs R/3_Transacation_Performance.

Opérations de travaux par lots
Vous pouvez extraire tous les travaux par lots au cours d'un intervalle de temps donné.

Procédure

Suivez les étapes après «Importation du transport ABAP dans le système SAP», à la page 758.

A faire : La constante Critique est définie pour tous les travaux par lots.

1. Pour extraire tous les travaux par lots actifs et annulés pendant un intervalle de temps donné.
   Ajoutez l'entrée suivante dans la table /IBMMON/ITM_CNFG.

Tableau 203. /IBMMON/ITM_CNFG	
PARM_NAME	**VALUE_CHAR**
BATCH_JOBS_PERF	YES

2. Pour extraire tous les travaux annulés au cours d'un intervalle de temps donné et tous les travaux actifs indépendamment de cet intervalle.
   Ajoutez l'entrée suivante dans la table /IBMMON/ITM_CNFG.

Tableau 204. /IBMMON/ITM_CNFG	
PARM_NAME	**VALUE_CHAR**
BATCH_JOBS_PERF	YES_LONG_RUN

3. Pour extraire tous les travaux par lots au cours d'un intervalle de temps donné et tous les travaux par lots actifs indépendamment de cet intervalle.
   Ajoutez l'entrée suivante dans la table /IBMMON/ITM_CNFG.

Tableau 205. /IBMMON/ITM_CNFG	
PARM_NAME	**VALUE_CHAR**
BATCH_JOBS_PERF	YES_ALL

Remarque :

- Si le paramètre de configuration n'est pas ajouté, il extrait tous les travaux par lots au cours d'un intervalle de temps donné sans que la constante Critique soit définie.
- Le nombre de lignes extraites est toujours égal à la valeur de la constante Critique définie dans le code de transaction /n/IBMMON/ITM_CONFIG.

Amélioration des performances du module de fonction /IBMMON/ITM_MAIALRT_INX
Vous pouvez améliorer les performances du module de fonction /IBMMON/ITM_MAIALRT_INX pour l'Agent SAP.

Procédure

Suivez les étapes pour améliorer les performances du module de fonction /IBMMON/ITM_MAIALRT_INX.

1. Connectez-vous à l'interface graphique de l'Agent SAP.
2. Exécutez le code de transaction SE16 et entrez le nom de la table au format /IBMMON/ITM_CNFG, puis appuyez sur la touche F7.
3. Appuyez sur la touche F5 ou cliquez sur **Create Entries** et ajoutez l'entrée suivante dans la table IBMMON/ITM_CNFG.

Tableau 206. /IBMMON/ITM_CNFG	
PARM_NAME	**VALUE_CHAR**
MAI_ALERTS_PERF	YES

Remarque :

- Si la constante Critique n'est pas définie dans le code de transaction - /N/IBMMON/ITM_CONFIG, la valeur par défaut est 2500.
- Ce processus s'applique uniquement à l'extraction des alertes MAI à partir du système SAP où PERIOD_START est PERIOD_END est initial.

  A faire : Le module de fonction /IBMMON/ITM_MAIALRT_INX extrait maintenant le nombre d'alertes MAI équivalent à la constante Critique définie dans le code de transaction - /N/IBMMON/ITM_CONFIG.
- Si cette entrée dans /IBMMON/ITM_CNFG n'est pas créée par défaut, les 2500 dernières alertes MAI sont extraites.
- Le nombre de lignes extraites est toujours égal à la valeur de la constante Critique définie dans le code de transaction /n/IBMMON/ITM_CONFIG.

Génération d'états du CCMS CEN
Centralized (CEN) Computing Center Management System (CCMS) est une fonctionnalité de surveillance SAP.

Cette fonctionnalité permet de signaler les alertes CCMS pour plusieurs systèmes SAP à un concentrateur de surveillance central. Vous pouvez surveiller l'environnement SAP à partir d'une seule console CCMS. La génération d'états du CCMS centralisée convient particulièrement à une utilisation dans les environnements suivants :

- Principalement un fonctionnement CCMS où les alertes du CCMS sont les seules données de surveillance requises.
- CCMS centralisé fait partie de l'environnement SAP.

- Grands environnements SAP avec de nombreux systèmes SAP tels qu'ISV et ISP.
- Intégration de IBM Tivoli Monitoring V5.x avec les adaptateurs CCMS de l'Agent SAP.
- Collecte d'alertes à partir de composants SAP non ABAP et de serveurs d'application.

L'Agent SAP prend en charge le CCMS centralisé pour la génération d'états d'alerte uniquement, ce qui vous permet de placer un Agent SAP sur un système SAP centralisé et d'afficher les alertes CCMS pour tout l'environnement SAP. Cette prise en charge est assurée selon les modalités suivantes :

- Lorsqu'il signale des alertes du CCMS, l'agent examine si les alertes sont associées au système SAP directement surveillé par l'agent. Si l'agent constate qu'une alerte appartient à un système SAP différent, il suppose l'exécution de CCMS centralisé et crée automatiquement des systèmes gérés R3_Group supplémentaires.
- Le système géré <local_SID>-All_CCMS_alerts:Grp est utilisé pour signaler l'ensemble complet d'alertes de tous les systèmes SAP distants. La valeur de <local_SID> est l'identificateur de système pour le système SAP surveillé directement. Par exemple, si le système SAP local était QA1, ce nom de groupe serait QA1-All_CCMS_alerts:Grp.
- Le système géré <local_SID>-<remote_SID>_CCMS_alerts:Grp est utilisé pour signaler toutes les alertes pour un système SAP distant. La valeur de <local_SID> est l'identificateur de système pour le système SAP surveillé directement. La valeur de <remote_SID> est l'identificateur de système pour le système SAP distant. Par exemple, si le système SAP local était QA1 et le système SAP distant QA2, ce nom de groupe serait QA1-QA2_CCMS_alerts:Grp.
- Chacun de ces systèmes gérés dans l'arborescence du navigateur comporte l'ensemble complet des widgets, mais seul le widget des alertes contient des données significatives.

L'Agent SAP gère ses définitions des groupes du CCMS centralisé dans le code ABAP (Advanced Business Application Programming) dans le système SAP géré directement. Vous pourriez avoir besoin de modifier ces définitions si un système SAP pour lequel vous recevez des alertes centralisées était aussi surveillé directement par une autre instance de l'Agent SAP. Vous ne voulez pas que les alertes soient signalées dans les deux systèmes. Vous pouvez limiter la génération d'états d'alerte centralisée comme suit :

- Utilisez la transaction `/IBMMON/ITM_CONFIG` pour mettre à jour les groupes gérés. Modifiez le groupe Toutes les alertes du CCMS. Supprimez le système distant de cette liste en modifiant la définition de groupe pour exclure (EXCLUDE) l'identificateur de système distant.
- Utilisez la transaction `/IBMMON/ITM_CONFIG` pour mettre à jour les groupes gérés. Supprimez le groupe <remote_SID> CCMS alerts. Par exemple, si le système SAP distant est QA2, ce nom de groupe sera alertes CCMS QA2.

Vous pouvez aussi utiliser le CCMS centralisé pour signaler les alertes de tous les systèmes SAP, mais empêcher la génération d'états d'alerte par chaque agent d'installation locale. Suivez les étapes ci-dessous pour mettre en place cette configuration :

- Configurez une instance de l'Agent SAP pour surveiller le système CCMS centralisé. Autorisez l'agent à détecter et signaler toutes les alertes de tous les systèmes SAP distants.
- Configurez une instance de l'Agent SAP pour surveiller chaque système SAP distant. Désactivez la collecte et la génération d'états d'alertes pour ces instances d'agent à l'aide de la transaction / IBMMON/ITM_CONFIG pour Sélectionner moniteurs et ensembles de moniteurs. Dans cette fonction, annulez les cases à cocher pour tous les moniteurs et enregistrez cette configuration.

La prise en charge de l'Agent SAP pour le CCMS centralisé est utilisée dans un environnement de surveillance CCMS pur afin d'afficher toutes les alertes sur une console commune. Il peut également être utilisé avec son ensemble complet de fonctions pour fournir des situations, des règles et des commandes Action aux systèmes SAP distants .

Désinstallation du transport ABAP (Advanced Business Application Programming) sur le système SAP
Si vous choisissez de supprimer l'Agent SAP de votre système, vous devez importer le transport DELETE sur le système SAP. Ce transport supprime les objets dictionnaire et modules de fonction de l'Agent SAP.

Avant de commencer
Si le système SAP est de version 7.20 ou ultérieure, avant d'importer le transport DELETE, vous devez ajouter le paramètre de profil de transport **tadirdeletions=true** dans votre profil de transport. Ce paramètre est disponible sur tp version 375.57.68 et également dans R3trans version 6.14 édition 700 ou suivante. Pour plus d'informations sur la suppression de demandes de transport du système SAP, voir Suppression de demandes de transport.

Procédure

1. Accédez au répertoire /ABAP sur le CD-ROM du produit.
2. Copiez les fichiers de transfert dans l'environnement SAP.
3. Copiez les fichiers K711_00xxx_DELETE et R711_00xxx_DELETE dans le répertoire de données du système de transfert SAP, comme suit :
   a) Copiez le fichier K711_00xxx_DELETE dans le répertoire cofiles.
   b) Copiez le fichier R711_00xxx_DELETE dans le répertoire data.
4. Exécutez les commandes suivantes :
   a) **tp addtobuffer ITMK711_00xxx_DELETE SID pf=\usr\sap\trans\bin***NOM_PROFIL*
   b) **tp import ITMK711_00xxx_DELETE SID client=nnn U16 pf=\usr\sap\trans\bin** *NOM_PROFIL*
   Où :
   SID
   ID système SAP cible
   NOM_PROFIL
   Nom du fichier de profil tp
   nnn
   Numéro du client cible sur lequel l'agent est exécuté

Personnalisation de l'instance SAP
Par défaut, toutes les instances du système SAP sont contrôlées et affichées sur le portail de l'interface utilisateur d'IBM Application Performance Management.

En tant qu'administrateur, vous choisissez l'instance SAP que vous souhaitez surveiller. De plus en tant qu'administrateur, vous pouvez désactiver une instance SAP que vous ne souhaitez pas surveiller.

La transaction personnalisée /IBMMON/ITM_INSTANCE est liée à la transaction /IBMMON/ITM_CONFIG.

Sélectionnez l'option **Instances SAP** pour afficher les instances disponibles du serveur SAP. Sélectionnez ensuite l'instance que vous souhaitez surveiller. Ces instances sont affichées sur le portail de l'interface utilisateur d'IBM Application Performance Management. Les instances inactives ou supprimées ne s'affichent pas sur le portail de l'interface utilisateur d'IBM Application Performance Management.

Fonction de test de connexion
La fonction de test de connexion vous permet de vérifier que vous pouvez connecter votre agent au système SAP sous surveillance.

Vous entrez les paramètres sur l'interface utilisateur pour effectuer la procédure de test de connexion. Si vous parvenez à vous connecter au système SAP, un message de réussite s'affiche. Si la connexion échoue, un message d'erreur s'affiche.

Le bouton **Tester la connexion** est disponible uniquement dans la fenêtre IBM Application Performance Management.

Activation de la conception CCMS
La surveillance de CCMS (Computing Center Management System) a été étendue afin de permettre la collecte des enregistrements CCMS dans un état ouvert ou fermé depuis la dernière période d'échantillonnage. Vous pouvez configurer la période d'échantillonnage ; elle a par défaut une valeur de 3 minutes. Toutefois, vous devez vous assurer que les fichiers de transfert référencés par l'Agent SAP et le transport ABAP (Advanced Business Application Programming) ont la même version.

Procédure

1. Connectez-vous au système SAP.
2. Ouvrez la transaction SE16 et ajoutez le nom de table `/IBMMON/ITM_CNFG` à la transaction.
3. Pour exécuter le module de fonction ABAP `/IBMMON/ITM_CNFG` et fournir les configurations du programme ABAP, appuyez sur **Entrée** puis sur **F8**.
4. Pour créer une nouvelle entrée à laquelle vous ajouterez les nouveaux paramètres de configuration, appuyez sur **F5**.
5. Pour créer un nouveau paramètre de configuration appelé **ISNEWCCMSDESIGN** avec la valeur *YES* sur le serveur SAP, dans la zone **PARM NAME**, entrez `ISNEWCCMSDESIGN`, et dans la zone **VALUE CHAR**, entrez YES.
6. Cliquez sur **Sauvegarder**.

   Vous pouvez ignorer la zone VALUE INT.

Modification de la valeur de seuil d'une alerte
Vous pouvez modifier la valeur de seuil **max ccms alert** associée à une alerte. Par défaut, la valeur est de 1000, ce qui signifie que vous pouvez afficher 1000 alertes dans IBM Application Performance Management. Les alertes plus anciennes sont supprimées du cache.

Procédure

1. Effectuez l'une des étapes suivantes :
   - Sous Windows, ouvrez le fichier `<candle home>\tmaitm6\KSAENV`.
   - Sur un système non Windows, ouvrez le fichier `<candle home>/config/sa.ini`.
2. Ajoutez *MAX_CCMS_ALERT_THRESHOLD=< Valeur>* à la fin du fichier.

   Remarque : La valeur doit être supérieure à 100.

Désactivation de la conception CCMS
Vous pouvez désactiver la conception CCMS (Computing Center Management System).

Procédure

1. Connectez-vous au système SAP.
2. Ouvrez la transaction SE16 et ajoutez le nom de table `/IBMMON/ITM_CNFG` à la transaction.
3. Pour exécuter le module de fonction ABAP `/IBMMON/ITM_CNFG` et fournir les configurations du programme ABAP, appuyez sur **Entrée** puis sur **F8**.
4. Pour supprimer l'entrée existante, sélectionnez **ISNEWCCMSDESIGN**, cliquez dessus avec le bouton droit de la souris, puis cliquez sur **Supprimer**.

Configuration de la surveillance de SAP HANA Database

Vous devez configurer l'Agent SAP HANA Database pour qu'il puisse collecter les données du serveur de base de données SAP HANA surveillé.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel en consultant Software Product Compatibility Reports for SAP HANA Database agent

Les prérequis suivants s'appliquent avant la configuration de l'Agent SAP HANA Database

1. Assurez-vous de créer les utilisateurs dans toutes les bases de données (système et titulaire) du système SAP HANA avec les privilèges suivants :
   - Rôle : Surveillance
   - Privilèges système : Surveillez l'administrateur

   Le nom d'utilisateur et le mot de passe pour les bases de données système et titulaire doivent être identiques.
2. Lorsque le basculement entre la connectivité principale et la connectivité de secours intervient sur le système de l'Agent SAP HANA Database, l'agent utilise le nom d'hôte du serveur de secours qui doit être résolu sur le système de l'agent. Pour résoudre le nom d'hôte en adresse IP, vous devez ajouter une entrée de mappage dans le fichier hôte de la machine sur laquelle l'agent est installé.

Remarque : Si vous configurez l'agent avec l'hôte principal, entrez le nom de système hôte qualifié complet ou l'adresse IP de l'hôte principal. Si l'utilisateur configure l'agent avec l'hôte de secours, entrez le nom de système hôte qualifié complet ou l'adresse IP de l'hôte de secours. Lorsque vous configurez l'agent via le noeud de secours, le noeud principal et la machine hôte doivent être arrêtés.

Pourquoi et quand exécuter cette tâche

L'Agent SAP HANA Database est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

Procédure

- Windows Pour configurer l'agent sur des systèmes Windows, procédez comme suit :
  a) Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
  b) Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Modèle** dans la colonne **Tâche/sous-système**, puis sélectionnez **Configurer avec les valeurs par défaut**.

  La fenêtre **Monitoring Agent for SAP HANA Database** s'ouvre.
  c) Dans la zone **Enter a unique instance name**, entrez le nom d'instance de l'agent et cliquez sur **OK**.

  Important : Le nom d'instance de l'agent doit correspondre à l'identificateur à 3 chiffres du système de base de données HANA (SID). Par exemple, si l'ID source de la base de données gérée SAP HANA est H01, entrez H01 comme nom d'instance.
  d) Dans la fenêtre **Monitoring Agent for SAP HANA Database**, spécifiez des valeurs pour les zones suivantes :

  Nom d'instance
  La valeur par défaut de cette zone est identique à celle que vous avez indiquée dans la zone **Enter a unique instance name**.

  Nom du serveur
  Le nom de système hôte qualifié complet ou l'adresse IP du serveur SAP HANA où la base de données du système est installée.

Nom de la base de données
Le nom de la base de données SAP HANA.

Numéro de port
Numéro de port SQL du service de serveur d'index sur la base de données du système du serveur de base de données SAP HANA.

Administrateur de la base de données HANA
Le nom d'utilisateur pour accéder au serveur de la base de données SAP HANA.

HANA DB Administrator Password
Le mot de passe pour accéder au serveur de la base de données SAP HANA.

Confirm HANA DB Administrator Password
Le mot de passe indiqué dans la zone **HANA DB Administrator Password**.

e) Cliquez sur **OK**.

f) Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis cliquez sur **Démarrer**.

- Linux AIX Pour configurer l'agent sur des systèmes Linux ou AIX, procédez comme suit :

  a) Dans la ligne de commande, modifiez le chemin d'accès au répertoire d'installation de l'agent. Exemple : `/opt/ibm/apm/agent/bin`

  b) Exécutez la commande suivante, où nom_instance est le nom que vous souhaitez donner à l'instance :

  `./sap_hana_database-agent.sh config` *`nom_instance`*

  Important : Le nom d'instance doit correspondre à l'identificateur à 3 chiffres du système de base de données HANA (SID). Si l'ID source de la base de données gérée SAP HANA est H01, entrez H01 comme nom d'instance.

  c) Lorsque la ligne de commande affiche le message suivant, entrez 1 et appuyez sur Entrée : `Edit 'Monitoring Agent for SAP HANA Database' setting? [1=Yes, 2=No]`

  d) Indiquez les valeurs pour les paramètres d'agent suivants :

  Nom du serveur
  Le nom de système hôte qualifié complet ou l'adresse IP du serveur SAP HANA où la base de données du système est installée.

  Nom de la base de données
  Le nom de la base de données SAP HANA.

  Numéro de port
  Numéro de port SQL du service de serveur d'index sur la base de données du système du serveur de base de données SAP HANA.

  Administrateur de la base de données HANA
  Le nom d'utilisateur pour accéder au serveur de la base de données SAP HANA.

  HANA DB Administrator Password
  Le mot de passe pour accéder au serveur de la base de données SAP HANA.

  Confirm HANA DB Administrator Password
  Le mot de passe indiqué dans la zone **HANA DB Administrator Password** .

  e) Exécutez la commande suivante pour démarrer l'Agent SAP HANA Database :

  `./sap_hana_database-agent.sh start` *`nom_instance`*

- Pour configurer l'agent à l'aide du fichier de réponses silencieux, procédez comme suit :

  a) Dans un éditeur de texte, ouvrez le fichier `sap_hana_silent_config.txt` disponible dans le chemin d'accès *`rép_install`*`\samples` et indiquez les valeurs pour tous les paramètres.

  Windows `C:\IBM\APM\samples`

  Linux AIX `/opt/ibm/apm/agent/samples`

  b) Sur la ligne de commande, changez le chemin d'accès au *`rép_install`* `\casier`

c) Exécutez la commande suivante :

Windows `sap_hana_database-agent.bat config` *`nom_instance rép_install`* `\samples\sap_hana_silent_config.txt`

Linux AIX `sap_hana_database-agent.sh config` *`nom_instance rép_install`*`\samples\sap_hana_silent_config.txt`

d) Démarrez l'agent.

Windows Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis sur **Démarrer**.

Linux AIX Exécutez la commande suivante : `./sap_hana_database-agent.sh start` *`nom_instance`*

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de la surveillance de SAP NetWeaver Java Stack

Vous devez configurer l'Agent SAP NetWeaver Java Stack pour qu'il puisse collecter les données de surveillance des ressources du serveur d'applications SAP NetWeaver surveillé. Pour surveiller les données de diagnostic et de suivi des transactions, vous devez effectuer certaines tâches de configuration.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel en consultant Software Product Compatibility Reports for SAP NetWeaver Java Stack agent

Assurez-vous d'effectuer les tâches prérequises suivantes avant de configurer l'agent :

- Copiez les fichiers JAR suivants dans le répertoire `bin` :
  - `sapj2eeclient.jar` (l'API client SAP J2EE Engine qui inclut l'adaptateur JMX)
  - `logging.jar` (la bibliothèque de journalisation)
  - `com_sap_pj_jmx.jar` (la bibliothèque SAP-JMX)
  - `exception.jar` (l'infrastructure des exceptions SAP)

  Le répertoire `bin` se trouve à l'emplacement suivant :

  Windows `candle_home\TMAITM6_x64`

  Linux `candle_home/interp/sv/bin`

  Important : Les fichiers JAR sont les mêmes pour tous les systèmes d'exploitation pris en charge. Ces fichiers sont disponibles dans le correctif de l'agent de diagnostic ou le gestionnaire SUM (Software Update Manager).
- Dans les variables d'environnement, ajoutez *<candleHome>\svdchome\<numéro de version>\toolkit\lib\win64\ttapi* à la variable path.
- Affectez le rôle NWA_READONLY à l'utilisateur *Invité* pour qu'il collecte les données de diagnostic et de suivi des transactions.

Pourquoi et quand exécuter cette tâche
L'Agent SAP NetWeaver Java Stack est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

- Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser l'interface graphique ou le fichier de réponses silencieux.
- Pour configurer l'agent sur des systèmes d'exploitation Linux ou AIX, vous pouvez utiliser la ligne de commande ou le fichier de réponses silencieux.

Pour configurer la collecte des données de diagnostic et de suivi des transactions, procédez comme suit :

1. Configurez le collecteur de données. Pour plus de détails, voir «Configuration du collecteur de données», à la page 789.
2. Activez la collecte des données de suivi des transactions et de diagnostic. Pour plus de détails, voir «Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 791.

Les instructions figurant dans cette rubrique concernent l'édition la plus récente de l'agent, sauf indication contraire. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Version de l'agent.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent sur les systèmes d'exploitation Windows à l'aide de la fenêtre **IBM Performance Management**.

Avant de commencer

Assurez-vous que les fichiers qui sont listés dans la section "Avant de commencer" de la rubrique «Configuration de la surveillance de SAP NetWeaver Java Stack», à la page 786 sont disponibles dans le répertoire `bin`.

Pourquoi et quand exécuter cette tâche

L'Agent SAP NetWeaver Java Stack fournit des valeurs par défaut pour certains paramètres. Vous pouvez spécifier différentes valeurs pour ces paramètres.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Modèle** dans la colonne **Tâche/sous-système**, puis cliquez sur **Configuration de l'agent**.

   La fenêtre **Monitoring Agent for SAP NetWeaver Java Stack** s'affiche.
3. Dans la zone **Enter a unique instance name**, entrez le nom d'instance de l'agent et cliquez sur **OK**.

   Important : Le nom d'instance de l'agent doit correspondre à l'identificateur système à 3 chiffres du système SAP NetWeaver Java Stack. Par exemple, si l'identificateur système (SID) du système géré SAP NetWeaver Java Stack est P14, entrez P14 comme nom d'instance.
4. Dans la fenêtre **Monitoring Agent for SAP NetWeaver Java Stack**, indiquez des valeurs pour les paramètres de configuration et cliquez sur **OK**.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 793.
5. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis cliquez sur **Démarrer**.

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données de surveillance des ressources collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir Démarrage de la console Performance Management.
- Pour collecter les données de diagnostic et de suivi des transactions, configurez le collecteur de données et activez la collecte de données de diagnostic et de suivi des transactions.

Configuration de l'agent sur des systèmes Linux ou AIX

Pour configurer l'agent sur les systèmes Linux ou AIX, vous devez exécuter le script et répondre aux invites.

Avant de commencer

Assurez-vous que les fichiers qui sont listés dans la section "Avant de commencer" de la rubrique «Configuration de la surveillance de SAP NetWeaver Java Stack», à la page 786 sont disponibles dans le répertoire `bin`.

Procédure

1. Dans la ligne de commande, modifiez le chemin d'accès au répertoire d'installation de l'agent.

   Linux `/opt/ibm/apm/agent/bin`

   Linux AIX `/opt/ibm/apm/agent/bin`
2. Exécutez la commande suivante :

   `./sap_netweaver_java_stack-agent.sh config` *`nom_instance`*

   où *nom_instance* est le nom à attribuer à l'instance.

   Important : Le nom d'instance de l'agent doit correspondre à l'identificateur système à 3 chiffres du système SAP NetWeaver Java Stack. Par exemple, si l'identificateur système (SID) du système géré SAP NetWeaver Java Stack est P14, entrez P14 comme nom d'instance.
3. Lorsque la ligne de commande affiche le message suivant, entrez 1 et appuyez sur Entrée :

   `Edit 'Monitoring Agent for SAP NetWeaver Java Stack' setting? [1=Yes, 2=No]`
4. A l'invite, indiquez les valeurs des paramètres de configuration.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 793
5. Exécutez la commande suivante pour démarrer l'agent :

   `./sap_netweaver_java_stack-agent.sh start` *`nom_instance`*

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données de surveillance des ressources collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir Démarrage de la console Performance Management.
- Pour collecter les données de diagnostic et de suivi des transactions, configurez le collecteur de données et activez la collecte des données de diagnostic et de suivi des transactions.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Avant de commencer

Assurez-vous que les fichiers qui sont listés dans la section "Avant de commencer" de la rubrique «Configuration de la surveillance de SAP NetWeaver Java Stack», à la page 786 sont disponibles dans le répertoire `bin`.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

1. Dans un éditeur de texte, ouvrez le fichier `sap_netweaver_java_stack_silent_config.txt` disponible dans le chemin d'accès suivant et indiquez les valeurs pour les paramètres de configuration.

   Windows `C:\IBM\APM\samples`

   Linux AIX `/opt/ibm/apm/agent/samples`

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 793
2. Sur la ligne de commande, changez le chemin d'accès au `rép_install\bin`.
3. Exécutez la commande suivante :

   Windows `sap_netweaver_java_stack-agent.bat config` *`nom_instance`* `rép_install\samples\sap_netweaver_java_stack_silent_config.txt`

   Linux AIX `./sap_netweaver_java_stack-agent.sh config` *`nom_instance`* `rép_install\samples\sap_netweaver_java_stack_silent_config.txt`
4. Démarrez l'agent.

   Windows Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur l'instance d'agent que vous avez créée, puis cliquez sur **Démarrer**. Sinon, vous pouvez également exécuter la commande suivante : `sap_netweaver_java_stack-agent.bat start` *`nom_instance`*

   Linux AIX Exécutez la commande suivante : `./sap_netweaver_java_stack-agent.sh start` *`nom_instance`*

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données de surveillance des ressources collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir Démarrage de la console Performance Management.
- Pour collecter les données de diagnostic et de suivi des transactions, configurez le collecteur de données et activez la collecte des données de diagnostic et de suivi des transactions.

Configuration du collecteur de données

Vous pouvez configurer le collecteur de données pour chaque instance du serveur d'applications que vous voulez surveiller.

Avant de commencer

Assurez-vous que les fichiers qui sont listés dans la section "Avant de commencer" de la rubrique «Configuration de la surveillance de SAP NetWeaver Java Stack», à la page 786 sont disponibles dans le répertoire `bin`.

Procédure

Pour configurer le collecteur de données en répondant à des invites, procédez comme suit :

1. Sur la ligne de commande, accédez au répertoire Windows `rép_install\svdchome\`*`n° de version`*`\bin\configNW` ou Linux AIX `rép_install/svdchome/`*`n° de version`*`/bin/configNW` et exécutez le script suivant :

   Windows config.bat

   Linux AIX config.sh
2. Sélectionnez la version de NetWeaver Server en saisissant le numéro qui correspond au produit pour lequel vous voulez configurer le collecteur de données et appuyez sur Entrée.
3. Lorsque vous êtes invité à indiquer le nom d'utilisateur, entrez celui qui est configuré sur SAP NetWeaver Application Server with Java Stack, et appuyez sur Entrée.
4. Lorsque vous êtes invité à indiquer un mot de passe, entrez le mot de passe, puis appuyez sur Entrée.
5. Lorsque vous êtes invité à entrer à nouveau le mot de passe, entrez-le à nouveau, puis appuyez sur Entrée.
6. Lorsque vous êtes invité à indiquer un numéro de port P4, entrez le numéro de port P4 de l'instance de SAP NetWeaver Application Server disponible sur l'ordinateur local, puis appuyez sur Entrée.

   Important : Utilisez cette formule pour calculer le numéro de port P4 : 50000 + (instance number*100) + 4
7. Lorsque vous êtes invité à sélectionner le numéro d'instance de NetWeaver Server, entrez le numéro qui correspond à l'instance que vous souhaitez configurer, puis appuyez sur Entrée.

   A faire : Vous devez, pour chaque instance, configurer le collecteur de données séparément.
8. Si vous êtes invité à entrer le chemin d'accès au répertoire de base Java, utilisez le répertoire JAVA_HOME de l'instance SAP. Par exemple, `E:\usr\sap\J01\J04\exe\sapjvm_6`.
9. A l'invite, entrez 1 si vous souhaitez activer la collecte des données de suivi des transactions. Sinon, entrez 2 et appuyez sur Entrée.
10. A l'invite, entrez 1 si vous souhaitez activer la collecte des données de diagnostic. Sinon, entrez 2 et appuyez sur Entrée.

Résultats

Le chemin d'accès est généré pour charger les fichiers classe.

Que faire ensuite

1. Ajoutez le chemin généré à la variable d'environnement appropriée.

   Windows *PATH*

   Linux *LD_LIBRARY_PATH* et *LIBPATH*

   AIX *LD LIBRARY PATH* et *LIB PATH*

   A faire :

   Windows Ajoutez le chemin généré à la variable d'environnement *PATH*.

   Linux Ajoutez le chemin généré aux variables d'environnement *LD_LIBRARY_PATH* et *LIBPATH* dans le fichier `/home/`*`sid`*`adm/.cshrc` au format suivant.

   ```
   setenv LD_LIBRARY_PATH /path
   setenv LIBPATH /path
   ```

   AIX Ajoutez le chemin généré aux variables d'environnement *LD LIBRARY PATH* et *LIB PATH* dans le fichier `/etc/environment` au format suivant.

   ```
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/path
   LIBPATH=$LIBPATH:/path
   ```

2. Redémarrez les instances du serveur d'applications.
3. Activez la collecte des données de suivi des transactions et de diagnostic. Pour plus de détails, voir «Activation de la collecte des données de suivi des transactions et de diagnostic», à la page 791.

Activation de la collecte des données de suivi des transactions et de diagnostic

Sur la page **Configuration d'agent**, vous pouvez activer ou désactiver la collecte des données de diagnostic ou de suivi des transactions.

Avant de commencer

Vérifiez que le collecteur de données est configuré. Pour plus de détails, voir «Configuration du collecteur de données», à la page 789.

Pourquoi et quand exécuter cette tâche

Lorsque vous activez la collecte des données de suivi des transactions, l'agent collecte les données des composants suivants :

- Servlet JSP
- RemoteEJB
- JMS

Procédure

Pour configurer la collecte des données pour chaque instance de SAP NetWeaver Application Server, procédez comme suit :

1. Connectez vous à console Cloud APM.
2. A partir de la barre de navigation, cliquez sur **Configuration système** > **Configuration d'agent**.
   La page **Configuration d'agent** s'affiche.
3. Cliquez sur l'onglet **NetWeaver**.
4. Cochez les cases des instances de SAP NetWeaver Application Server pour lesquelles vous souhaitez configurer la collecte de données, puis effectuez l'une des actions suivantes de la liste **Actions**.
   - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Enabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour sur Enabled pour chaque instance de SAP NetWeaver Application Server sélectionnée.
   - Pour activer la collecte des données de diagnostic, cliquez sur **Set Diagnostic Mode** > **Enabled Diagnostic Mode Only**. Le statut indiqué dans la colonne Diagnostic Mode est mis à jour sur Enabled pour chaque instance de SAP NetWeaver Application Server sélectionnée.
   - Pour activer la collecte des données de diagnostic et la trace de méthode, cliquez sur **Set Diagnostic Mode** > **Enabled Diagnostic Mode and Method Trace**. Le statut indiqué dans les colonnes Diagnostic Mode and Method Trace est mis à jour sur Enabled pour chaque instance de SAP NetWeaver Application Server sélectionnée.
   - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Disabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour sur Disabled pour chaque instance de SAP NetWeaver Application Server sélectionnée.
   - Pour désactiver la collecte des données de diagnostic, cliquez sur **Set Diagnostic Mode** > **Disabled Diagnostic Mode and Method Trace**. Le statut indiqué dans les colonnes **Diagnostic Mode and Method Trace** est mis à jour sur Disabled pour chaque instance de SAP NetWeaver Application Server sélectionnée.

Résultats

La collecte de données est configurée pour chaque instance de SAP NetWeaver Application Server sélectionnée.

Que faire ensuite
Connectez-vous à la console Cloud APM pour afficher les données de suivi des transactions et de diagnostic collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Suppression de la configuration du collecteur de données

Vous pouvez annuler les modifications effectuées lors de la configuration du collecteur de données pour une instance de SAP Netweaver Application Server with Java Stack.

Procédure

Pour supprimer la configuration du collecteur de données en répondant à des invites, procédez comme suit :

1. Sur la ligne de commande, accédez au répertoire Windows `rép_install\svdchome\`*`n° de version`*`\bin\configNW` ou Linux AIX `rép_install/svdchome/`*`n° de version`*`/bin/configNW` et exécutez le script suivant :

   Windows unconfig.bat

   Linux AIX unconfig.sh

   Toutes les instances pour lesquelles le collecteur de données est configuré sont répertoriées.
2. Entrez le numéro qui correspond à l'instance pour laquelle vous voulez supprimer la configuration du collecteur de données et appuyez sur Entrée.

   Conseil : Pour supprimer la configuration du collecteur de données pour plusieurs instances, entrez le numéro qui correspond aux instances séparé par des virgules. Pour supprimer la configuration du collecteur de données pour toutes les instances, vous pouvez exécuter les scripts suivants :

   Windows config.bat -a

   Linux AIX config.sh -a

Que faire ensuite
Redémarrez les instances de SAP NetWeaver AS with Java Stack.

Restauration de l'instance SAP NetWeaver Application Server

Vous pouvez utiliser l'utilitaire de restauration pour restaurer les paramètres JVM si l'instance SAP NetWeaver Application Server ne démarre pas après la configuration de SAP NetWeaver Data Collector, ou pour restaurer l'instance SAP NetWeaver Application Server.

Procédure

Pour restaurer l'instance SAP NetWeaver Application Server en répondant aux invites, procédez comme suit :

1. Sur la ligne de commande, accédez au répertoire Windows `rép_install\svdchome\`*`n° de version`*`\bin\configNW` ou Linux AIX `rép_install/svdchome/`*`n° de version`*`/bin/configNW` et exécutez le script suivant :

   Windows `restoreNW.bat`

   Linux AIX `restoreNW.sh`
2. Sélectionnez la version de NetWeaver Server en entrant le numéro qui correspond au produit pour lequel vous souhaitez restaurer les paramètres JVM, puis appuyez sur Entrée.
3. Lorsque vous êtes invité à indiquer le nom d'utilisateur, entrez celui de l'instance SAP NetWeaver Application Server et appuyez sur Entrée.
4. Lorsque vous êtes invité à indiquer le mot de passe utilisateur, entrez celui de l'instance SAP NetWeaver Application Server et appuyez sur Entrée.

5. Lorsque vous êtes invité à indiquer un numéro de port P4, entrez celui de l'instance SAP NetWeaver Application Server disponible sur l'ordinateur local et appuyez sur Entrée.

   Si les informations d'instance sont introuvables avec le port P4 indiqué, le message `Could not connect to SAP NetWeaver Server` s'affiche et vous êtes invité à entrer le chemin du répertoire principal de l'instance NetWeaver Server.

   Par exemple : `usr\sap\`*`nom_système`*`\`*`numéro_instance`*
6. Lorsque vous êtes invité à sélectionner le numéro d'instance NetWeaver Server, entrez le numéro qui correspond à l'instance à restaurer, puis appuyez sur Entrée.

Résultats

Le message suivant s'affiche :

```
Restore successful. Please restart the instance.
```

Paramètres de configuration de l'agent

Lorsque vous configurez l'Agent SAP NetWeaver Java Stack, vous pouvez modifier la valeur par défaut des paramètres, comme SAP_NETWEAVER_P4_HOSTNAME et SAP_NETWEAVER_P4_PORT.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de l'Agent SAP NetWeaver Java Stack. Vous devez indiquer une valeur pour toutes les zones car elles sont obligatoires.

Tableau 207. Noms et descriptions des paramètres de configuration

Nom du paramètre	Description
Nom d'instance	Nom de l'instance. La valeur par défaut de cette zone est identique à celle que vous avez indiquée dans la zone **Enter a unique instance name**.
SAP_NETWEAVER_P4_ HOSTNAME	Nom d'hôte ou adresse IP du serveur SAP NetWeaver Application Server.
SAP_NETWEAVER_P4_ PORT	Numéro de port P4 du serveur SAP NetWeaver Application Server.
SAP_NETWEAVER_P4_ USERNAME	Nom d'utilisateur de l'administrateur donnant accès au serveur SAP NetWeaver Application Server.
SAP_NETWEAVER_P4_ PASSWORD	Mot de passe de l'administrateur donnant accès au serveur SAP NetWeaver Application Server.
Confirm SAP_NETWEAVER_P4_ PASSWORD	Mot de passe spécifié pour le paramètre **SAP_NETWEAVER_P4_PASSWORD**.

Configuration de la surveillance de Siebel

L'agent Siebel permet de surveiller de manière centralisée vos ressources Siebel, notamment les statistiques Siebel, les sessions utilisateur, les composants, les tâches, le serveur d'application, le serveur de noms de passerelle Siebel, l'utilisation de la mémoire et de l'UC de processus et la surveillance des événements du journal.

Avant de commencer

- Lisez l'intégralité de la rubrique «Configuration de la surveillance de Siebel», à la page 793 pour déterminer les éléments nécessaires à l'achèvement de la configuration.
- Les instructions figurant dans cette rubrique concernent l'édition la plus récente de l'agent, sauf indication contraire.

- Assurez-vous que votre environnement possède la configuration système requise pour l'agent Siebel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Siebel.
- Avant de configurer l'agent Siebel, vous devez vérifier le compte utilisateur Siebel utilisé par l'agent Siebel.

Le paramètre "Per Component Statistics Monitoring" est désactivé par défaut. Vous pouvez activer le paramètre "Per Component Statistics Monitoring".

Pourquoi et quand exécuter cette tâche

L'agent Siebel est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

Procédure

1. Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser la fenêtre IBM Performance Management ou le fichier de réponses silencieux.
   - «Configuration de l'agent sur des systèmes Windows», à la page 796.
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 801.
2. Pour configurer l'agent sur des systèmes d'exploitation Linux et UNIX, vous pouvez exécuter le script et répondre aux invites ou utiliser le fichier de réponses silencieux.
   - «Configuration de l'agent en répondant à des invites», à la page 800.
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 801.

Que faire ensuite

Dans la console Cloud APM, accédez aux pages du Tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont :

- Linux AIX `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Pour identifier et résoudre les incidents, reportez-vous au forum Cloud Application Performance Management.

Vérification du compte utilisateur Siebel

Vous devez vérifier le compte utilisateur qui est utilisé pour exécuter l'agent Siebel avant de configurer l'agent.

Pourquoi et quand exécuter cette tâche

Le compte utilisateur qui est utilisé pour exécuter l'agent Siebel doit disposer de droits lui permettant d'exécuter l'utilitaire de ligne de commande Siebel **srvrmgr**. Pour vérifier que le compte utilisateur dispose des droits requis, procédez comme suit :

Procédure

1. Connectez-vous à l'ordinateur avec le compte utilisateur utilisé pour exécuter l'agent Siebel.
2. Déplacez le répertoire à l'emplacement où le serveur Siebel est installé.
3. Sourcez le fichier d'environnement Siebel :

   ```
   source siebenv.sh
   ```

4. Exécutez la commande suivante :

```
srvrmgr /s serveur_Siebel /g passerelle_Siebel /e entreprise_Siebel
/u compte_utilisateur /p mot_de_passe
/c "list servers"
```

où

serveur_Siebel
Nom du serveur d'applications Siebel.

passerelle_Siebel
Nom du serveur de noms de passerelle actuellement actif.

entreprise_Siebel
Nom de l'entreprise Siebel.

compte_utilisateur
Compte utilisateur que vous utilisez pour vous connecter à l'ordinateur.

mot_de_passe
Mot de passe associé au compte utilisateur.

Si le compte utilisateur dispose des droits requis, une sortie similaire à l'exemple suivant indique que le nombre de zones renvoyées est limité à trois :

```
Connected to 1 server(s) out of a total of 1 server(s) in the enterprise

srvrmgr:s82win8> list servers show SBLSRVR_NAME, HOST_NAME, SBLSRVR_STATUS

SBLSRVR_NAME  HOST_NAME  SBLSRVR_STATUS
------------  ---------  --------------------------------
s82win8       s82win8    16.0.0.0 [23057] LANG_INDEPENDENT

1 row returned.
```

Si la commande **srvrmgr** ne s'exécute pas correctement, adressez-vous à l'administrateur Siebel du serveur. Veillez à définir les variables d'environnement Siebel requises pour le compte utilisateur et assurez-vous que le compte utilisateur dispose des droits appropriés lui permettant d'exécuter la commande **srvrmgr**.

Activation du paramètre "Per Component Statistics Monitoring"

Le paramètre "Per Component Statistics Monitoring" est désactivé par défaut. Vous pouvez activer le paramètre "Per Component Statistics Monitoring" à l'aide de la variable d'environnement KUY_ENABLE_COMP_STATS.

Avant de commencer

En raison d'un problème connu lié aux serveurs de Siebel V8.1 et ultérieure, la collecte des statistiques de composant Siebel risque d'avoir un impact négatif sur l'utilisation de la mémoire du serveur de passerelle Siebel. Ce problème est décrit dans la note technique publiée par Oracle nommée "Gateway Service on Siebel 8.1 or 8.2 Might Consume High Memory Consumption: Recovery (ID document 1269177.1)". Cet article fournit un correctif à ce problème, qui est mis en oeuvre sur le serveur Siebel.

Si le paramètre "Per Component Statistic Monitoring" est requis dans l'environnement, appliquez le correctif Oracle aux serveurs de passerelle de Siebel version 8.1 ou ultérieure avant d'activer le paramètre "Per Component Statistics Monitoring".

Pourquoi et quand exécuter cette tâche

Après avoir appliqué le correctif Oracle, procédez comme suit pour activer le paramètre "Per Component Statistics Monitoring" dans l'agent Siebel :

Procédure

1. Accédez au répertoire d'installation de l'agent Siebel :

- Windows *rép_install*\TMAITM6_x64
- Linux AIX *rép_install*/config

2. Editez le fichier de configuration de l'agent Siebel de sorte à définir KUY_ENABLE_COMP_STATS sur true.
   - Windows KUYENV_*nom_instance*
   - Linux AIX uy.environment

   où *nom_instance* est le nom d'instance de l'agent Siebel.
3. Redémarrez l'agent.

   Important : Pour que ce paramètre soit défini par défaut pour toutes les nouvelles instances d'agent, définissez KUY_ENABLE_COMP_STATS sur true dans les modèles de fichier de configuration :
   - Windows KUYENV
   - Linux AIX Ce paramètre a déjà été défini par défaut pour les nouvelles instances d'agent en éditant uy.environment à l'étape 2.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent Siebel sur les systèmes d'exploitation Windows dans la fenêtre IBM Cloud Application Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur le modèle **Monitoring Agent for Siebel**, puis cliquez sur **Configure agent**.

   A faire : Après avoir configuré une instance d'agent pour la première fois, l'option **Configure agent** est désactivée. Pour reconfigurer l'instance d'agent, cliquez dessus avec le bouton droit de la souris et sélectionnez **Reconfigure**.
3. Entrez un nom d'instance unique, puis cliquez sur **OK**. N'utilisez que des lettres, des chiffres arabes, le caractère de soulignement et le caractère moins dans le nom de l'instance. Par exemple : siebel01.

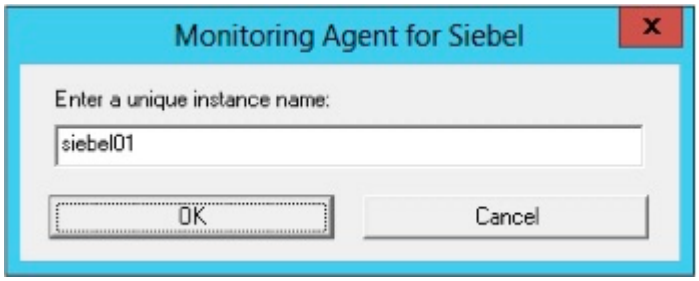


Figure 22. Fenêtre de saisie d'un nom d'instance unique.

4. Sélectionnez un type de serveur et entrez les valeurs appropriées dans les zones obligatoires, puis cliquez sur **Suivant**.

   Pour obtenir une description de chaque paramètre de configuration, voir Tableau 208, à la page 802.

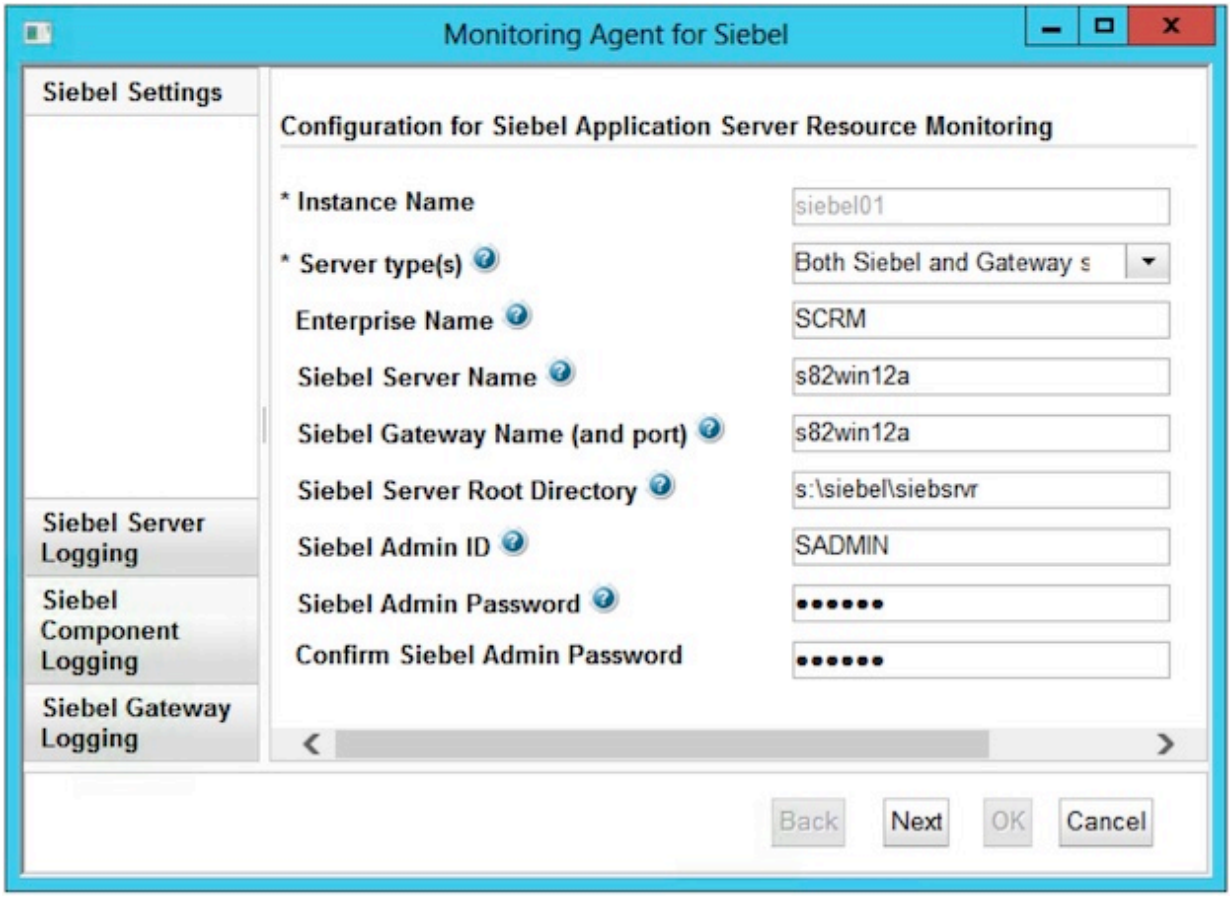


Figure 23. Fenêtre des paramètres de configuration pour les types de serveur Siebel installés sur un hôte Siebel

Important : Si l'agent Siebel est installé sur un ordinateur avec le serveur de noms de passerelle Siebel mais sans le serveur Siebel, les données qui s'affichent dans le Tableau de bord des applications s'appliquent uniquement au serveur de noms de passerelle Siebel pour cette instance. Toutes les autres vues de l'agent Siebel sont vides.

5. Facultatif : Editez les valeurs de consignation du serveur Siebel, puis cliquez sur **Suivant**.
   Pour obtenir une description de chaque paramètre de configuration, voir Tableau 209, à la page 803.

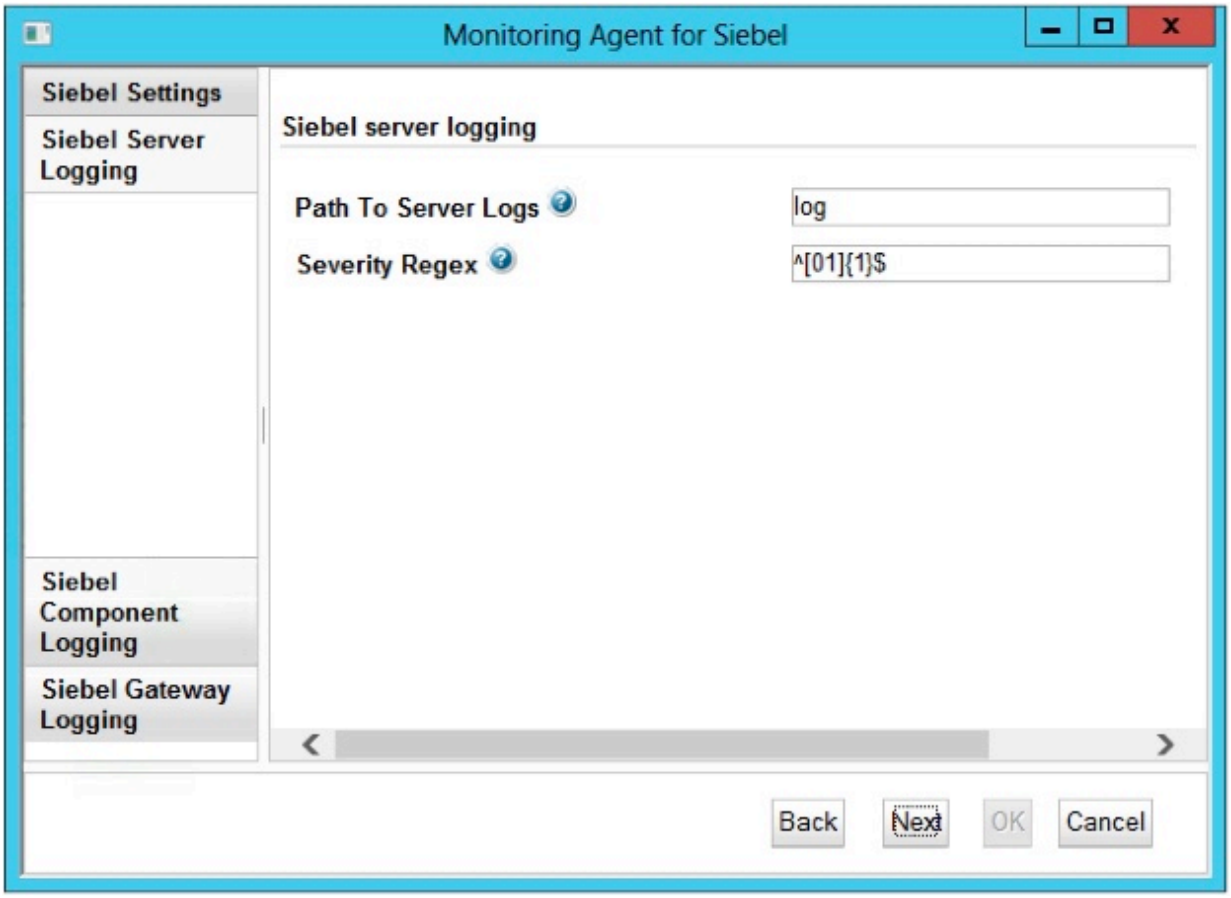


Figure 24. Fenêtre de spécification des paramètres de consignation du serveur Siebel

6. Facultatif : Editez les valeurs de consignation du composant Siebel, puis cliquez sur **Suivant**. Par défaut, les journaux des composants du Tableau 212, à la page 805 sont surveillés par l'agent Siebel. Pour ajouter jusqu'à 10 journaux de composant supplémentaires à surveiller, indiquez l'alias de composant correspondant, `SCBroker` par exemple.

   Pour obtenir une description de chaque paramètre de configuration, voir Tableau 210, à la page 804.

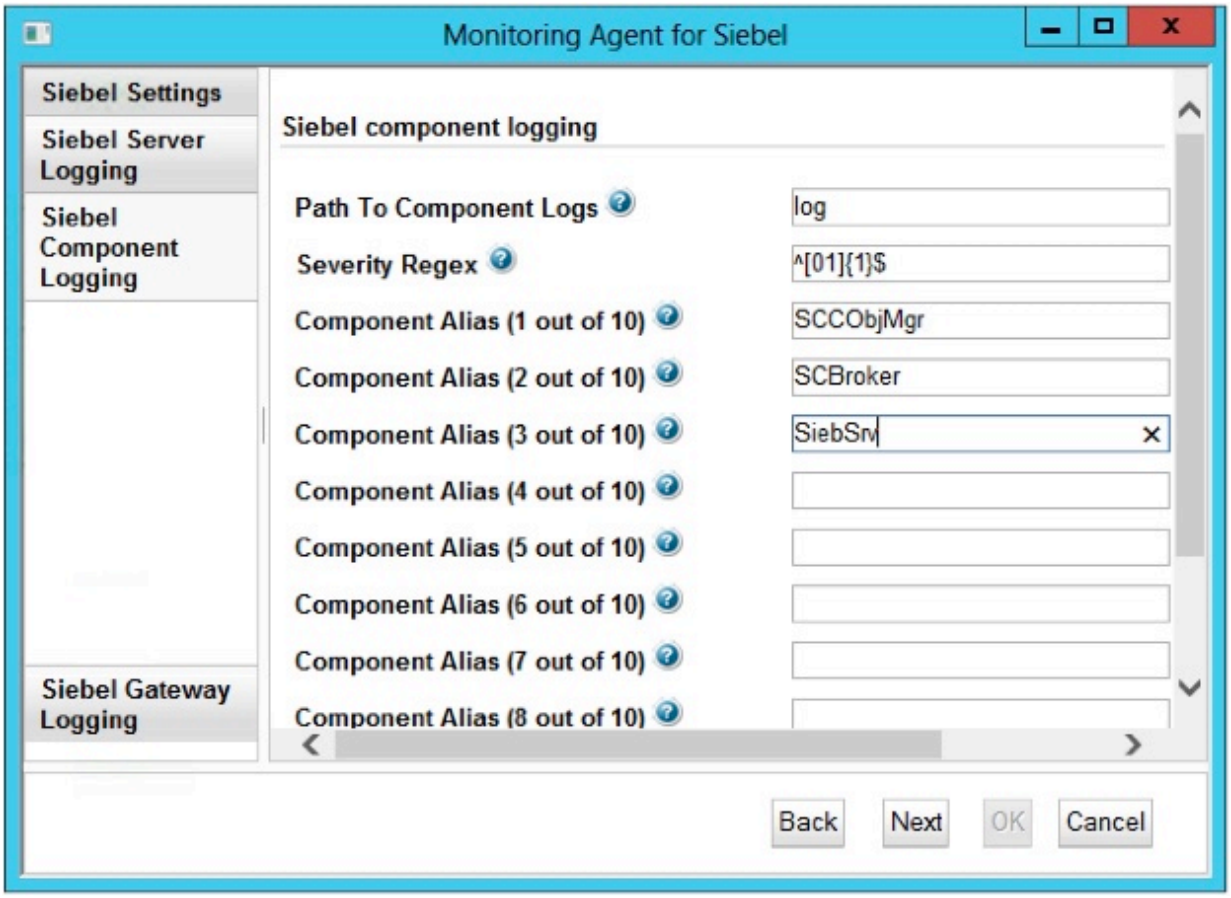


Figure 25. Fenêtre de spécification de journaux de composant supplémentaires à surveiller

7. Facultatif : Editez les valeurs de consignation de la passerelle Siebel.
   Pour obtenir une description de chaque paramètre de configuration, voir Tableau 211, à la page 804.

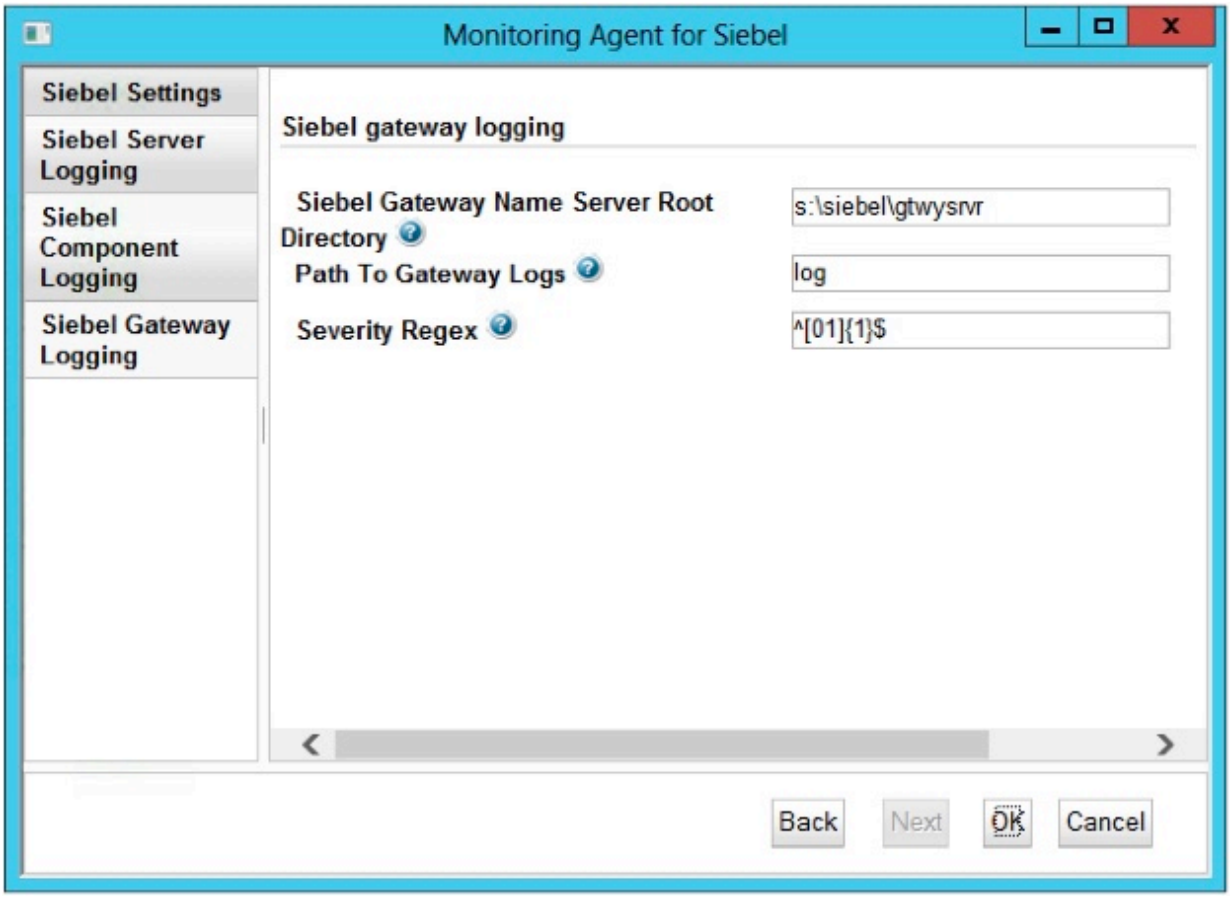


Figure 26. Fenêtre de spécification des paramètres de consignation de la passerelle Siebel

8. Cliquez sur **OK** pour terminer la configuration.
9. Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur l'instance que vous avez configurée, puis cliquez sur **Démarrer**.

Configuration de l'agent en répondant à des invites

Après avoir installé l'agent Siebel, vous devez le configurer pour pouvoir le démarrer. Si l'agent Siebel est installé sur un ordinateur Linux ou UNIX local, vous pouvez suivre ces instructions pour le configurer de manière interactive en suivant des invites de ligne de commande.

Pourquoi et quand exécuter cette tâche

A faire : Si vous reconfigurez une instance d'agent configurée, la valeur définie dans la dernière configuration s'affiche pour chaque paramètre. Pour effacer une valeur existante, appuyez sur la touche Espace lorsque le paramètre s'affiche.

Procédure

- Procédez comme suit pour configurer l'agent Siebel en exécutant un script et en répondant aux invites.
  a) A partir d'une ligne de commande, exécutez la commande suivante :

  rép_install/bin/siebel-agent.sh config **nom_instance**

  où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent.

  Exemple

```
/opt/ibm/apm/agent/bin/siebel-agent.sh config example-inst01
```

b) Répondez aux invites pour définir les valeurs de configuration de l'agent.

Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'agent Siebel», à la page 802.

c) Exécutez la commande suivante pour démarrer l'agent :

rép_install/bin/siebel-agent.sh start **nom_instance**

où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

Exemple

```
/opt/ibm/apm/agent/bin/siebel-agent.sh start example-inst01
```

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

- Pour configurer l'agent Siebel en mode silencieux, procédez comme suit :
  a) Dans un éditeur de texte, ouvrez le fichier `siebel_silent_config.txt` disponible à l'emplacement suivant :
     – Linux AIX *rép_install*/samples/siebel_silent_config.txt
     – Windows *rép_install*\samples\siebel_silent_config.txt

     où *rép_install* représente le chemin d'installation de l'agent.

     Exemple

     – Linux AIX /opt/ibm/apm/agent/samples/siebel_silent_config.txt
     – Windows C:\IBM\APM\samples\siebel_silent_config.txt
  b) Dans le fichier `siebel_silent_config.txt`, indiquez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.

     Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'agent Siebel», à la page 802.
  c) Sauvegardez et fermez le fichier `siebel_silent_config.txt` et exécutez la commande suivante :
     – Linux AIX *rép_install*/bin/siebel-agent.sh config **nom_instance** *rép_install*/samples/siebel_silent_config.txt
     – Windows *rép_install*\bin\siebel-agent.bat config **nom_instance** *rép_install*\samples\siebel_silent_config.txt

     où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.

Exemple

– Linux AIX `/opt/ibm/apm/agent/bin/siebel-agent.sh config example-inst01 /opt/ibm/apm/agent/samples/siebel_silent_config.txt`

– Windows `C:\IBM\APM\bin\ siebel-agent.bat config example-inst01 C:\IBM\APM\samples\siebel_silent_config.txt`

d) Exécutez la commande suivante pour démarrer l'agent :

– Linux AIX *rép_install*`/bin/siebel-agent.sh start` **nom_instance**

– Windows *rép_install*`\bin\siebel-agent.bat start` **nom_instance**

où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

Exemple

– Linux AIX `/opt/ibm/apm/agent/bin/siebel-agent.sh start example-inst01`

– Windows `C:\IBM\APM\bin\siebel-agent.bat start example-inst01`

Paramètres de configuration de l'agent Siebel

Les paramètres de configuration de l'agent Siebel sont affichés dans des tableaux qui les regroupent par catégories.

1. Paramètres Siebel - Paramètres généraux de l'environnement Siebel.
2. Consignation du serveur Siebel - Paramètres propres à la surveillance des journaux du serveur Siebel.
3. Consignation du composant Siebel - Paramètres propres à la surveillance d'une liste personnalisée de journaux du composant Siebel.
4. Consignation de la passerelle Siebel - Paramètres propres à la surveillance des journaux de la passerelle Siebel.

Tableau 208. Paramètres Siebel

Nom du paramètre	Description	Requis pour la sélection du type de serveur	Nom du paramètre de fichier de configuration en mode silencieux
Server type(s)	Indique les types de serveur installés sur l'ordinateur local.	• **Gateway server only** • **Siebel server only** • **Both Siebel and Gateway server**	**KUY_SERVER_TYPE**
Enterprise Name	Nom de l'entreprise Siebel.	• **Siebel server only** • **Both Siebel and Gateway server**	**KUY_ENTERPRISE**

Tableau 208. Paramètres Siebel (suite)

Nom du paramètre	Description	Requis pour la sélection du type de serveur	Nom du paramètre de fichier de configuration en mode silencieux
Siebel Server Name	Nom du serveur Siebel à surveiller. **Remarque :** Il ne s'agit pas du nom d'hôte du serveur, mais du nom de serveur utilisé lorsque vous exécutez la commande Siebel **`srvrmgr`**.	• **Siebel server only** • **Both Siebel and Gateway server**	**KUY_SERVER**
Siebel Gateway Name	Serveur de noms de passerelle Siebel à surveiller et éventuellement le port, par exemple, `gtwysrvr` ou `gtwysrvr:1234`.	• **Siebel server only** • **Both Siebel and Gateway server**	**KUY_GATEWAY**
Siebel Server Root Directory	Répertoire d'installation de base du serveur d'applications Siebel.	• **Siebel server only** • **Both Siebel and Gateway server**	**KUY_INSTALL_ROOT**
Siebel Admin ID	ID utilisateur propre à Siebel utilisé par l'agent pour s'authentifier auprès de l'entreprise Siebel lorsque vous exécutez la commande **`srvrmgr`**. Par exemple : `SADMIN`	• **Siebel server only** • **Both Siebel and Gateway server**	**KUY_ADMIN_ID**
Siebel Admin password	Mot de passe de l'administrateur du serveur Siebel.	• **Siebel server only** • **Both Siebel and Gateway server**	**KUY_ADMIN_PASSWORD**

Tableau 209. Paramètres de consignation du serveur Siebel

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Path To Server Logs	Chemin d'accès relatif issu de "Siebel Server Root Directory" aux journaux du serveur. Pour désactiver la capture de la consignation de serveur Siebel, entrez un chemin d'accès non valide. Par exemple : `xyz`.	**KUY_SERVER_LOGGING_PATH**

Tableau 209. Paramètres de consignation du serveur Siebel (suite)		
Nom du paramètre	**Description**	**Nom du paramètre de fichier de configuration en mode silencieux**
Severity Regex	Expression régulière permettant de capturer les journaux du serveur Siebel correspondant à un niveau de gravité. La valeur par défaut `^[01]{1}$` aide à capturer les erreurs de niveau 0 et 1.	**KUY_SERVER_LOGGING_SEVERITY_REGEX**

Tableau 210. Paramètres de consignation du composant Siebel		
Nom du paramètre	**Description**	**Nom du paramètre de fichier de configuration en mode silencieux**
Path To Component Logs	Chemin d'accès relatif issu de "Siebel Server Root Directory" aux journaux du serveur. Pour désactiver la capture de la consignation de serveur Siebel, entrez un chemin d'accès non valide. Par exemple : `xyz`.	**KUY_COMPONENT_LOGGING_PATH**
Severity Regex	Expression régulière permettant de capturer les journaux du serveur Siebel correspondant à un niveau de gravité. La valeur par défaut `^[01]{1}$` aide à capturer les erreurs de niveau 0 et 1.	**KUY_COMPONENT_LOGGING_SEVERITY_ REGEX**
Component Alias (*N* out of 10)	Alias de composant pour lequel surveiller le journal d'un composant supplémentaire. Exemple : `SCBroker`. Où *N* indique le nombre de composants facultatifs, entre 1 et 10.	**KUY_CUSTCOMPLOG_00** à **KUY_CUSTCOMPLOG_09**

Tableau 211. Paramètres de consignation de la passerelle Siebel		
Nom du paramètre	**Description**	**Nom du paramètre de fichier de configuration en mode silencieux**
Siebel Gateway Name Server Root Directory	Répertoire d'installation de base du serveur de noms de passerelle Siebel.	**KUY_GATEWAY_ROOT**

Tableau 211. Paramètres de consignation de la passerelle Siebel (suite)		
Nom du paramètre	**Description**	**Nom du paramètre de fichier de configuration en mode silencieux**
Path To Gateway Logs	Chemin d'accès relatif issu de "Siebel Gateway Name Server Root Directory" aux journaux de la passerelle. Pour désactiver la capture de la consignation de serveur de noms de passerelle, entrez un chemin d'accès non valide. Par exemple : `xyz`.	**KUY_GW_LOGGING_PATH**
Severity Regex	Expression régulière permettant de capturer les journaux du serveur Siebel correspondant à un niveau de gravité. La valeur par défaut `^[01]{1}$` aide à capturer les erreurs de niveau 0 et 1.	**KUY_GW_LOGGING_SEVERITY_REGEX**

Journaux de composant Siebel toujours surveillés

Les journaux de composant sont toujours surveillés pour 10 composants Siebel.

Tableau 212. Alias et noms des composants Siebel pour lesquels les journaux de composant sont toujours surveillés	
Alias du composant	**Nom du composant**
SCCObjMgr	Call Center Object Manager
SMObjMgr	Marketing Object Manager
SSEObjMgr	Sales Object Manager
CommInboundRcvr	Communications Inbound Receiver
CommOutboundMg	Communications Outbound Manager
CommSessionMgr	Communications Session Manager
WorkMon	Workflow Monitor Agent
WfProcBatchMgr	Workflow Process Batch Manager
WfProcMgr	Workflow Process Manager
SiebSrvr	Siebel Server

Configuration de la surveillance Sterling Connect Direct

Vous devez configurer l'Agent Sterling Connect Direct pour qu'il puisse collecter les données issues des serveurs Connect Direct afin de surveiller les statistiques du transfert de fichiers et la santé des serveurs Connect Direct.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel à la page Software Product Compatibility Reports for Sterling Connect Direct agent

Pourquoi et quand exécuter cette tâche

- Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser la fenêtre IBM Cloud Application Performance Management ou le fichier de réponses silencieux.
- Pour configurer l'agent sur les systèmes Linux, vous pouvez exécuter le script et répondre aux invites, ou utiliser le fichier de réponses silencieux.

Configuration de l'agent sur des systèmes Windows

Vous pouvez utiliser la fenêtre IBM Cloud Application Performance Management pour configurer l'agent sur des systèmes Windows.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Modèle** dans la colonne **Tâche/sous-système**, puis cliquez sur **Configuration de l'agent**.
3. Dans la zone **Enter a unique instance name**, entrez le nom d'instance de l'agent et cliquez sur **OK**.

   Remarque : Limitez la longueur du nom d'instance de l'agent, de préférence entre 7 et 10 caractères.
4. Dans la fenêtre **Monitoring Agent for Sterling Connect Direct**, sous l'onglet **Connect Direct Server Details**, spécifiez les valeurs des paramètres de configuration et cliquez sur **OK**.

   Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 807.
5. Cliquez sur **Suivant**.
6. Dans l'onglet Java Parameters, conservez les valeurs par défaut et cliquez sur **Suivant**.
7. Dans l'onglet Configuration client de l'interface de programme d'application Java, cliquez sur **OK**.
8. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur l'instance d'agent créée, puis cliquez sur **Démarrer** pour démarrer l'agent.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console, voir «Démarrage de la console Cloud APM», à la page 1003.

Pour obtenir de l'aide sur le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration de l'agent sur des systèmes Linux

Pour configurer l'agent sur des systèmes d'exploitation Linux, vous pouvez exécuter le script ou répondre à des invites.

Procédure

1. Dans la ligne de commande, modifiez le chemin d'accès au répertoire d'installation de l'agent. Par exemple : `/opt/ibm/apm/agent/bin`
2. Exécutez la commande : **`/sterling_connect_direct-agent.sh config nom_instance`**.

   Remarque : *nom_instance* est le nom que vous souhaitez attribuer à l'instance d'agent.
3. La ligne de commande affiche le message : `Edit 'Monitoring Agent for Sterling Connect Direct' setting? [1=Yes, 2=No]`.
4. Entrez 1 pour éditer les paramètres.
5. A l'invite, indiquez les valeurs des paramètres de configuration. Pour plus d'informations sur les paramètres de configuration, voir «Paramètres de configuration de l'agent», à la page 807.
6. Exécutez la commande suivante pour démarrer l'agent : **`./sterling_connect_direct-agent.sh start nom_instance`**

Que faire ensuite
Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir la rubrique «Démarrage de la console Cloud APM», à la page 1003.

Pour obtenir de l'aide sur le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration de l'agent. Ce mode de configuration est appelé mode silencieux.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le fichier de réponses silencieux pour configurer Monitoring Agent for Sterling Connect Direct sur les systèmes Linux and Windows. Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

1. Dans un éditeur de texte, ouvrez le fichier de réponses silencieux dans *rép_install*/samples/sterling_connect_direct_silent_config.txt.
2. Entrez le nom du serveur, le nom d'utilisateur, le mot de passe et le répertoire d'installation dans le fichier et sauvegardez-le.
3. Dans l'invite de commande, accédez à *rép_install*/bin et exécutez la commande.

   Linux AIX `./sterling_connect_direct-agent.sh config <nom_instance>` *rép_install*/samples/sterling_connect_direct_silent_config.txt.

   Windows `./sterling_connect_direct-agent.bat config <nom_instance>` *rép_install*/samples/sterling_connect_direct_silent_config.txt.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Pour obtenir de l'aide sur le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.

Paramètres de configuration de l'agent

Lorsque vous configurez Monitoring Agent for Sterling Connect Direct, vous pouvez définir les valeurs des paramètres de configuration.

Le tableau ci-après contient les descriptions détaillées des paramètres de configuration de Monitoring Agent for Sterling Connect Direct.

Tableau 213. Noms et descriptions des paramètres de configuration

Nom du paramètre	Description	Zone obligatoire
Nom d'instance	La valeur par défaut de cette zone est identique à celle que vous indiquez dans la zone **Enter a unique instance name**.	Oui
Nom du serveur	Nom d'hôte ou IP du serveur Sterling Connect Direct.	Oui
Port du serveur	Port du serveur Sterling Connect Direct. La valeur par défaut pour Sterling Connect Direct est 1363.	Oui

Tableau 213. Noms et descriptions des paramètres de configuration (suite)		
Nom du paramètre	**Description**	**Zone obligatoire**
Nom d'utilisateur	Nom d'utilisateur permettant de se connecter au serveur Sterling Connect Direct.	Oui
Mot de passe	Mot de passe permettant de se connecter au serveur Sterling Connect Direct.	Oui
Répertoire de base Java	Chemin d'accès au dossier où Java est installé.	Non
Niveau de trace Java	Niveau de trace utilisé par les fournisseurs Java. La valeur par défaut pour Sterling Connect Direct est Error	Oui
Arguments JVM	Ce paramètre permet d'indiquer une liste facultative d'arguments pour la machine virtuelle Java.	Non
Chemin d'accès aux classes pour les fichiers JAR	Chemin d'accès aux fichiers JAR requis par le fournisseur de données d'interface de programme d'application Java qui ne sont pas inclus avec l'agent.	Non

Configuration de la surveillance Sterling File Gateway

Monitoring Agent for Sterling File Gateway surveille l'application IBM Sterling File Gateway à l'aide des API REST business-to-business (B2B) et de la base de données de passerelle de fichiers. Vous devez configurer l'Agent Sterling File Gateway pour qu'il puisse collecter les données issues des sources de données et surveiller les statistiques et la santé de l'application Sterling File Gateway. Vous pouvez configurer l'agent sur les systèmes Windows et Linux.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel à la page Software Product Compatibility Reports for Sterling File Gateway agent
- Vérifiez que les API REST B2B sont installées sur votre noeud de passerelle de fichiers. Pour plus d'informations sur l'installation de l'API REST B2B, voir «Installation de l'API REST B2B», à la page 808.

Pourquoi et quand exécuter cette tâche

L'Agent Sterling File Gateway est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

- Pour configurer l'agent sur des systèmes Windows, vous pouvez utiliser la fenêtre **IBM Performance Management** ou le fichier de réponses silencieux.
- Pour configurer l'agent sur les systèmes Linux, vous pouvez exécuter le script et répondre aux invites, ou utiliser le fichier de réponses silencieux.

Installation de l'API REST B2B

Vous pouvez installer et configurer les API REST business-to-business (B2B) sur votre noeud Sterling File Gateway. Les API REST B2B sont disponibles dans le programme d'installation de B2B Integrator (V5.2.6.2).

Procédure

1. Accédez au répertoire `<rép_install>/bin`.

   Où *rép_install* est le répertoire du programme d'installation de l'agent pour B2B Integrator.

2. Exécutez la commande suivante :

   - Linux `./InstallService.sh/rép_install/bin/b2bAPIs_10000602.jar`

     Où *<rép_install>* est l'emplacement d'extraction du contenu du fichier de support.
   - Windows `./InstallService.cmd/rép_install/bin/b2bAPIs_10000602.jar`

     Où *<rép_install>* est le dossier du programme d'installation de B2B.

Configuration de l'Agent Sterling File Gateway sur des systèmes Windows

Vous pouvez configurer l'Agent Sterling File Gateway sur des systèmes d'exploitation Windows à l'aide de la fenêtre **IBM Cloud Application Performance Management**. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Pourquoi et quand exécuter cette tâche

L'Agent Sterling File Gateway fournit les valeurs par défaut de certains paramètres. Vous pouvez spécifier différentes valeurs pour ces paramètres.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Monitoring Agent for Sterling File Gateway**, puis sur **Configuration de l'agent**.

   A faire : La première fois que vous configurez l'agent, l'option **Configuration de l'agent** n'est pas disponible. Pour reconfigurer l'agent, cliquez sur **Reconfigurer**.
3. Dans la fenêtre Agent Sterling File Gateway, procédez comme suit :
   a) Entrez un nom unique pour l'instance d'Agent Sterling File Gateway et cliquez sur **OK**.
   b) Dans l'onglet relatif aux **détails d'API B2B**, indiquez les valeurs des paramètres de configuration, puis cliquez sur **Suivant**.
   c) Dans l'onglet relatif aux **détails de base de données**, indiquez les valeurs des paramètres de configuration, puis cliquez sur **Suivant**.
   d) Dans l'onglet relatif à l'**API Java**, indiquez les valeurs des paramètres de configuration, puis cliquez sur **OK**.

   Pour plus d'informations sur les paramètres de configuration dans chaque onglet de la fenêtre Agent Sterling File Gateway, consultez les rubriques suivantes :

   - «Paramètres de configuration des détails de l'API B2B», à la page 813
   - «Paramètres de configuration des détails de la base de données», à la page 814
   - «Paramètres de configuration de l'API Java», à la page 814
4. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Agent Sterling File Gateway**, puis sur **Démarrer**.

Configuration de l'Agent Sterling File Gateway sur les systèmes Linux

Vous pouvez exécuter le script de configuration et répondre aux invites pour configurer l'Agent Sterling File Gateway sur les systèmes d'exploitation Linux.

Procédure

1. Accédez à la ligne de commande et exécutez la commande **<rép_install>/bin/sterling_file_gateway-agent.sh config nom_instance**.

   Où *nom_instance* est le nom à attribuer à l'instance, et *rép_install* est le chemin d'accès au répertoire d'installation de l'agent.

2. Vous êtes invité à saisir des valeurs pour tous les paramètres de configuration obligatoires. Vous pouvez modifier les valeurs par défaut des paramètres de configuration.

   Pour plus d'informations sur les paramètres de configuration, voir les rubriques suivantes :

   - «Paramètres de configuration des détails de l'API B2B», à la page 813
   - «Paramètres de configuration des détails de la base de données», à la page 814
   - «Paramètres de configuration de l'API Java», à la page 814
3. Pour démarrer l'agent, exécutez la commande **<rép_install>/bin/sterling_file_gateway-agent.sh start nom_instance**.

Configuration de l'Agent Sterling File Gateway à l'aide du fichier de réponses silencieux

Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'Agent Sterling File Gateway sans répondre aux invites quand vous exécutez le script de configuration. Vous pouvez configurer l'agent qui utilise le fichier de réponses silencieux sur les systèmes Windows et Linux. Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration de l'agent. Ce mode de configuration est appelé mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

- Pour configurer l'Agent Sterling File Gateway en mode silencieux, procédez comme suit :
  a) Dans un éditeur de texte, ouvrez le fichier `sterling_file_gatway_silent_config.txt` disponible à l'emplacement suivant :
     – Linux *rép_install*`/samples/sterling_file_gatway_silent_config.txt`

       Par exemple : **/opt/ibm/apm/agent/samples/sterling_file_gateway_silent_config.txt**
     – Windows *rép_install*`\samples\sterling_file_gateway_silent_config.txt`

       Par exemple : **C:\IBM\APM\samples\sterling_file_gateway_silent_config.txt**
  b) Dans le fichier `sterling_file_gateway_silent_config.txt`, spécifiez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.

     Pour plus d'informations sur les paramètres de configuration, voir les rubriques suivantes :
     – «Paramètres de configuration des détails de l'API B2B», à la page 813
     – «Paramètres de configuration des détails de la base de données», à la page 814
     – «Paramètres de configuration de l'API Java», à la page 814
  c) Sauvegardez et fermez le fichier `sterling_file_gateway_silent_config.txt` et exécutez la commande suivante :
     – Linux *rép_install*`/bin/sterling_file_gateway-agent.sh config` *nom_instance* *rép_install*`/samples/sterling_file_gateway_silent_config.txt`

Par exemple : **/opt/ibm/apm/agent/bin/sterling_file_gateway-agent.sh config nom_instance /opt/ibm/apm/agent/samples/ sterling_file_gateway_silent_config.txt**

– Windows *rép_install*/bin/sterling_file_gateway-agent.bat config *nom_instance* *rép_install*/samples/sterling_file_gateway_silent_config.txt

Par exemple : **C:\IBM\APM\bin\sterling_file_gateway-agent.bat config nom_instance C:\IBM\APM\samples\sterling_file_gateway_silent_config.txt**

Où *nom_instance* est le nom à attribuer à l'instance et *rép_install* est le chemin d'accès au répertoire d'installation de l'agent.

Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.

d) Exécutez la commande suivante pour démarrer l'agent :

– Linux *rép_install*/bin/sterling_file_gateway-agent.sh start *nom_instance*

Par exemple : **/opt/ibm/apm/agent/bin/sterling_file_gateway-agent.sh start nom_instance**

– Windows *rép_install*\bin\sterling_file_gateway-agent.bat start *nom_instance*

Par exemple : **C:\IBM\APM\bin\sterling_file_gateway-agent.bat start nom_instance**

Configuration de variables d'environnement d'agent pour le fournisseur de données sous Linux

Vous pouvez configurer les variables d'environnement de l'Agent Sterling File Gateway pour le fournisseur de données sur les systèmes d'exploitation Linux.

Pourquoi et quand exécuter cette tâche

L'Agent Sterling File Gateway fournit des variables d'environnement que vous pouvez configurer pour le fournisseur de données.

Procédure

1. Accédez au répertoire <rép_install>/agent/config.
2. Ouvrez le fichier .fg.environment dans un éditeur et éditez les variables d'environnement.

   Pour plus d'informations sur les variables d'environnement d'agent que vous pouvez configurer, voir «Variables d'environnement du fournisseur de données», à la page 812.

Configuration de variables d'environnement d'agent pour le fournisseur de données sous Windows

Vous pouvez configurer les variables d'environnement de l'Agent Sterling File Gateway pour le fournisseur de données sur les systèmes d'exploitation Windows à l'aide de la fenêtre **IBM Performance Management**.

Pourquoi et quand exécuter cette tâche

L'Agent Sterling File Gateway fournit des variables d'environnement que vous pouvez configurer pour le fournisseur de données.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > > **Agents IBM Monitoring** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur l'instance d'agent et cliquez sur **Advanced** > **Edit ENV File**, puis éditez les valeurs par défaut des variables d'environnement.

   Pour plus d'informations sur les variables d'environnement d'agent que vous pouvez configurer, voir «Variables d'environnement du fournisseur de données», à la page 812.

Variables d'environnement du fournisseur de données

Après avoir configuré l'Agent Sterling File Gateway, vous pouvez modifier certaines valeurs de durée de seuil relatives à la collecte de données de l'agent. Vous pouvez spécifier ces valeurs dans le fichier d'environnement de l'agent.

Le tableau ci-après contient une description détaillée des variables d'environnement du fournisseur de données.

Tableau 214. Nom et description des variables d'environnement du fournisseur de données

Nom du paramètre	Description
Durée de collecte pour le transfert des fichiers (en heures) (**KFG_FILE_ARRIVED_INTERVAL**)	Durée en heures pendant laquelle l'agent collecte les données pour les transferts de fichiers. La valeur par défaut est 24 heures.
Intervalles de collecte pour les activités de transfert de fichiers qui s'affichent sous forme d'un graphique à courbes (en heures) (**KFG_FILE_ACTIVITY_INTERVAL**)	Durée en heures pendant laquelle l'agent collecte les données pour les activités de transfert de fichiers. La valeur par défaut est 1 heure. Par exemple, l'agent collecte les activités de transfert de fichiers qui se sont produites pendant la dernière heure. Ces données sont visibles sous forme de graphiques à courbes sur la page de l'instance. La valeur par défaut est 1 heure.
Intervalle de seuil des partenaires inactifs (en jours) (**KFG_INACTIVE_PARTNERS_INTERVAL**)	Durée de seuil pendant laquelle le partenaire est inactif ou pendant laquelle il n'a ni reçu ni transféré de fichier. La valeur par défaut est 10 jours. Par exemple, si un partenaire n'a ni reçu ni transféré de fichier ces 10 derniers jours, il apparaît comme "Inactive" sur l'agent.
Nombre maximal de fichiers journaux du fournisseur de données (**KFG_LOG_FILE_MAX_COUNT**)	Nombre maximal de fichiers journaux créés par le fournisseur de données avant qu'il remplace les anciens fichiers journaux. La valeur par défaut est 10.
Taille maximale en ko de chaque journal du fournisseur de données (**KFG_LOG_FILE_MAX_SIZE**)	Taille maximale en ko qu'un fichier journal de fournisseur de données doit atteindre avant que le fournisseur de données ne crée un autre fichier journal. La valeur par défaut est 5190 ko.

Tableau 214. Nom et description des variables d'environnement du fournisseur de données (suite)	
Nom du paramètre	**Description**
Niveau de détail dans le journal du fournisseur de données (**KFG_LOG_LEVEL**)	Niveau des détails inclus dans le fichier journal que le fournisseur de données crée. La valeur par défaut est 4 (Info). Les valeurs suivantes sont valides : • 1 (Off) : aucun message n'est consigné. • 2 (Severe) : seules les erreurs sont consignées. • 3 (Warning) : toutes les erreurs et tous les messages consignés au niveau Severe et les erreurs potentielles qui peuvent entraîner un comportement non souhaité. • 4 (Info) : toutes les erreurs et tous les messages consignés au niveau Warning et les messages d'information de niveau supérieur qui décrivent l'état du fournisseur de données pendant son traitement. • 5 (Fine) : toutes les erreurs et tous les messages consignés au niveau Info et les messages d'information de niveau inférieur qui décrivent l'état du fournisseur de données pendant son traitement. • 6 (Finer) : toutes les erreurs et tous les messages consignés au niveau Fine plus les messages d'information détaillés, tels que les informations sur le profil de performance et les données de débogage. Si vous sélectionnez cette option, cela peut affecter les performances de l'agent de surveillance. Ce paramètre n'est destiné qu'à être utilisé comme un outil pour l'identification des problèmes, en collaboration avec l'équipe de support IBM. • 7 (Finest) : toutes les erreurs et tous les messages consignés au niveau Fine et les messages d'information les plus détaillés qui incluent les messages et les données de programmation de niveau inférieur. Si vous sélectionnez cette option, cela risque d'affecter les performances de l'agent de surveillance. Ce paramètre n'est destiné qu'à être utilisé comme un outil pour l'identification des problèmes, en collaboration avec l'équipe de support IBM. • 8 (All) : toutes les erreurs et tous les messages sont consignés.
Extraction d'événements pour tous les transferts de fichiers (**KFG_ALL_FGEVENTS**)	Indicateur d'extraction des événements pour tous les transferts de fichiers. Les valeurs admises sont Yes ou No. La valeur par défaut est No. Si la valeur est définie sur No, l'agent extrait les événements associés aux transferts de fichiers ayant échoué pour une durée configurable par l'utilisateur. Si la valeur est définie sur Yes, l'agent extrait les événements associés à tous les transferts de fichiers pour une durée configurable par l'utilisateur.

Paramètres de configuration des détails de l'API B2B

Lorsque vous configurez l'Agent Sterling File Gateway, vous devez spécifier les valeurs des paramètres de configuration pour les détails de l'API business-to-business (B2B).

Le tableau ci-après contient une description détaillée des paramètres de configuration des détails de l'API B2B.

Tableau 215. Nom et description des paramètres de configuration des détails de l'API B2B	
Nom du paramètre	**Description**
Nom de l'instance (**KFG_Instance_Name**)	Nom de l'instance. **Restriction :** La zone Nom d'instance contient le nom de l'instance que vous spécifiez lorsque vous configurez l'agent pour la première fois. Lorsque vous reconfigurez l'agent, vous ne pouvez pas modifier le nom d'instance de l'agent.
Nom du serveur (**KFG_API_SERVICES_Node_ADDRESS**)	Nom d'hôte ou adresse IP du service d'API B2B.
Port du serveur (**KFG_API_SERVICES_PORT**)	Port de l'API B2B.
Nom d'utilisateur (**KFG_API_SERVICES_USERNAME**)	Nom d'utilisateur permettant de se connecter au service d'API B2B.
Mot de passe (**KFG_API_SERVICES_PASSWORD**)	Mot de passe associé au nom d'utilisateur permettant de se connecter au service d'API B2B.

Paramètres de configuration des détails de la base de données

Lorsque vous configurez l'Agent Sterling File Gateway, vous devez spécifier les valeurs des paramètres de configuration pour les détails de la base de données.

Le tableau ci-après contient une description détaillée des paramètres de configuration des détails de la base de données.

Tableau 216. Nom et description des paramètres de configuration des détails de la base de données	
Nom du paramètre	**Description**
Nom du serveur de base de données (**KFG_DB_Node_ADDRESS**)	Nom d'hôte ou adresse IP du serveur de base de données Sterling File Gateway.
Utilisateur de la base de données (**KFG_DB_USERNAME**)	Nom de l'utilisateur de la base de données.
Mot de passe de la base de données (**KFG_DB_PASSWORD**)	Mot de passe de la base de données.
Port de la base de données (**KFG_DB_PORT**)	Port de la base de données.
Type de base de données (**KFG_DB_TYPE**)	Type de la base de données.

Paramètres de configuration de l'API Java

Lorsque vous configurez l'Agent Sterling File Gateway, vous devez spécifier les valeurs des paramètres de configuration pour l'API Java.

Le tableau ci-après contient une description détaillée des paramètres de configuration de l'API Java.

Tableau 217. Nom et description des paramètres de configuration de l'API Java	
Nom du paramètre	**Description**
Chemin d'accès aux classes pour le fichier JAR externe (**KFG_CLASSPATH**)	Chemin d'accès au fichier JAR du pilote de base de données que vous voulez spécifier pour la base de données correspondante.

Configuration de la surveillance de Sybase Server

L'agent Sybase offre un point central de gestion des bases de données réparties. Il collecte les informations requises pour que les administrateurs de base de données et système puissent examiner les performances du système Sybase Server, détecter rapidement les problèmes et les empêcher. Les administrateurs de base de données et système peuvent définir les options et seuils requis pour déclencher des alertes lorsque le système atteint ces seuils.
Vous devez configurer Monitoring Agent for Sybase Server pour surveiller le serveur Sybase.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'agent Sybase.

Pourquoi et quand exécuter cette tâche

Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

L'agent Sybase est un agent multi-instance ; vous devez configurer et démarrer chaque instance d'agent manuellement.

Procédure

1. Configurez l'agent de surveillance.
   - «Configuration de l'agent à l'aide de l'interface de ligne de commande», à la page 817
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 818
2. Démarrez et arrêtez l'agent de surveillance à l'aide de la commande d'agent **sybase-agent**.

   Pour plus d'informations sur la commande **sybase-agent**, voir *Utilisation des commandes de l'agent* dans https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/welcome.htm.
3. Connectez l'agent de surveillance au serveur Performance Management à l'aide de la commande **agent2server**.

   Pour plus d'informations sur la commande **agent2server**, voir *Utilisation des commandes de l'agent* dans https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/welcome.htm.

Octroi de droits d'accès

Vous devez octroyer des droits à l'ID utilisateur utilisé pour surveiller le serveur Sybase.

Avant de commencer

Installez l'agent Sybase.

Vous devez disposer du rôle d'administrateur de base de données pour accorder des droits.

Pourquoi et quand exécuter cette tâche

L'ID utilisateur utilisé par l'agent de surveillance doit avoir accès aux tables Sybase et aux tables de surveillance installées.

Vous pouvez effectuer les tâches suivantes :

- Créer un ID utilisateur pour l'agent de surveillance.
- Octroyer des droits au nouvel ID utilisateur et aux tables de surveillance installées.

Si vous n'exécutez pas l'agent Sybase en tant qu'utilisateur `root`, assurez-vous que votre ID utilisateur appartient au groupe `Sybase` et qu'il possède un accès en lecture aux fichiers journaux Sybase.

Procédure

1. Entrez la commande correspondant au système d'exploitation que vous utilisez.
   - Windows

     ```
     cd rép_install\tmaitm6\SQLLIB
     ```

   - UNIX

     ```
     cd rép_install/misc
     ```

   Où *rép_install* représente le répertoire de base dans lequel le serveur Sybase est installé.
2. Utilisez la commande **isql** pour vous connecter au serveur Sybase en tant qu'utilisateur `sa`.
3. Exécutez la commande suivante pour configurer l'ID utilisé par l'agent Sybase pour communiquer avec le serveur Sybase :

   ```
   1>sp_addlogin nom_utilisateur, mdp 2>g
   ```

   Où :
   - *nom_utilisateur* représente l'ID utilisateur. Par défaut, il s'agit de `tivoli`.

     Si l'ID utilisateur n'est pas `tivoli`, éditez le fichier `koygrant.sql` et remplacez `tivoli` par l'ID utilisateur approprié.
   - *mdp* représente le mot de passe de l'utilisateur.

   Remarque :

   Emplacement du fichier `koygrant.sql` :
   - Windows `\opt\ibm\apm\agent\misc\`
   - UNIX `/opt/ibm/apm/agent/misc/`
4. Exécutez la commande suivante pour octroyer des droits aux tables de la base de données :

   ```
   isql -U sa -P mdp -S nomserveur -i chemin_fichier_koygrantkoygrant.sql
   ```

   Où :
   - *mdp* représente le mot de passe de l'utilisateur `sa`.
   - *nomserveur* représente le nom du serveur de base de données.
   - *chemin_fichier_koygrant* correspond à l'emplacement suivant :

     Remarque :

     – Windows `\opt\ibm\apm\agent\misc\`

     – UNIX `/opt/ibm/apm/agent/misc/`
5. Exécutez la commande suivante pour créer les tables proxy utilisées pour les tables de surveillance installées :

   ```
   isql -U sa -P mdp -S nomserveur
        -i $SYBASE/ASE-12_5/scripts/installmontables
   ```

   Où :
   - *mdp* représente le mot de passe de l'utilisateur `sa`.
   - *nomserveur* représente le nom du serveur de base de données.

Que faire ensuite

Une fois que les droits ont été octroyés, vous pouvez configurer l'agent de surveillance.

Configuration de l'agent à l'aide de l'interface de ligne de commande

Vous pouvez configurer Monitoring Agent for Sybase Server à l'aide de l'interface de ligne de commande.

Avant de commencer

L'agent Sybase ne prend pas en charge la configuration à distance. Par conséquent, vous devez vous assurer que le serveur Sybase est installé sur le même hôte que l'agent Sybase.

L'agent Sybase ne prend en charge que Sybase Server versions 15.7 et 16.0.

L'ID utilisateur permettant de se connecter au serveur de base de données est créé.

Pourquoi et quand exécuter cette tâche

L'agent Sybase est un agent multi-instance ; vous devez configurer et démarrer chaque instance d'agent manuellement.

Procédure

1. Exécutez la commande ci-après pour configurer l'agent.
   - Windows

     ```
     rép_install\bin\sybase-agent.batnom_instance
     ```

   - UNIX

     ```
     rép_install/bin/sybase-agent.sh nom_instance
     ```

   Où :
   - *rép_install* est le répertoire d'installation de l'agent.
   - *nom_instance* représente le nom d'instance du serveur Sybase.
2. Lorsque vous êtes invité à saisir des valeurs pour les paramètres ci-après, appuyez sur Entrée pour accepter la valeur par défaut ou spécifiez une valeur, puis appuyez sur Entrée.
   a) Pour le paramètre `Home Directory`, entrez le chemin d'accès du répertoire principal du serveur Sybase.
      - Windows

        L'exemple de `Home Directory` est `\opt\sybase`.
      - UNIX

        L'exemple de `Home Directory` est `/opt/sybase`.

   b) Pour le paramètre `ASE Directory`, entrez le chemin d'accès du serveur de base de données ASE.
      - Windows

        L'exemple d'`ASE Directory` est `\opt\sybase\ASE-12_5`.
      - UNIX

        L'exemple d'`ASE Directory` est `/opt/sybase/ASE-12_5`.

   c) Pour le paramètre `Open Client Directory`, entrez l'emplacement d'installation de Sybase Open Client.
      - Windows

        L'exemple d'`Open Client Directory` est `\opt\sap\ocs-16_0`.
      - UNIX

L'exemple d'`Open Client Directory` est `/opt/sap/ocs-16_0`.

d) Pour le paramètre `USER ID`, entrez l'ID utilisateur utilisé par l'agent de surveillance pour se connecter au serveur Sybase.

La valeur `USER ID` par défaut est `tivoli`.

e) Pour le paramètre `PASSWORD`, entrez le mot de passe de l'ID utilisateur utilisé par l'agent de surveillance pour se connecter au serveur Sybase.

f) Pour le paramètre `VERSION`, entrez la version du serveur Sybase.

L'agent Sybase ne prend en charge que Sybase server versions 15.7 et 16.0.

g) Pour le paramètre `ERROR LOG FILE`, entrez le nom de fichier complet du fichier du journal des erreurs du serveur Sybase.

- Windows

  L'exemple d'`ERROR LOG FILE` est `\opt\sap\ASE-16_0\install\`*`nomserveur`*`.log`.

- UNIX

  L'exemple d'`ERROR LOG FILE` est `/opt/sap/ASE-16_0/install/`*`nomserveur`*`.log`.

Où *nomserveur* correspond au nom du serveur Sybase.

h) Pour le paramètre `EXTENDED`, entrez le paramètre étendu utilisé par le support pour exclure certaines exécutions de curseur. Appuyez éventuellement sur Entrée sans spécifier de valeurs pour exécuter tous les curseurs.

Les options du paramètre `EXTENDED` sont `DBD2,DBD15,KOYSEGD`.

- `DBD2` exclut l'exécution des curseurs pour les ensembles de données Sybase_Database_Detail et Sybase_Database_Summary.
- `DBD15` exclut l'exécution des curseurs pour l'ensemble de données Sybase_Database_Detail.
- `KOYSEGD` exclut l'exécution des curseurs pour l'ensemble de données Sybase_Segment_Detail.

Que faire ensuite

Une fois que la configuration est terminée, vous pouvez démarrer l'agent de surveillance et le connecter au serveur Performance Management.

Pour démarrer l'agent Sybase, utilisez la commande d'agent `sybase-agent`.

Pour connecter l'agent Sybase au serveur Performance Management, utilisez la commande `agent2server`.

Pour plus d'informations sur les commandes `sybase-agent` et `agent2server`, voir *Utilisation des commandes de l'agent* dans https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/welcome.htm.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Vous pouvez configurer Monitoring Agent for Sybase Server à l'aide du fichier de réponses silencieux.

Avant de commencer

L'agent Sybase ne prend pas en charge la configuration à distance. Par conséquent, vous devez vous assurer que le serveur Sybase est installé sur le même hôte que l'agent Sybase.

L'agent Sybase ne prend en charge que Sybase server versions 15.7 et 16.0.

L'ID utilisateur permettant de se connecter au serveur de base de données est créé.

Pourquoi et quand exécuter cette tâche

L'agent Sybase est un agent multi-instance ; vous devez configurer et démarrer chaque instance d'agent manuellement.

Vous devez éditer le fichier de réponses silencieux et exécuter la commande d'agent pour configurer l'agent de surveillance.

Procédure

1. Editez le fichier de réponses silencieux.
   - Windows

     Le fichier de réponses silencieux se trouve à l'emplacement suivant : *rép_install*\samples\sybase_silent_config.txt.
   - UNIX

     Le fichier de réponses silencieux se trouve à l'emplacement suivant : *rép_install*/samples/sybase_silent_config.txt.

   Où *rép_install* représente le répertoire d'installation de l'agent.

   a) Pour le paramètre Home Directory, spécifiez le répertoire principal du serveur Sybase.
      - Windows

        L'exemple de Home Directory est \opt\sybase.
      - UNIX

        L'exemple de Home Directory est /opt/sybase.

   b) Pour le paramètre ASE Directory, spécifiez le chemin d'accès du serveur de base de données ASE.
      - Windows

        L'exemple d'ASE Directory est \opt\sybase\ASE-12_5.
      - UNIX

        L'exemple d'ASE Directory est /opt/sybase/ASE-12_5.

   c) Pour le paramètre Open Client Directory, spécifiez l'emplacement d'installation de Sybase Open Client.
      - Windows

        L'exemple d'Open Client Directory est \opt\sap\ocs-16_0.
      - UNIX

        L'exemple d'Open Client Directory est /opt/sap/ocs-16_0.

   d) Pour le paramètre USER ID, spécifiez l'ID utilisateur utilisé par l'agent de surveillance pour se connecter au serveur Sybase.

      La valeur USER ID par défaut est tivoli.

   e) Pour le paramètre PASSWORD, spécifiez le mot de passe de l'ID utilisateur utilisé par l'agent de surveillance pour se connecter au serveur Sybase.

   f) Pour le paramètre VERSION, spécifiez la version du serveur Sybase.

      L'agent Sybase ne prend en charge que Sybase server versions 15.7 et 16.0.

   g) Pour le paramètre ERROR LOG FILE, spécifiez le nom de fichier complet du fichier du journal des erreurs du serveur Sybase.
      - Windows

        L'exemple d'ERROR LOG FILE est \opt\sap\ASE-16_0\install*nomserveur*.log.
      - UNIX

        L'exemple d'ERROR LOG FILE est /opt/sap/ASE-16_0/install/*nomserveur*.log.

      Où *nomserveur* correspond au nom du serveur Sybase.

h) Pour le paramètre EXTENDED, spécifiez le paramètre étendu utilisé par le support pour exclure certaines exécutions de curseur. Vous pouvez également ne pas le renseigner pour exécuter tous les curseurs.

Les options du paramètre EXTENDED sont DBD2,DBD15,KOYSEGD.

- DBD2 exclut l'exécution des curseurs pour les ensembles de données Sybase_Database_Detail et Sybase_Database_Summary.
- DBD15 exclut l'exécution des curseurs pour l'ensemble de données Sybase_Database_Detail.
- KOYSEGD exclut l'exécution des curseurs pour l'ensemble de données Sybase_Segment_Detail.

2. Sauvegardez le fichier de réponses silencieux.
3. Exécutez la commande d'agent ci-après pour configurer l'agent de surveillance.
   - Windows

     ```
     rép_install\bin\sybase-agent.bat config nom_instance
      rép_install\samples\sybase_silent_config.txt
     ```

   - UNIX

     ```
     rép_install/bin/sybase-agent.sh config nom_instance
      rép_install/samples/sybase_silent_config.txt
     ```

   Où :

   - *rép_install* est le répertoire d'installation de l'agent.
   - *nom_instance* représente le nom du serveur Sybase.

Que faire ensuite

Une fois que la configuration est terminée, vous pouvez démarrer l'agent de surveillance et le connecter au serveur Performance Management.

Pour démarrer l'agent Sybase, utilisez la commande **sybase-agent**.

Pour connecter l'agent Sybase au serveur Performance Management, utilisez la commande **agent2server**.

Pour plus d'informations sur les commandes **sybase-agent** et **agent2server**, voir *Utilisation des commandes de l'agent* dans https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/welcome.htm.

Désactivation de la lecture de pages modifiées pour la requête

Par défaut, l'agent Sybase active le paramètre `dirty reads` (lecture de pages modifiées) pour exécuter ses requêtes afin d'éviter le verrouillage.
Ce paramètre est activé ou désactivé à l'aide de la variable COLL_USE_NOLOCK.
Lorsqu'il est activé, la requête s'exécute au niveau d'isolement zéro pour éviter le verrouillage.
Pour le désactiver, attribuez la valeur zéro à la variable COLL_USE_NOLOCK.

Avant de commencer

Pour désactiver `dirty reads` pour la requête de l'agent, vérifiez que ce dernier est installé.

Pourquoi et quand exécuter cette tâche

Par défaut, l'agent Sybase active le paramètre `dirty reads`. Pour le désactiver, procédez comme suit.

Procédure

1. Arrêtez l'agent.
2. Attribuez la valeur zéro à la variable COLL_USE_NOLOCK.

- UNIX
  a. Ajoutez **COLL_USE_NOLOCK=0** dans le fichier *CANDLEHOME*/config/.oy.environment.
  b. Sauvegardez et fermez le fichier.
- Windows
  a. Localisez le fichier de l'instance d'agent *CANDLEHOME*\TMAITM6_x64\KOYENV_*NOMINSTANCE*.
  b. Ajoutez la ligne suivante dans le fichier.

     COLL_USE_NOLOCK=0
  c. Sauvegardez et fermez le fichier.

CANDLEHOME est le répertoire d'installation de l'agent.
NOMINSTANCE est le nom d'instance de l'agent.

3. Démarrez l'agent.

Configuration de la surveillance de Synthetic Playback

Vous devez configurer l'Agent Synthetic Playback pour qu'il puisse collecter les données de disponibilité et de performances des applications Web internes. Ces données sont affichées dans le Tableau de bord d'Application Performance.

Pourquoi et quand exécuter cette tâche

Configurez l'Agent Synthetic Playback en exécutant un script et en répondant à des invites. Démarrez le script et vérifiez qu'il est en cours d'exécution.

Important : Seuls les utilisateurs existants du module complémentaire IBM Website Monitoring on Cloud peuvent installer, configurer et exécuter l'Agent Synthetic Playback. L'Website Monitoring est remplacé par l'IBM Cloud Availability Monitoring. Pour plus d'informations, voir «A propos d'Availability Monitoring», à la page 1076.

Procédure

- Pour configurer l'agent en exécutant le script et en répondant aux invites, procédez comme suit :
  a) Entrez *rép_install*/bin/synthetic_playback-agent.sh config où *rép_install* est le répertoire d'installation de l'Agent Synthetic Playback.
  b) A l'invite Edit Monitoring Agent for Synthetic Playback settings, entrez 1 pour continuer.
  c) Lorsque vous êtes invité à entrer un nom de centre de données pour votre point de présence de réexécution, entrez un nom qui identifie l'emplacement de l'agent.

     Important : Sélectionnez un nom décrivant le point de présence de réexécution. Lorsque vous effectuez l'installation de votre agent, vous pouvez sélectionner cet emplacement par nom en tant qu'emplacement de réexécution des transactions synthétiques et afficher les données de transaction à partir de cet emplacement dans le Tableau de bord d'Application Performance.
  d) A l'invite Java parameters, sélectionnez un niveau de trace Java. Appuyez sur Entrée pour choisir le paramètre par défaut ou entrez un nombre compris entre 1 et 8 pour définir un niveau de trace.
  e) A l'invite Class path for external jars, appuyez sur Entrée pour laisser la zone vide ou indiquer l'emplacement d'un fichier JAR externe.
- Pour configurer l'agent à l'aide du fichier de réponses silencieux, procédez comme suit :
  a) Dans un éditeur de texte, ouvrez le fichier synthetic_playback_silent_config.txt disponible à l'emplacement *rép_install*/samples.
  Par exemple :

  Linux /opt/ibm/apm/agent/samples

b) Dans le fichier `synthetic_playback_silent_config.txt`, supprimez la mise en commentaire et affectez des valeurs aux propriétés suivantes :

   – Pour `LOCATION`, définissez ce paramètre sur le nom de votre centre de données ou un nom décrivant où votre agent est installé.
   – Pour `JAVA_TRACE_LEVEL`, définissez ce paramètre sur l'un des niveaux de trace énumérés, tel que `JAVA_TRACE_LEVEL=ERROR`.

   Sauvegardez le fichier.

c) Sur la ligne de commande, accédez au répertoire *rép_install*`/bin`.

d) Exécutez la commande suivante pour configurer l'agent en mode silencieux :

```
synthetic_playback-agent.sh config rép_install/samples/
synthetic_playback_silent_config.txt
```

- Pour démarrer l'Agent Synthetic Playback, entrez : *rép_install*`/bin/synthetic_playback-agent.sh start`.
- Pour vérifier que l'Agent Synthetic Playback est en cours d'exécution, entrez : *rép_install*`/bin/synthetic_playback-agent.sh status`. Pour plus d'informations, voir Tableau 12, à la page 184.

Que faire ensuite

Pour afficher les performances d'applications Web internes, vous devez créer des transactions synthétiques dans Synthetic Script Manager. Pour plus d'informations, voir «Gestion des transactions et des événements synthétiques avec Website Monitoring», à la page 1057.

Activation de la prise en charge de proxy en amont pour l'Agent Synthetic Playback

Activez la prise en charge de proxy en amont pour l'Agent Synthetic Playback afin de surveiller les requêtes HTTP en provenance des applications Web internes à destination des applications Web externes.

Avant de commencer

Vérifiez que vous exécutez bien l'Agent Synthetic Playback version 01.00.05.08 ou suivante. Pour vérifier la version de l'agent que vous exécutez, entrez *rép_install*`/bin/cinfo -t` sur la ligne de commande, où *rép_install* désigne l'emplacement d'installation de l'agent. Si vous exécutez une autre version de l'Agent Synthetic Playback, vous devez télécharger et installer l'Agent Synthetic Playback correctif temporaire 08 d'IBM Cloud Application Performance Management, Private 8.1.4.0 depuis IBM Fix Central (Entrez `Synthetic` dans la zone **Search** ; la liste des correctifs temporaires de l'Agent Synthetic Playback s'affiche alors). Pour des instructions d'installation, voir le fichier readme 8.1.4.0-IBM-IPM-SYNTHETIC-PLAYBACK-AGENT-IF0008.

Pourquoi et quand exécuter cette tâche

Les applications Web internes situées derrière un pare-feu d'entreprise requièrent un proxy en amont pour pouvoir accéder aux ressources Web externes. Configurez le paramètre proxy de l'Agent Synthetic Playback afin de permettre à votre agent de prendre en charge votre proxy en amont. Vous pourrez ainsi surveiller les requêtes HTTP provenant des applications Web internes à destination des applications Web externes.

Procédure

- Pour configurer et activer la prise en charge de proxy en amont pour votre agent, procédez comme suit :

  a) En tant que superutilisateur, configurez les paramètres du proxy en exécutant les commandes suivantes sur la ligne de commande.

```
cd rép_install/agent/lx8266/sn/bin
#./set_proxy.sh
```

Lorsque vous y êtes invité, entrez le chemin d'installation de l'agent qui correspond par défaut à `/opt/ibm/apm/agent`. Entrez le numéro correspondant au type du proxy à configurer pour votre Agent Synthetic Playback.

Exemple :

```
# cd /rép_install/agent/lx8266/sn/bin/
#./set_proxy.sh
please input the agent install path, default is (/opt/ibm/apm/agent)
agent install path is:/opt/ibm/apm/agent
please input the number of proxy type:
1 system proxy
2 manual proxy
3 pac proxy
4 no proxy
```

b) Entrez *rép_install*`/bin/synthetic_playback-agent.sh start` pour redémarrer votre agent.

- Linux Pour désactiver la prise en charge de proxy en amont pour votre agent, exécutez à nouveau la commande `./set_proxy.sh` et sélectionnez `4 no proxy`. Démarrez ensuite l'agent.

Configuration de la surveillance de Tomcat

Vous pouvez configurer Monitoring Agent for Tomcat à l'aide des paramètres personnalisés ou par défaut pour surveiller les ressources des serveurs d'applications Tomcat. L'agent peut être configuré sur les systèmes Windows et Linux.

Avant de commencer

Prenez connaissance des prérequis aux niveaux matériel et logiciel. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent Tomcat.

Pourquoi et quand exécuter cette tâche

L'Agent Tomcat est un agent d'instance multiple. Vous devez créer la première instance et démarrer l'agent manuellement. Le nom de système géré inclut le nom d'instance que vous spécifiez, *nom_instance*`:`*nom_hôte*`:`*cp* par exemple, où *cp* est le code produit à deux caractères. Il est limité à 32 caractères. Le nom d'instance que vous entrez est limité à 28 caractères, en excluant la longueur de votre nom d'hôte. Par exemple, si vous indiquez `TOMCAT2` comme nom d'instance, le nom du système géré est `TOMCAT2:hostname:OT`. Si vous indiquez un nom d'instance long, le nom du système géré est tronqué et le code d'agent ne s'affiche pas entièrement.

Afin d'éviter tout problème de droits lorsque vous configurez l'agent, veillez à utiliser le même ID d'utilisateur superutilisateur ou non superutilisateur que celui utilisé pour installer l'agent. Si vous avez installé votre agent en tant qu'utilisateur sélectionné et que vous voulez le configurer en tant qu'un autre utilisateur, voir «Configuration des agents en tant qu'utilisateur non superutilisateur», à la page 188. Si vous avez installé et configuré votre agent en tant qu'utilisateur sélectionné et que vous voulez démarrer l'agent en tant qu'un autre utilisateur, voir «Démarrage des agents en tant qu'utilisateur non superutilisateur», à la page 1042.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Configuration de l'Agent Tomcat avec les paramètres par défaut

Vous pouvez utiliser les paramètres par défaut de l'Agent Tomcat pour surveiller le serveur Tomcat. Il n'est pas nécessaire de fournir des informations de configuration supplémentaires autres que le nom de la nouvelle instance.

Avant de commencer

Pour pouvoir configurer l'agent avec les paramètres par défaut, assurez-vous que les prérequis suivants sont remplis :

- L'agent est installé dans le répertoire par défaut.
- L'URL du service JMX utilise le port 8686.
- Le serveur Tomcat est configuré sans autorisation JMX.

Pourquoi et quand exécuter cette tâche

A faire : Lorsque vous configurez l'agent avec les paramètres par défaut, la collection des données de suivi et de diagnostic approfondi des transactions n'est pas activée.

Procédure

1. Exécutez la commande suivante :
   Linux `rép_install/bin/tomcat-agent.sh config nom_instance rép_install/samples/tomcat_silent_config.txt`
   Windows `rép_install/bin/tomcat-agent.bat config nom_instance rép_install/samples/tomcat_silent_config.txt`
   Où
   rép_install
   Répertoire d'installation de l'Agent Tomcat.
   nom_instance
   Est le nom que vous voulez attribuer à l'instance.
2. Exécutez la commande suivante pour démarrer l'agent :
   Linux `rép_install/bin/tomcat-agent.sh start nom_instance`
   Windows `rép_install/bin/tomcat-agent.bat start nom_instance`

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent sur les systèmes d'exploitation Windows à l'aide de la fenêtre **IBM Performance Management**.

Avant de commencer

Assurez-vous que les prérequis suivants sont respectés :

- Java est installé sur le serveur Tomcat où l'agent est installé.
- JDK 1.6 ou version ultérieure est défini à l'invite à partir de l'emplacement du programme d'installation de l'agent.
- JMX Remote est activé pour le serveur Tomcat. Pour plus de détails, voir Enabling JMX Remote.
- Le serveur Tomcat est opérationnel.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer l'agent à partir de l'invite de commande. Pour plus de détails, suivez les étapes indiquées dans la rubrique «Configuration de l'Agent Tomcat sur les systèmes Linux», à la page 828 et exécutez les commandes avec l'extension .bat au lieu de .sh. La procédure suivante indique comment configurer l'agent à l'aide du panneau de configuration de l'agent.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Monitoring Agent for Tomcat**.
3. Cliquez sur **Configuration de l'agent**.

   Avertissement : Si **Configuration de l'agent** n'est pas disponible, cliquez sur **Reconfigurer**.
4. Dans la fenêtre **Nom de l'instance**, indiquez un nom unique pour l'instance d'Agent Tomcat et cliquez sur **OK**.

   Restriction : Le MSN ne doit pas contenir plus de 32 caractères.
5. Dans la zone **SERVER NAME**, entrez un nom unique pour identifier le serveur Tomcat qui est surveillé.
6. Dans la fenêtre **Java Parameter Settings**, effectuez l'une des actions suivantes :
   - Cliquez sur **Next** pour accepter l'emplacement d'installation par défaut de Java, Le chemin d'installation par défaut est `C:\IBM\APM\java\java80_x64\jre`.
   - Dans la zone **Java Home**, indiquez le chemin d'accès si IBM Java est installé à un autre emplacement.
7. Dans la fenêtre **JSR-160-Complaint Server**, indiquez les détails des paramètres suivants :
   a) Dans la zone **ID utilisateur JMX**, indiquez l'ID de l'utilisateur utilisé pour se connecter au serveur MBean Tomcat lorsque l'autorisation JMX est activée dans Tomcat.
   b) Dans la zone **Mot de passe JMX**, indiquez le mot de passe de l'utilisateur JMX lorsque l'autorisation JMX est activée dans Tomcat.
   c) Dans la zone **Adresse URL de service JMX**, entrez l'URL utilisée pour se connecter au serveur MBean Tomcat.

      Le format de l'URL est `service:jmx:rmi:///jndi/rmi://`*`nom_hôte`*`:`*`numéro_port`*`/jmxrmi`. L'adresse URL par défaut est valide lorsque le serveur s'exécute sur l'hôte local et utilise le port 8686 comme port JMX. Vous pouvez modifier le nom d'hôte et le numéro de port dans l'URL en conservant le même format.
   d) Dans la liste **Data Collector Configuration**, sélectionnez Oui si vous souhaitez activer la collecte des données de suivi et d'analyse approfondie des transactions.
8. Dans la fenêtre **Monitoring Agent for Tomcat**, cliquez avec le bouton droit de la souris sur l'instance de l'Agent Tomcat et cliquez sur **Start**.
9. Activez la collecte des données de suivi des transactions et d'analyse approfondie et redémarrez le serveur Tomcat.

Que faire ensuite

Si l'Agent Tomcat est exécuté en tant que service, configurez le collecteur de données Tomcat après avoir configuré l'agent sous Windows. Pour plus d'informations, voir «Configuration du collecteur de données Tomcat », à la page 827.

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Fourniture de la stratégie de sécurité locale pour l'exécution de Monitoring Agent for Tomcat sous Windows en tant qu'utilisateur non-administrateur

Des stratégies de sécurité locales sont disponibles pour permettre à un utilisateur non-administrateur d'exécuter un Monitoring Agent for Tomcat sous Windows.

Pourquoi et quand exécuter cette tâche

La combinaison des deux stratégies de sécurité locales suivantes permet à un utilisateur non-administrateur d'exécuter l'Agent Tomcat sous Windows. Avec ces stratégies, l'utilisateur non-administrateur peut démarrer/arrêter, configurer un Agent Tomcat et en vérifier les données :

1. Déboguer les programmes.
2. Ouvrir une session en tant que service.

Suivez la procédure fournie pour accorder les droits de sécurité locaux à un utilisateur non-administrateur.

Procédure

1. Accédez à TEMA et définissez les paramètres de démarrage de l'agent Tomcat pour un utilisateur non-administrateur.
2. Ajoutez l'utilisateur non-administrateur sous le dossier d'installation de l'agent Tomcat et accordez des droits complets à ce dossier.
3. Ajoutez l'utilisateur non-administrateur sous la clé de Registre HKEY_LOCAL_MACHINE et cliquez sur **Droits complets**.
4. Exécutez la commande **`secpol.msc`** dans le **menu Démarrer** pour ouvrir les stratégies de sécurité locales.
5. Ensuite, pour ajouter un utilisateur non-administrateur dans les stratégies, reportez-vous à «Droits de la stratégie de sécurité locale», à la page 826.
6. Redémarrez l'agent Tomcat.
7. Vérifiez le statut des agents Tomcat ainsi que les données sur le portail APM.

Droits de la stratégie de sécurité locale

Octroi du droit Déboguer les programmes

Pourquoi et quand exécuter cette tâche

Pour accorder le droit Déboguer les programmes, suivez la procédure relative à l'Agent Tomcat décrite ci-dessous :

Procédure

1. Cliquez sur **Démarrer > Outils d'administration > Stratégie de sécurité locale**. La fenêtre **Stratégie de sécurité locale** s'affiche.
2. Développez **Attribution des droits utilisateur**. La liste des droits utilisateur s'affiche.
3. Cliquez deux fois sur la stratégie **Déboguer les programmes**. La fenêtre **Propriétés de Déboguer les programmes** apparaît.
4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre **Sélectionner des utilisateurs ou des groupes** apparaît.
5. Dans la zone Entrer les noms d'objet à sélectionner, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **OK**.

Octroi du droit Ouvrir une session en tant que service

Pourquoi et quand exécuter cette tâche
Pour accorder le droit Ouvrir une session en tant que service, suivez la procédure relative à l'Agent Tomcat décrite ci-dessous :

Procédure

1. Cliquez sur **Démarrer > Outils d'administration > Stratégie de sécurité locale**. La fenêtre **Stratégie de sécurité locale** s'affiche.
2. Développez **Attribution des droits utilisateur**. La liste des droits utilisateur s'affiche.
3. Cliquez deux fois sur la stratégie **Ouvrir une session en tant que service**. La fenêtre **Propriétés de Ouvrir une session en tant que service** apparaît.
4. Cliquez sur **Ajouter un utilisateur ou un groupe**. La fenêtre **Sélectionner des utilisateurs ou des groupes** apparaît.
5. Dans la zone Entrer les noms d'objet à sélectionner, entrez le nom du compte utilisateur auquel vous voulez accorder des droits, puis cliquez sur **OK**.
6. Cliquez sur **OK**.

Configuration du collecteur de données Tomcat
Si l'Agent Tomcat est exécuté en tant que service, configurez le collecteur de données Tomcat après avoir configuré l'agent sous Windows en suivant les instructions fournies ici.

Pourquoi et quand exécuter cette tâche

Une fois que l'instance de l'Agent Tomcat a été configurée et démarrée, le fichier `setenv.bat` dans `/CANDLEHOME/setenv_<nom_instance>.bat` est généré ou mis à jour. Ce fichier contient les paramètres de configuration du collecteur de données nécessaires à la configuration du collecteur de données Tomcat.

Procédure

1. Ouvrez la fenêtre **Propriétés Apache Tomcat** et cliquez sur **Java**
2. Ouvrez `setenv_<nomInstance>.bat` à partir de l'emplacement `/CANDLEHOME/setenv_<nom_instance>.bat`
3. Copiez la valeur du paramètre **JAVA_OPTS** à partir de `setenv_<nom_instance>.bat` présenté dans le bloc :

```
agentlib:am_ibm_16=C:\IBM\APM\otdchome\7.3.0.13.0\runtime\TOMTKWIN1
-Xbootclasspath/p:C:\IBM\APM\otdchome\7.3.0.13.0\toolkit\lib\bcm-bootstrap.jar
-Djava.security.policy=C:\IBM\APM\otdchome\7.3.0.13.0\itcamdc\etc\datacollector.policy
-Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=
C:\IBM\APM\otdchome\7.3.0.13.0\runtime\TOMTKWIN1\TOM_TK_1_DCManual.txt
-Dcom.ibm.tivoli.itcam.serverHome=C:\TOMCAT_9\apache-tomcat-9.0.5\apache-tomcat-9.0.5
-Dam.home=C:\IBM\APM\otdchome\7.3.0.13.0\itcamdc
-Dcom.ibm.tivoli.itcam.toolkit.runtime.dir=C:\IBM\APM\otdchome\7.3.0.13.0\runtime
```

4. Collez cette valeur dans la zone de texte **Options Java** de l'onglet **Java** sous **Propriétés Apache Tomcat**
5. Cliquez sur **Appliquer**.
6. Accédez à **Panneau de configuration**, cliquez sur **Système** > **Avancé** > **Variables d'environnement**
7. Dans **Variables système**, modifiez la variable *PATH* en ajoutant le chemin du fichier `<OTDC_home>\toolkit\lib\win64;<OTDC_HOME>/ toolkit\lib\win64\ttapi` et cliquez sur **OK**

   Remarque : Remplacez <OTDC_home> par le chemin réel du répertoire d'installation du kit d'outils. Par exemple, `C:\IBM\APM\otdchome\7.3.0.13.0\toolkit\lib\win64;C:\IBM\APM\otdchome\7.3.0.13.0\toolkit\lib\win64\ttapi`
8. Cliquez sur **NOUVEAU** pour ajouter une variable *RUNTIME_DIR*.

9. Ajoutez **Variable Name** dans *RUNTIME_DIR* et **Variable Path** dans `C:\IBM\APM\otdchome\7.3.0.13.0\runtime`. Ce chemin est disponible dans `setenv_<nom_instance>.bat`
10. Redémarrez Windows. Vérifiez que le démarrage du service Tomcat est défini sur Automatique

Configuration de l'Agent Tomcat sur les systèmes Linux

Exécutez le script de configuration et répondez aux invites pour configurer l'Agent Tomcat sur les systèmes Linux.

Avant de commencer

- JMX Remote est activé pour le serveur Tomcat. Pour plus de détails, voir Enabling JMX Remote.
- Le serveur Tomcat est opérationnel.

Procédure

1. Exécutez la commande suivante :
   rép_install`/bin/tomcat-agent.sh config` *nom_instance*
   Où *nom_instance* est le nom à attribuer à l'instance.
2. Lorsque vous êtes invité à indiquer une valeur pour SERVER, spécifiez un nom unique pour identifier le serveur Tomcat qui est surveillé et appuyez sur la touche Entrée.
3. Lorsque vous êtes invité à indiquer une valeur pour `Java home`, appuyez sur Entrée pour accepter l'emplacement par défaut dans lequel la machine virtuelle Java est installée. L'emplacement par défaut est `/opt/ibm/apm/agent/JRE/lx8266/jre`. Si l'agent n'est pas installé dans le répertoire par défaut, spécifiez *rép_install*`/JRE/lx8266/jre`.
4. Lorsque vous êtes invité à indiquer une valeur pour `JMX user ID`, spécifiez l'ID de l'utilisateur qui se connecte au serveur MBean Tomcat. Si l'autorisation JMX n'est pas activée, appuyez sur Entrée.
5. Lorsque vous êtes invité à indiquer une valeur pour `JMX password`, indiquez le mot de passe de l'utilisateur JMX et confirmez-le. Si l'autorisation JMX n'est pas activée, appuyez sur Entrée.
6. Lorsque vous êtes invité à indiquer une valeur pour `JMX service URL`, appuyez sur Entrée pour accepter l'URL par défaut ou spécifiez une autre adresse URL de service pour vous connecter au serveur MBean Tomcat.
   Le format de l'URL est `service:jmx:rmi:///jndi/rmi://`*nom_hôte*`:`*numéro_port*`/jmxrmi`. L'adresse URL par défaut est valide lorsque le serveur s'exécute sur l'hôte local et utilise le port 8686 comme port JMX. Vous pouvez modifier le nom d'hôte et le port dans l'URL en conservant le même format.
7. Lorsque vous êtes invité à indiquer une valeur pour `Data Collector Configuration`, spécifiez `1`, puis appuyez sur la touche Entrée pour activer la collecte des données de suivi et d'analyse approfondie des transactions.
8. Exécutez la commande suivante pour démarrer l'agent :
   rép_install`/bin/tomcat-agent.sh start` *nom_instance*
9. Activez la collecte des données de suivi des transactions et d'analyse approfondie et redémarrez le serveur Tomcat.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Configuration de l'Agent Tomcat à l'aide du fichier de réponses silencieux

Vous pouvez utiliser le fichier de réponses silencieux pour configurer l'Agent Tomcat sans répondre aux invites.

Procédure

1. Dans un éditeur de texte, ouvrez le fichier `tomcat_silent_config.txt` disponible à l'emplacement suivant :
   rép_install`/samples`
2. Pour le paramètre **KOT_SERVER**, spécifiez un nom unique pour identifier le serveur Tomcat surveillé.
3. Pour le paramètre **Java home**, indiquez le chemin dans lequel la machine virtuelle Java est installée. L'emplacement par défaut est `/opt/ibm/apm/agent/JRE/lx8266/jre`. Si l'agent n'est pas installé dans le répertoire par défaut, spécifiez *rép_install*`/JRE/lx8266/jre`.
4. Pour le paramètre **JMX user ID**, spécifiez l'ID de l'utilisateur qui est utilisé pour se connecter au serveur MBean Tomcat. Vous devez spécifier une valeur pour ce paramètre lorsque l'autorisation JMX est activée dans Tomcat.
5. Pour le paramètre **JMX password**, spécifiez le mot de passe de l'utilisateur JMX. Vous devez spécifier une valeur pour ce paramètre lorsque l'autorisation JMX est activée dans Tomcat.
6. Pour le paramètre **JMX service URL**, spécifiez l'adresse URL de service pour vous connecter au serveur MBean Tomcat. Le format de l'URL est `service:jmx:rmi:///jndi/rmi://`*nom_hôte*`:`*numéro_port*`/jmxrmi`. L'adresse URL par défaut est valide lorsque le serveur s'exécute sur l'hôte local et utilise le port 8686 comme port JMX. Vous pouvez modifier le nom d'hôte et le numéro de port dans l'URL en conservant le même format.
7. Pour le paramètre **KOT_DCCONFIGURATION**, spécifiez `Yes` si vous souhaitez activer une collection de données de suivi et d'analyse approfondie des transactions.
8. Sauvegardez et fermez le fichier `tomcat_silent_config.txt`, puis exécutez la commande suivante pour mettre à jour les paramètres de configuration d'agent :
   Linux *rép_install*`/bin/tomcat-agent.sh config` *nom_instance rép_install*`/samples/tomcat_silent_config.txt`
   Windows *rép_install*`\bin\tomcat-agent.bat config` *nom_instance rép_install*`\samples\tomcat_silent_config.txt`
   Où *nom_instance* est le nom à attribuer à l'instance, et *rép_install* est le répertoire d'installation de l'Agent Tomcat.
9. Exécutez la commande suivante pour démarrer l'agent :
   Linux *rép_install*`/bin/tomcat-agent.sh start` *nom_instance*
   Windows *rép_install*`\bin\tomcat-agent.bat start` *nom_instance*
10. Si vous activez la collecte des données de suivi et d'analyse approfondie des transactions, redémarrez le serveur Tomcat.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Activation de la collecte des données de suivi des transactions et de diagnostic

Sur la page **Configuration d'agent**, vous pouvez activer ou désactiver la collecte des données de suivi des transactions et de diagnostic.

Pourquoi et quand exécuter cette tâche

Lorsque vous activez la collecte des données de suivi des transactions, l'agent collecte les données des composants suivants :

- Servlet JSP
- Applications EJB

- JMS

Procédure

Procédez comme suit pour configurer la collecte des données pour chaque système géré.

1. Connectez vous à console Cloud APM.
2. A partir de la barre de navigation, cliquez sur **Configuration système** > **Configuration d'agent**.
   La page **Configuration d'agent** s'affiche.
3. Cliquez sur l'onglet **Tomcat**.
4. Cochez les cases des systèmes gérés pour lesquels vous voulez configurer la collecte de données et effectuez l'une des actions suivantes de la liste **Actions**.
   - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Enabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour sur Enabled pour chaque système géré sélectionné.
   - Pour activer la collecte des données de diagnostic, cliquez sur **Set Diagnostic Mode** > **Enabled Diagnostic Mode Only**. Le statut indiqué dans la colonne Diagnostic Mode est mis à jour et défini sur Enabled pour chaque système géré sélectionné.
   - Pour activer la collecte des données de diagnostic et la trace de méthode, cliquez sur **Set Diagnostic Mode** > **Enabled Diagnostic Mode and Method Trace**. Le statut indiqué dans les colonnes Diagnostic Mode et Method Trace est mis à jour et défini sur Enabled pour chaque système géré sélectionné.
   - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Disabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour et défini sur Disabled pour chaque système géré sélectionné.
   - Pour désactiver la collecte des données de diagnostic, cliquez sur **Set Diagnostic Mode** > **Disabled Diagnostic Mode and Method Trace**. Le statut indiqué dans les colonnes **Diagnostic Mode et Method Trace** est mis à jour et défini sur Disabled pour chaque système géré sélectionné.

Que faire ensuite

Connectez-vous à la console Cloud APM pour afficher les données de suivi des transactions et de diagnostic collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Mise à jour ou modification du serveur d'applications Tomcat

Pour mettre à jour ou modifier le serveur d'applications Tomcat après la configuration de l'Agent Tomcat, procédez comme décrit dans la présente rubrique. Cette procédure s'applique à la configuration de Tomcat sous Windows et Linux.

Procédure

1. Arrêtez l'instance de l'Agent Tomcat et le serveur Tomcat
2. Accédez à <TOMCAT_SERVER>/bin et ouvrez le fichier `setenv.sh` dans un éditeur
3. Supprimez tous les paramètres de démarrage du collecteur de données de `setenv.sh`. Supprimez les lignes suivantes du fichier

```
export LD_LIBRARY_PATH="<CANDLE_HOME>/otdchome/7.3.0.13.0/toolkit/lib/lx8266"
export RUNTIME_DIR="<CANDLE_HOME>/otdchome/7.3.0.13.0/runtime"
export JAVA_OPTS="-agentlib:am_ibm_16=<CANDLE_HOME>/otdchome/7.3.0.13.0/runtime/
<Tomcat_Application_
Server> -
Xbootclasspath/p:<CANDLE_HOME>/otdchome/7.3.0.13.0/toolkit/lib/bcm-bootstrap.jar -
Djava.security.policy=<CANDLE_HOME>/otdchome/7.3.0.13.0/itcamdc/etc/datacollector.policy -
Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=<CANDLE_HOME>/otdchome/7.3.0.13.0/runtime/
<Tomcat_
Application_Server>/<Agent_Instance>_DCManual.txt -
Dcom.ibm.tivoli.itcam.serverHome=<TOMCAT_HOME> -
```

```
Dam.home=<CANDLE_HOME>/otdchome/7.3.0.13.0/itcamdc -
Dcom.ibm.tivoli.itcam.toolkit.runtime.dir=<CANDLE_HOME>/otdchome/7.3.0.13.0/runtime"
```

4. Sauvegardez les modifications et démarrez le serveur Tomcat
5. Reconfigurez l'Agent Tomcat de sorte à mettre à jour ou à modifier le serveur d'applications Tomcat
6. Ne mettez à jour ou ne modifiez que le serveur d'applications Tomcat et ne modifiez aucun autre paramètre de configuration
7. Démarrez l'instance de l'Agent Tomcat
8. Vérifiez que le fichier `setenv.sh` a été mis à jour avec le nouveau serveur d'applications Tomcat en contrôlant les paramètres de démarrage du collecteur de données
9. Redémarrez le serveur Tomcat
10. Vérifiez que les modifications apportées au serveur d'applications Tomcat ont été répercutées dans la machine agent et sur le tableau de bord IBM Cloud Application Performance Management
    - Vérifiez que le serveur d'applications Tomcat a été modifié à l'emplacement `<CANDLE_HOME>/otdchome/7.3.0.13.0/runtime/<Tomcat_Application_Server>` sur la machine agent
    - Vérifiez que le serveur d'applications Tomcat a été modifié sur la page **Agréger une topologie de transaction** et dans l'attribut *appserver* sous le groupe d'attributs *KOT_Server* sur le tableau de bord IBM Cloud Application Performance Management

Configuration de la surveillance de VMware VI

Après avoir installé Monitoring Agent for VMware VI, vous devez créer la première instance et démarrer manuellement l'agent pour la collecte des données de l'infrastructure virtuelle VMware en cours de surveillance.

Avant de commencer

- Prenez connaissance des prérequis aux niveaux matériel et logiciel.
- Créez un ID utilisateur dans votre infrastructure virtuelle VMware. L'agent utilise cet ID utilisateur pour se connecter au vCenter VMware afin de surveiller l'infrastructure virtuelle VMware. Vérifiez que vous disposez des privilèges "System.View" et "System.Read" sur tous les vCenters et serveurs ESX qui sont surveillés. Pour plus d'informations sur la création de l'ID utilisateur, voir les rubriques relatives à la gestion des utilisateurs, des groupes, des droits et des rôles dans la documentation VMware.
- Déterminez si le vCenter est configuré pour la communication SSL. S'il est configuré, alors vous devez configurer Agent VMware VI pour utiliser SSL pour communiquer avec le vCenter.
  - Pour déterminer si le vCenter utilise SSL pour la communication, utilisez l'URL `https://`*`adresseIPvCenter`* pour accéder au vCenter. Si vous pouvez accéder au vCenter, alors cela indique que le vCenter utilise SSL pour communiquer sur le réseau.
  - Pour configurer l'Agent VMware VI de façon à ce qu'il utilise SSL pour communiquer avec le vCenter, effectuez les étapes décrites dans la section «Activation de la communication SSL avec les sources de données VMware VI», à la page 833.
- Déterminez le nombre d'instances d'agent dont vous avez besoin pour surveiller votre infrastructure virtuelle VMware. Pour plus d'informations sur la définition du nombre d'instances d'agent conformément à votre environnement de surveillance, voir «Définition de la taille et planification du déploiement de l'Agent VMware VI», à la page 832.

Pourquoi et quand exécuter cette tâche

L'Agent VMware VI est un agent multi-instance. Contrairement à un agent doté d'une seule instance, que vous pouvez configurer pour surveiller et collecter les données pour une seule application surveillée, l'Agent VMware VI peut avoir plusieurs instances configurées qui se connectent à plusieurs serveurs vCenter et surveillent votre infrastructure virtuelle VMware à distance.

Les paramètres de configuration définissent les sources de données de l'infrastructure virtuelle VMware surveillées et établissent une connexion au vCenter VMware, au dispositif serveur vCenter ou à un serveur ESX VMware individuel. Pour connaître les versions prises en charge de ces applications, voir les rapports de compatibilité des produits logiciels pour l'Agent VMware VI.

Les versions du produit et de l'agent sont souvent différentes. Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Vous devez configurer manuellement l'agent pour afficher les données de tous les attributs d'agent.

- Pour configurer l'agent sur des systèmes d'exploitation Windows, vous pouvez utiliser la fenêtre **IBM Performance Management** ou le fichier de réponses silencieux.
- Pour configurer l'agent sur les systèmes d'exploitation Linux, vous pouvez exécuter le script et répondre aux invites, ou utiliser le fichier de réponses silencieux.

Définition de la taille et planification du déploiement de l'Agent VMware VI

Le nombre d'instances d'agent que vous pouvez configurer sur un système unique dépend de la disponibilité et de l'utilisation des ressources sur le système.

Le tableau suivant catégorise l'environnement VMware en fonction de différentes tailles avec la taille de segment de mémoire Java requise :

Tableau 218. Environnement VMware et taille de segment de mémoire Java

Taille de l'environnement VMware	Nombre de serveurs ESX	Taille de segment de mémoire Java
Environnement de petite taille	Un serveur vCenter qui gère jusqu'à 125 serveurs ESX(i) et entre 300 et 1500 invités.	**-Xmx2048m** (2 Go)
Environnement de taille moyenne	Un serveur vCenter qui gère entre 125 et 250 serveurs ESX(i) et entre 1500 et 4000 invités.	**-Xmx4096m** (4 Go)
Environnement de grande taille	Un serveur vCenter qui gère entre 250 et 500 serveurs ESX(i) et entre 4000 et 7500 invités.	**-Xmx8192m** (8 Go)
Environnement de très grande taille	Un serveur vCenter qui gère plus de 500 serveurs ESX(i) et plus de 7500 invités.	**-Xmx16384m** (16 Go)

Pour augmenter la taille de segment de mémoire pour le fournisseur de données Java, effectuez les étapes décrites dans la section «Augmentation de la taille de segment de mémoire Java», à la page 839.

Pour que les instances d'agent surveillent correctement l'environnement, le serveur sur lequel vous installez l'agent doit disposer d'une quantité de ressources de mémoire suffisante pour pouvoir accueillir les données collectées par ces instances d'agent. Une instance unique de l'Agent VMware VI nécessite entre 300 et 400 Mo environ pour surveiller un environnement de petite taille. Reportez-vous aux instructions relatives au nombre d'instances d'agent à configurer :

- Utilisez une instance unique pour surveiller un vCenter unique. N'utilisez pas la même instance pour surveiller plusieurs vCenters.
- Dans un environnement non cluster, utilisez une instance unique pour surveiller un maximum de 8 serveurs ESX de petite taille (entre 100 et 200 machines virtuelles dans un serveur ESX). Ne configurez pas plusieurs serveurs ESX individuels au sein d'une instance d'agent unique.

- Utilisez plusieurs instances de l'Agent VMware VI pour surveiller un environnement contenant plusieurs vCenters. Avant de configurer plusieurs instances, vérifiez que le système sur lequel vous installez l'agent dispose d'une quantité de ressources de mémoire suffisante.

Activation de la communication SSL avec les sources de données VMware VI

Avant de configurer l'agent afin de communiquer de manière sécurisée avec ses sources de données d'infrastructure virtuelle VMware à l'aide de SSL, vous devez ajouter un certificat SSL de source de données au magasin de certificats de confiance de l'agent.

Pourquoi et quand exécuter cette tâche

Important : Les informations ci-dessous ne s'appliquent que si l'agent est configuré de manière à valider les certificats SSL.

Si la validation de certificat SSL est désactivée, l'Agent VMware VI se connecte aux sources de données VMware même si leurs certificats SSL ont expiré, ne sont pas dignes de confiance ou ne sont pas valides. Cependant, la désactivation de la validation des certificats SSL peut poser des problèmes de sécurité et doit être effectuée avec précaution.

Si une source de données VMware utilise un certificat SSL signé par une autorité de certification commune (par exemple Verisign, Entrust ou Thawte), il n'est pas nécessaire d'ajouter des certificats au magasin de clés de confiance de certificats de l'Agent VMware VI. En revanche, si la source de données utilise un certificat qui n'est pas signé par une autorité de certification courante, comme c'est le cas par défaut, vous devez ajouter le certificat au magasin de confiance pour permettre à l'agent de se connecter et de collecter des données.

Remarque :

1. Le fichier de certificat VMware par défaut se nomme `rui.crt`.
2. Pour un centre virtuel, le fichier de certificat SSL se trouve par défaut dans le chemin suivant :

   ```
   C:\Documents and Settings\All Users\Application Data\VMware\VMware
   VirtualCenter\SSL
   ```
3. Pour un serveur ESX, le fichier du certificat SSL se trouve par défaut dans le répertoire `/etc/vmware/ssl`.

Procédure

1. Copiez le fichier de certificat de votre source de données vers l'ordinateur de l'agent.
2. Sur l'ordinateur de l'agent, placez le fichier de certificat dans le répertoire de votre choix. Evitez tout écrasement des fichiers de certificat. Utilisez un nom de fichier et un libellé uniques pour chaque certificat ajouté.
3. Utilisez la commande *keytool* pour ajouter le certificat de source de données au magasin de clés de confiance de l'agent :

   ```
   keytool -import -noprompt -trustcacerts -alias CertificateAlias -file
   CertificateFile -keystore Truststore -storepass TruststorePassword
   ```

   Où

   CertificateAlias

   Référence unique pour chaque certificat ajouté au magasin de clés de confiance de l'agent ; par exemple, *datasource* est un alias approprié pour le certificat provenant de *datasource.example.com*.

   CertificateFile

   Nom et chemin d'accès complet au fichier de certificat de source de données VMware à ajouter au magasin de clés de confiance.

Truststore

Nom et chemin d'accès complet au fichier de la base de données de certificats de l'Agent VMware VI. Utilisez le chemin et le nom de fichier suivants :

- Windows (64 bits) : *rép_install*\tmaitm6_x64\kvm.truststore
- Linux (64 bits) : *rép_install*/lx8266/vm/etc/kvm.truststore

TruststorePassword

ITMVMWAREVI est le mot de passe par défaut du magasin de clés de confiance de l'Agent VMware VI. Pour modifier ce mot de passe, reportez-vous à la documentation relative à l'environnement d'exécution Java pour plus d'informations sur les outils à utiliser.

Important : Pour utiliser la commande *keytool*, le répertoire bin de l'environnement d'exécution Java doit être indiqué dans le chemin. Utilisez les commandes suivantes :

- Windows (64 bits) : `set PATH=%PATH%;`*rép_install*`\java\java70_x64\jre\bin`
- Linux (64 bits) : `PATH="$PATH":/opt/ibm/apm/agent/JRE/lx8266/bin`

4. Après avoir ajouté tous les certificats de source de données, démarrez l'agent de surveillance.

Que faire ensuite
Terminez la configuration de l'agent.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'agent sur les systèmes d'exploitation Windows à l'aide de la fenêtre **IBM Performance Management**. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Pourquoi et quand exécuter cette tâche

L'Agent VMware VI fournit les valeurs par défaut de certains paramètres. Vous pouvez indiquer d'autres valeurs pour ces paramètres.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur **Monitoring Agent for VMware VI**, puis sur **Configuration de l'agent**.

   A faire : La première fois que vous configurez l'agent, l'option **Configuration de l'agent** est désactivée. Pour reconfigurer l'agent, cliquez sur **Reconfigurer**.
3. Dans la fenêtre Monitoring Agent for VMware VI, procédez comme suit :
   a) Entrez un nom unique pour l'instance d'Agent VMware VI et cliquez sur **OK**.
   b) Dans l'onglet **Fournisseur de données**, indiquez les valeurs des paramètres de configuration, puis cliquez sur **Suivant**.
   c) Dans l'onglet **Source de données**, indiquez les valeurs des paramètres de configuration, puis cliquez sur **Suivant**.

      L'Agent VMware VI est un agent applicable à plusieurs sources de données. Vous pouvez surveiller plusieurs sources de données à partir du même agent.

      - Si vous souhaitez configurer une nouvelle source de données, cliquez sur **Nouveau**.
      - Si vous souhaitez supprimer une source de données existante, cliquez sur **Supprimer**.

      Pour plus d'informations sur les paramètres de configuration dans chaque onglet de la fenêtre Monitoring Agent for VMware VI, consultez les rubriques suivantes :

- Paramètres de configuration du fournisseur de données
- Paramètres de configuration de la source de données

4. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur l'instance que vous avez configurée, puis cliquez sur **Démarrer**.

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

  Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.
- Si vous surveillez un environnement VMware de grande taille regroupant plus de 500 hôtes ESX, vous devrez sans doute augmenter la taille du segment de mémoire pour le fournisseur de données Java. Pour plus d'informations, voir «Augmentation de la taille de segment de mémoire Java», à la page 839.

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

- Pour configurer l'Agent VMware VI en mode silencieux, procédez comme suit :
  a) Dans un éditeur de texte, ouvrez le fichier `vmware_vi_silent_config.txt` disponible dans l'emplacement suivant :
     - Linux *rép_install*`/samples/vmware_vi_silent_config.txt`

       Exemple : `/opt/ibm/apm/agent/samples/vmware_vi_silent_config.txt`
     - Windows *rép_install*`\samples\vmware_vi_silent_config.txt`

       Exemple : `C:\IBM\APM\samples\vmware_vi_silent_config.txt`

  b) Dans le fichier `vmware_vi_silent_config.txt`, indiquez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.

     Pour plus d'informations sur les paramètres de configuration, voir les rubriques suivantes :
     - «Paramètres de configuration du fournisseur de données», à la page 838
     - «Paramètres de configuration de la source de données», à la page 837

  c) Sauvegardez et fermez le fichier `vmware_vi_silent_config.txt`, puis exécutez la commande suivante :
     - Linux *rép_install*`/bin/vmware_vi-agent.sh config` *nom_instance* *rép_install*`/samples/vmware_vi_silent_config.txt`

       Exemple : **`/opt/ibm/apm/agent/bin/vmware_vi-agent.sh config nom_instance /opt/ibm/apm/agent/samples/vmware_vi_silent_config.txt`**

– Windows *rép_install*\bin\vmware_vi-agent.bat config *nom_instance* *rép_install*\samples\vmware_vi_silent_config.txt

Exemple : **C:\IBM\APM\bin\ vmware_vi-agent.bat config nom_instance C:\IBM\APM\samples\vmware_vi_silent_config.txt**

Où

nom_instance
Nom à attribuer à l'instance.

rép_install
Chemin d'installation de l'agent.

Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.

d) Exécutez la commande suivante pour démarrer l'agent :

– Linux *rép_install*/bin/vmware_vi-agent.sh start *nom_instance*

Exemple : **/opt/ibm/apm/agent/bin/vmware_vi-agent.sh start nom_instance**

– Windows *rép_install*\bin\vmware_vi-agent.bat start *nom_instance*

Exemple : **C:\IBM\APM\bin\vmware_vi-agent.bat start nom_instance**

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

  Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.
- Si vous surveillez un environnement VMware de grande taille regroupant plus de 500 hôtes ESX, vous devrez sans doute augmenter la taille du segment de mémoire pour le fournisseur de données Java. Pour plus d'informations, voir «Augmentation de la taille de segment de mémoire Java», à la page 839.

Configuration de l'agent en répondant à des invites.

Pour configurer l'agent sur des systèmes d'exploitation Linux, vous pouvez exécuter le script ou répondre à des invites.

Procédure

- Pour configurer l'agent en exécutant le script et en répondant aux invites, procédez comme suit :
  a) A partir d'une ligne de commande, exécutez la commande suivante :

  rép_install/bin/vmware_vi-agent.sh config *nom_instance*

  Exemple : **/opt/ibm/apm/agent/bin/vmware_vi-agent.sh config nom_instance**

  Où

  nom_instance
  Nom à attribuer à l'instance.

  rép_install
  Chemin d'installation de l'agent.

  b) Répondez aux invites en vous référant aux rubriques suivantes :

  – «Paramètres de configuration du fournisseur de données», à la page 838
  – «Paramètres de configuration de la source de données», à la page 837

  c) Exécutez la commande suivante pour démarrer l'agent :

rép_install/bin/vmware_vi-agent.sh start *nom_instance*

Exemple : **/opt/ibm/apm/agent/bin/vmware_vi-agent.sh start nom_instance**

Que faire ensuite

- Connectez-vous à la console Cloud APM pour afficher les données collectées par l'agent dans les tableaux de bord. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

  Si vous avez besoin d'aide pour le traitement des incidents, voir le forum IBM Cloud APM sur developerWorks.
- Si vous surveillez un environnement VMware de grande taille regroupant plus de 500 hôtes ESX, vous devrez sans doute augmenter la taille du segment de mémoire pour le fournisseur de données Java. Pour plus d'informations, voir «Augmentation de la taille de segment de mémoire Java», à la page 839.

Paramètres de configuration de la source de données

Lorsque vous configurez l'Agent VMware VI, vous pouvez modifier les valeurs par défaut des paramètres de la source de données, comme l'adresse, l'ID utilisateur et le mot de passe de la source de données.

Le tableau ci-après contient une description détaillée des paramètres de configuration de la source de données.

Tableau 219. Noms et descriptions des paramètres de configuration de la source de données

Nom du paramètre	Description	Zone obligatoire
Data Source ID	ID de la source de données.	Oui
Data Source Address	Adresse de la source de données. Si vous ne souhaitez pas que l'agent valide les certificats SSL, définissez une valeur correspondant au nom d'hôte ou à l'adresse IP du centre virtuel VMware ou du serveur ESX surveillé. Si vous souhaitez que l'agent valide les certificats SSL lorsque SSL est utilisé pour communiquer via le réseau, configurez l'agent à l'aide de l'élément Subject Alternative Name fourni dans le certificat. Pour afficher l'élément subject alternative name du centre de données, procédez comme suit : 1. Ouvrez le certificat. 2. Dans la fenêtre **Certificate**, cliquez sur l'onglet **Details**. 3. Sélectionnez **Subject Alternative Name** et utilisez la valeur de DNS Name. Par exemple, si la valeur de DNS Name est "ibmesx3v3vc.ITMfVS.com", utilisez la valeur "ibmesx3v3vc.ITMfVS.com" pour le nom d'hôte.	Oui
Use SSL Connection to Data Source	Indique si l'agent utilise une connexion SSL pour se connecter aux sources de données de l'infrastructure virtuelle VMware. Indiquez Yes si l'agent utilise une connexion SSL pour se connecter aux sources de données. Sinon, indiquez No. La valeur par défaut est Yes.	Oui
Data Source User ID	ID utilisateur doté de privilèges suffisants pour collecter des données de surveillance et reconnu par la source de données.	Oui

Tableau 219. Noms et descriptions des paramètres de configuration de la source de données (suite)		
Nom du paramètre	**Description**	**Zone obligatoire**
Data Source Password	Mot de passe de l'ID utilisateur configuré pour accéder à la source de données.	Oui
Confirm Data Source Password	Mot de passe correspondant à celui indiqué dans la zone **Data Source Password**.	

Paramètres de configuration du fournisseur de données

Lorsque vous configurez l'Agent VMware VI, vous pouvez modifier les valeurs par défaut des paramètres pour le fournisseur de données, comme le nombre maximal de fichiers journaux du fournisseur de données, la taille maximale du fichier journal et le niveau de détail inclus.

Le tableau ci-après contient une description détaillée des paramètres du fournisseur de données.

Tableau 220. Noms et descriptions des paramètres de configuration du fournisseur de données		
Nom du paramètre	**Description**	**Zone obligatoire**
Nom d'instance	Nom de l'instance. **Restriction :** La zone **Nom d'instance** contient le nom de l'instance que vous spécifiez lorsque vous configurez l'agent pour la première fois. Lorsque vous reconfigurez l'agent, vous ne pouvez pas modifier le nom d'instance de l'agent.	Oui
Certificats SSL valides	Indique si l'agent valide des certificats SSL lorsqu'il utilise SSL pour communiquer sur le réseau. Définissez la valeur `Yes` si vous souhaitez que l'agent valide des certificats SSL lorsqu'il utilise SSL pour communiquer sur le réseau. Indiquez la valeur `No` pour empêcher l'agent de valider les certificats SSL. La valeur par défaut est `Oui`. Pour plus d'informations sur l'ajout d'un certificat SSL de source de données dans le magasin de certificats de confiance de l'agent, voir «Activation de la communication SSL avec les sources de données VMware VI», à la page 833.	Oui
Maximum number of Data Provider Log Files	Nombre maximal de fichiers journaux créés par le fournisseur de données avant qu'il remplace les anciens fichiers journaux. La valeur par défaut est 10.	Oui
Maximum Size in KB of Each Data Provider Log	Taille maximale en ko qu'un fichier journal du fournisseur de données doit atteindre avant que le fournisseur de données ne crée un autre fichier journal. La valeur par défaut est 5190 ko.	Oui
Level of Detail in Data Provider Log	Niveau de détail qui peut être inclus dans le fichier journal que le fournisseur de données crée. La valeur par défaut est INFO. Les valeurs admises sont les suivantes : OFF, SEVERE, WARNING, INFO, FINE, FINER, FINEST et ALL.	Oui

Tableau 220. Noms et descriptions des paramètres de configuration du fournisseur de données (suite)		
Nom du paramètre	**Description**	**Zone obligatoire**
KEY_STORE_PASSWORD	Ce paramètre permet à l'utilisateur de configurer l'agent avec le nouveau mot de passe du magasin de clés défini pour l'environnement JRE de l'agent. Sachez que ce magasin de clés Java n'a aucun lien avec le magasin de clés de vCenter. Il n'est pas obligatoire d'entrer le mot de passe dans chaque configuration. Si cette zone est laissée à blanc, l'agent considère que le mot de passe du magasin de clés Java par défaut doit être utilisé avec l'environnement JRE de l'agent.	Non

Augmentation de la taille de segment de mémoire Java

Après avoir configuré l'Agent VMware VI, si vous surveillez un environnement d'infrastructure virtuelle VMware de grande taille, vous devrez sans doute augmenter la taille de segment de mémoire pour le fournisseur de données de Java.

Pourquoi et quand exécuter cette tâche

La taille de segment de mémoire maximale par défaut du fournisseur de données Java est de 256 mégaoctets. Vous devez définir la taille de segment de mémoire maximale sur une valeur appropriée qui dépend de la taille de l'environnement VMware. Pour plus d'informations sur les tailles de segment de mémoire requises pour les différents environnements VMware, voir Tableau 218, à la page 832.

Important : Le système sur lequel vous installez et configurez l'Agent VMware VI doit disposer d'un espace mémoire suffisant pour pouvoir s'adapter à la taille de segment de mémoire requise.

Si l'un des problèmes suivants survient, il peut s'avérer nécessaire d'augmenter la taille de segment de mémoire :

- Le fournisseur de données Java s'arrête en raison d'un problème `javacore` et crée un fichier nommé `javacore.`*`date.heure.numéro`*`.txt` dans le répertoire `CANDLEHOME\tmaitm6_x64`.
- Le fichier `javacore.`*`date.heure.numéro`*`.txt` contient la chaîne `java/lang/OutOfMemoryError`.

Procédure

- Windows

  Pour définir une taille de segment de mémoire de 1 Go, procédez comme suit :

  1. Ouvrez le fichier `%CANDLE_HOME%\TMAITM6_x64\kvm_data_provider.bat`.
  2. Ajoutez la ligne suivante avant la ligne qui commence par `KVM_JVM_ARGS="%KVM_CUSTOM_JVM_ARGS...` :

     ```
     SET KVM_CUSTOM_JVM_ARGS=-Xmx1024m
     ```

  3. Redémarrez l'agent.

- Linux

  Pour définir une taille de segment de mémoire de 1 Go, procédez comme suit :

  1. Ouvrez le fichier `$CANDLEHOME/lx8266/vm/bin/kvm_data_provider.sh`.
  2. Ajoutez la ligne suivante avant la ligne commençant par `KVM_JVM_ARGS="$KVM_CUSTOM_JVM_ARGS...` :

     ```
     KVM_CUSTOM_JVM_ARGS=-Xmx1024m
     ```

  3. Redémarrez l'agent.

Configuration de la surveillance de WebLogic

Monitoring Agent for WebLogic permet de surveiller de manière centralisée la santé, la disponibilité et les performances de votre environnement de serveur WebLogic. L'agent affiche un ensemble complet de mesures qui vous aident à prendre des décisions avisées concernant vos ressources WebLogic, y compris les machines virtuelles Java, le service de messagerie Java et la connectivité Java Database Connectivity (JDBC).

Avant de commencer

- Les instructions figurant dans cette rubrique concernent l'édition la plus récente de l'agent, sauf indication contraire.
- Assurez-vous que votre environnement possède la configuration système requise pour l'Agent WebLogic. Pour les toutes dernières informations sur la configuration système requise, voir les rapports de compatibilité des produits logiciels (SPCR) de l'Agent WebLogic.
- Avant de configurer l'Agent WebLogic, le serveur Oracle WebLogic doit d'abord être configuré en procédant comme suit :

  Remarque : La majorité de la configuration du serveur Oracle WebLogic est effectuée via la console d'administration, habituellement sur `http://weblogic-server:7001/console`.

  1. Configurez l'utilisateur du moniteur dans le groupe Monitors.
     a. Sélectionnez le domaine à surveiller ou modifier.
     b. Sélectionnez **Domaines de sécurité**.
     c. Sélectionnez votre domaine de sécurité (ou créez-en un s'il n'y en a aucun).
     d. Créez un utilisateur qui sera utilisé pour communiquer avec WebLogic via JMX.
     e. Ajoutez cet utilisateur au groupe Monitors.
     f. Sauvegardez les modifications apportées au domaine.
  2. Activez les ports d'écoute.
     a. Sélectionnez le domaine à surveiller ou modifier.
     b. Sur chaque serveur que vous souhaitez surveiller, cliquez sur **Environnement** > **Serveurs** > ***Sélectionner un serveur***.
     c. Vérifiez que le **port d'écoute** est activé et notez son numéro.
     d. Si vous souhaitez activer SSL, assurez-vous que le **port d'écoute SSL** est activé puis définissez aussi un port pour SSL.
  3. Activez les connexions au serveur JMX MBean.
     a. Sélectionnez le domaine que vous souhaitez surveiller ou modifier.
     b. Sélectionnez **Configurer** > **Avancé**.
     c. Vérifiez l'option **Platform Mbean Server Enabled**.
     d. Sauvegardez la modification.
  4. Activez l'option Protocole IIOP.
     a. Sélectionnez le domaine que vous souhaitez surveiller ou modifier.
     b. Sur chaque serveur que vous souhaitez surveiller, cliquez sur **Environnement** > **Serveurs**, puis sélectionnez un serveur.
     c. Sélectionnez l'**onglet Protocole** > ***Sélectionner IIOP***.
     d. Dans la section **Avancé**, saisissez le nom d'utilisateur et le mot de passe IIOP par défaut.
     e. Sauvegardez la modification.
  5. Activez SSL.

a. Activez HTTP Tunneling.

1) Accédez à **Environnement** > **Serveurs** > ***Sélectionner un serveur*** > **Protocole** > **Général**.

2) Vérifiez l'option **Activer HTTP Tunneling**.

b. Activez le port d'écoute SSL.

1) Accédez à **Environnement** > **Serveurs** > ***Sélectionner un serveur*** > **Configuration** > **Général**.

2) Configurez un numéro de port.

Pourquoi et quand exécuter cette tâche

L'Agent WebLogic est un agent à plusieurs instances et à plusieurs sous-noeuds. Vous pouvez créer une instance d'agent à plusieurs sous-noeuds - un pour chaque serveur WebLogic ou une instance d'agent pour chaque serveur WebLogic avec un sous-noeud pour ce serveur. Vous pouvez également créer une combinaison de chaque type de configuration. Après avoir configuré les instances d'agent, démarrez chacune d'elles manuellement.

Procédure

1. Pour configurer l'agent sur les systèmes Windows, utilisez la fenêtre **IBM Performance Management** ou le fichier de réponses silencieux avec le fichier de commandes de configuration.
   - «Configuration de l'agent sur des systèmes Windows», à la page 842.
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 846.
2. Pour configurer l'agent sur les systèmes Linux et UNIX, exécutez le script de configuration de l'agent et répondez aux invites ou utilisez le fichier de réponses silencieux.
   - «Configuration de l'agent en répondant à des invites», à la page 846.
   - «Configuration de l'agent à l'aide du fichier de réponses silencieux», à la page 846.
3. Facultatif : Pour configurer le suivi des transactions, configurez les instances d'agent individuelles pour fournir les données de suivi des transactions et configurez votre Tableau de bord d'Application Performance pour afficher les données de suivi des transactions.
   a) Suivez la procédure pour «Configuration du suivi des transactions pour l'Agent WebLogic», à la page 849.
   b) Suivez la procédure pour «Configuration de votre Tableau de bord d'Application Performance pour l'affichage des données de suivi des transactions de l'Agent WebLogic», à la page 855.

   Remarque : La fonction de suivi des transactions est disponible pour l'Agent WebLogic dans l'offre Cloud APM, Advanced. Pour l'Agent WebLogic avec la fonction de base de surveillance des ressources, présente dans l'offre Cloud APM, Base, ignorez cette étape.

Que faire ensuite

Dans la console Cloud APM, accédez à votre Tableau de bord d'Application Performance pour afficher les données collectées. Pour plus d'informations sur l'utilisation de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003.

Si vous ne parvenez pas à visualiser les données dans les tableaux de bord de l'agent, commencez par examiner les journaux de connexion du serveur, puis les journaux du fournisseur de données. Les chemins d'accès par défaut à ces journaux sont :

- Linux AIX `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Pour identifier et résoudre les incidents, reportez-vous au forum Cloud Application Performance Management.

Configuration de l'agent sur des systèmes Windows

Vous pouvez configurer l'Agent WebLogic sur les systèmes d'exploitation Windows dans la fenêtre IBM Cloud Application Performance Management. Après avoir mis à jour les valeurs de configuration, vous devez démarrer l'agent pour sauvegarder les valeurs mises à jour.

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **Agents IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. Dans la fenêtre **IBM Performance Management**, cliquez avec le bouton droit de la souris sur le modèle **Monitoring Agent for WebLogic**, puis cliquez sur **Configure agent**.

   A faire : Après avoir configuré une instance d'agent pour la première fois, l'option **Configure agent** est désactivée. Pour reconfigurer l'instance d'agent, cliquez dessus avec le bouton droit de la souris et sélectionnez **Reconfigure**.
3. Entrez un nom d'instance unique, puis cliquez sur **OK**. N'utilisez que des lettres, des chiffres arabes, le caractère de soulignement et le caractère moins dans le nom de l'instance. Par exemple : `weblogic01`.

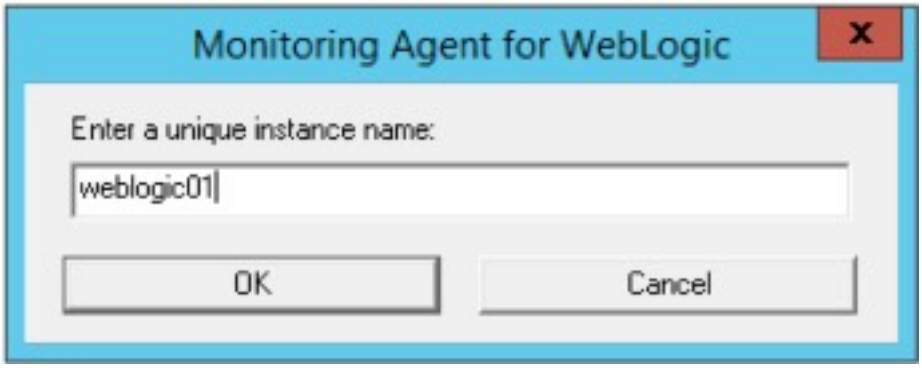
   

   Figure 27. Fenêtre de saisie d'un nom d'instance unique
4. Cliquez sur **Suivant** dans le panneau de configuration de l'agent **Nom d'instance**.

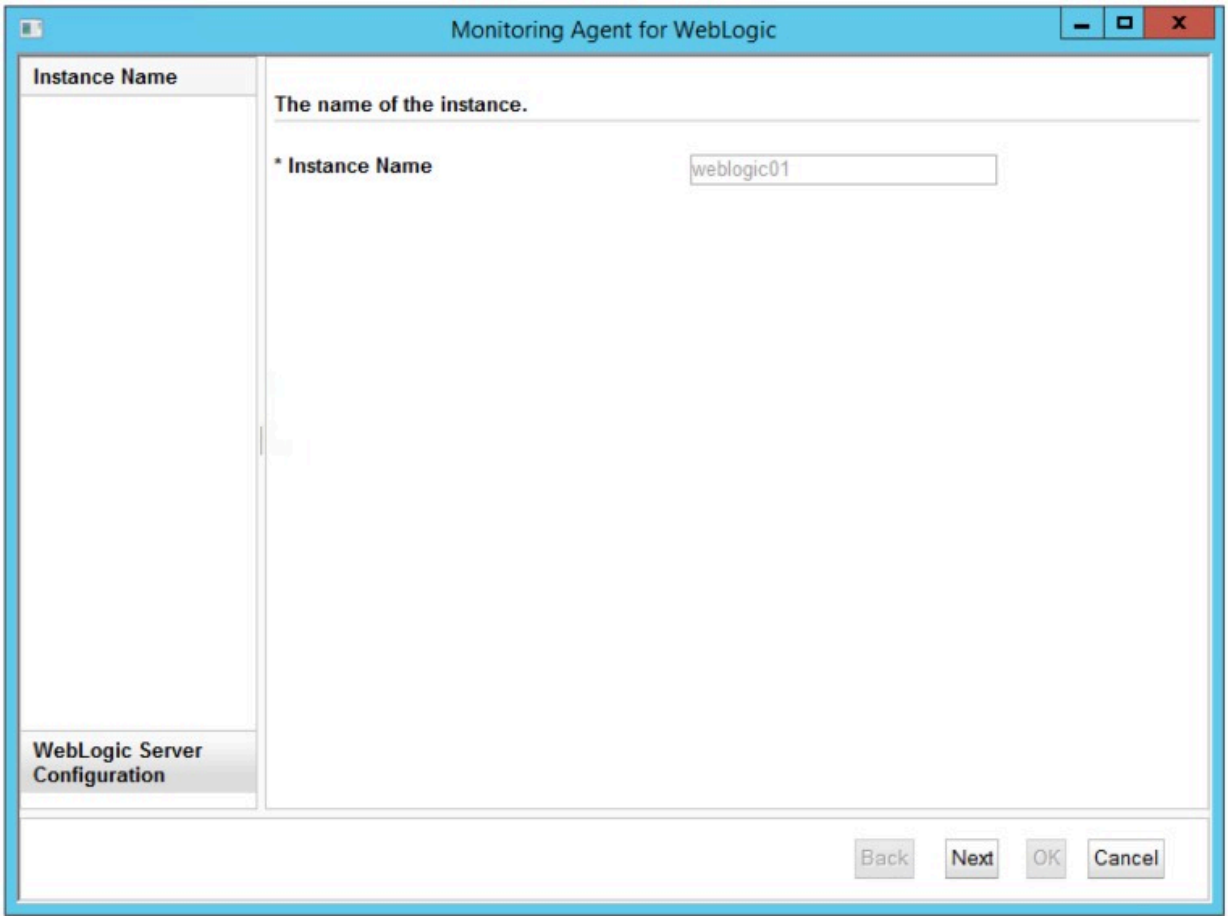


Figure 28. Fenêtre d'affichage du nom d'instance de l'agent

5. Entrez les paramètres du modèle d'instance de **Configuration du serveur WebLogic**.

   Remarque : Cette section ne décrit pas la configuration de l'instance de connexion au serveur WebLogic. Il s'agit d'un modèle de section qui permet de définir les valeurs par défaut lorsque vous ajoutez les configurations d'instance de connexion au serveur WebLogic réelles à partir de l'étape 6.

   Pour obtenir une description de chaque paramètre de configuration, voir Tableau 221, à la page 848.

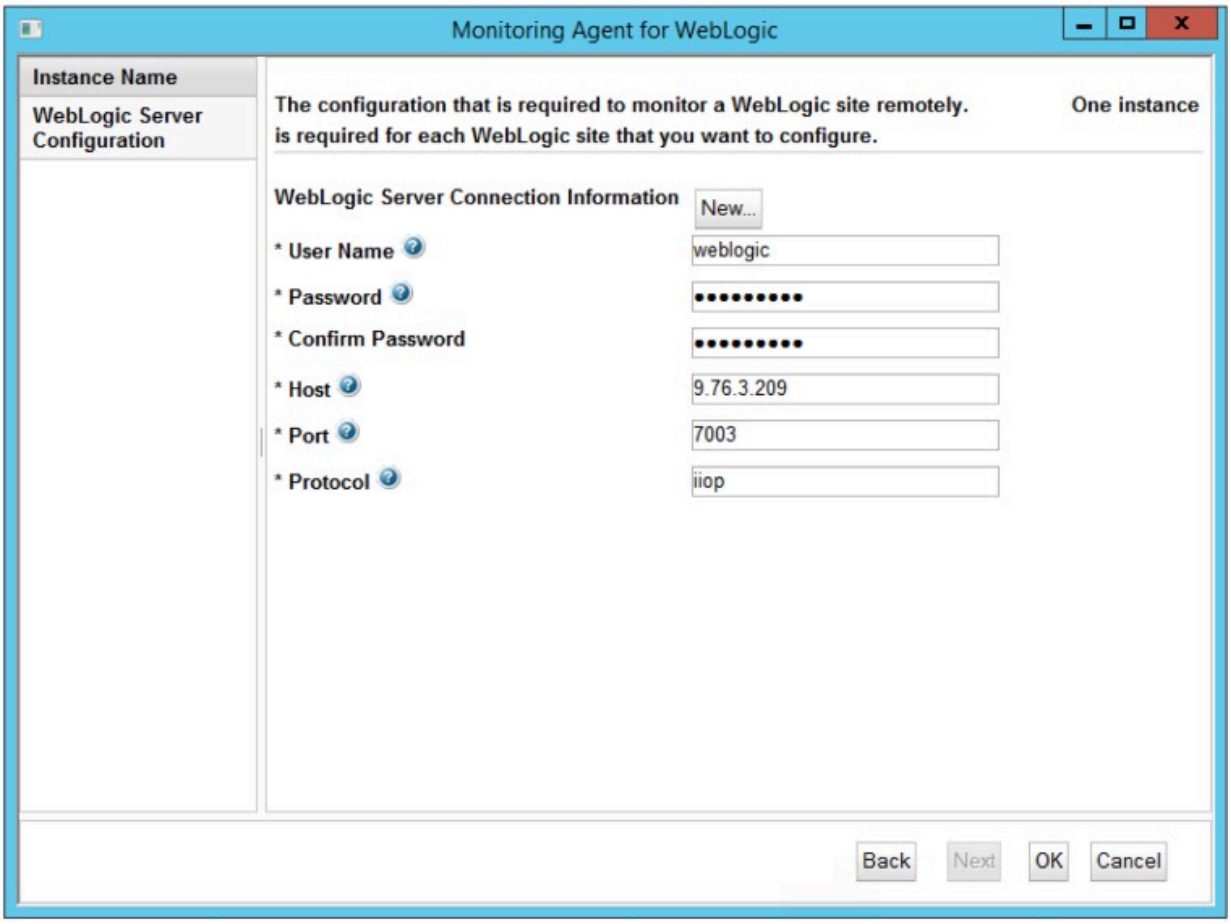


Figure 29. Fenêtre de spécification des paramètres du modèle d'instance de connexion au serveur WebLogic

6. Cliquez sur **Nouveau** et entrez les paramètres d'instance de connexion au serveur WebLogic, puis cliquez sur **Suivant**.

   Pour obtenir une description de chaque paramètre de configuration, voir Tableau 221, à la page 848.

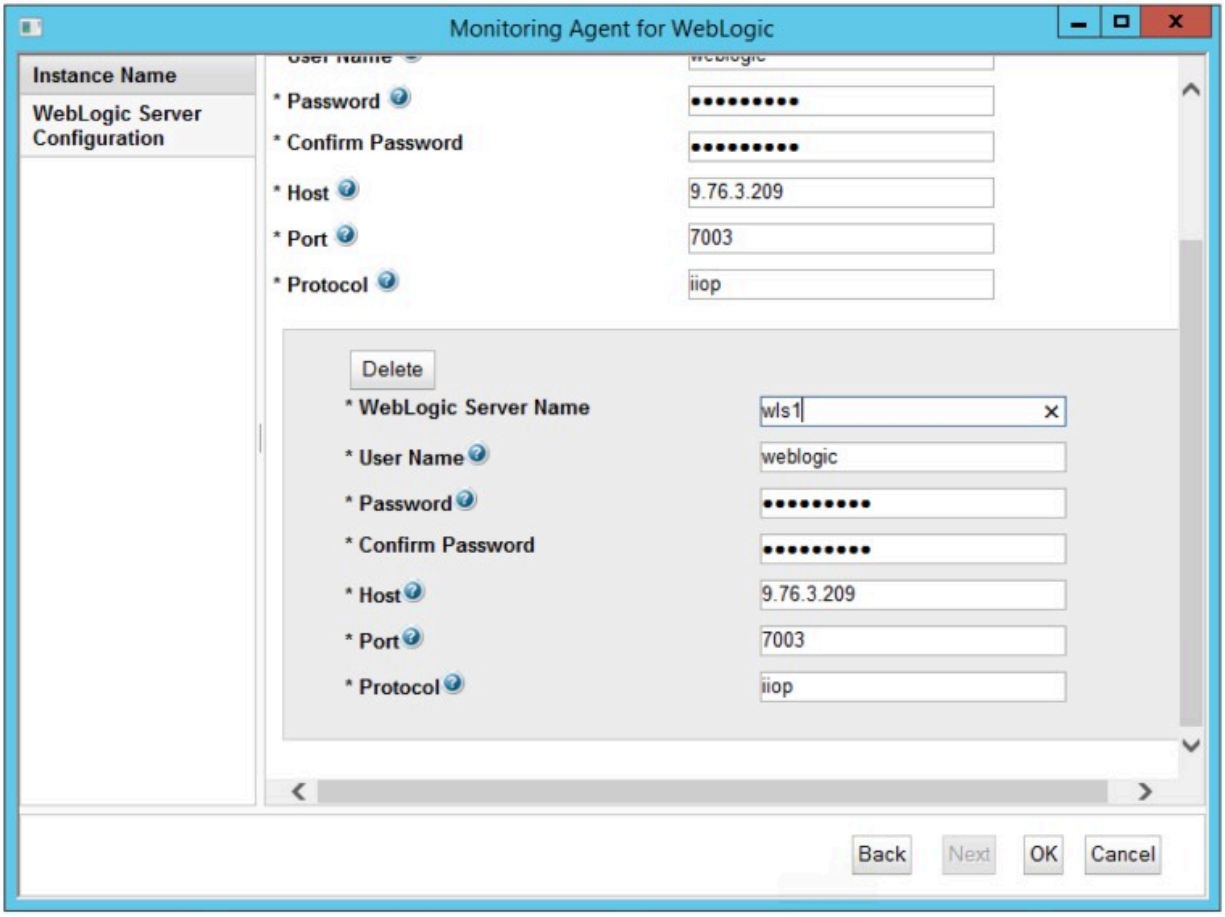


Figure 30. Fenêtre de spécification des paramètres d'instance de connexion au serveur WebLogic

7. Cliquez sur **OK** pour terminer la configuration.
8. Copiez les fichiers de sécurité de WebLogic dans le répertoire des fichiers binaires de l'Agent WebLogic.
   a. Localisez les fichiers `wlclient.jar` et `wljmxclient.jar` dans `ORACLE_HOME`. Par exemple, `C:\Oracle\Middleware\Oracle_Home\wlserver\server\lib`.
   b. Copiez les fichiers de l'étape «8.a», à la page 845 dans le répertoire des fichiers binaires de l'Agent WebLogic.
      - Linux AIX *rép_install*`/bin`.
      - Windows *rép_install*`\TMAITM6_x64`

      où *rép_install* représente le chemin d'installation de l'agent. Les chemins d'accès *rép_install* par défaut sont répertoriés ici :
      - Linux AIX `/opt/ibm/apm/agent`
      - Windows `C:\IBM\APM\TMAITM6_x64`
9. Dans la fenêtre IBM Cloud Application Performance Management, cliquez avec le bouton droit de la souris sur l'instance que vous avez configurée, puis cliquez sur **Démarrer**.

Configuration de l'agent en répondant à des invites

Après avoir installé l'Agent WebLogic, vous devez le configurer pour pouvoir le démarrer. Si l'Agent WebLogic est installé sur un ordinateur Linux ou UNIX local, vous pouvez suivre ces instructions pour le configurer de manière interactive en suivant des invites de ligne de commande.

Pourquoi et quand exécuter cette tâche

A faire : Si vous reconfigurez une instance d'agent configurée, la valeur définie dans la dernière configuration s'affiche pour chaque paramètre. Pour effacer une valeur existante, appuyez sur la touche Espace lorsque le paramètre s'affiche.

Procédure

Procédez comme suit pour configurer l'Agent WebLogic en exécutant un script et en répondant aux invites.

1. Exécutez la commande suivante :

   rép_install/bin/weblogic-agent.sh config **nom_instance**

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent.

   Exemple

   ```
   /opt/ibm/apm/agent/bin/weblogic-agent.sh config example-inst01
   ```

2. Répondez aux invites pour définir les valeurs de configuration de l'agent.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'Agent WebLogic», à la page 848.

3. Copiez les fichiers de la bibliothèque client WebLogic dans le répertoire des fichiers binaires de l'Agent WebLogic.

   a) Localisez les fichiers `wlclient.jar` et `wljmxclient.jar` dans `ORACLE_HOME`.

   b) Copiez les fichiers de l'étape «3.a», à la page 846 dans le répertoire des fichiers binaires de l'Agent WebLogic.

   rép_install/bin

   où *rép_install* représente le chemin d'installation de l'agent.

   Exemple

   ```
   /opt/ibm/apm/agent/bin
   ```

4. Exécutez la commande suivante pour démarrer l'agent :

   rép_install/bin/weblogic-agent.sh start **nom_instance**

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

   Exemple

   ```
   /opt/ibm/apm/agent/bin/weblogic-agent.sh start example-inst01
   ```

Configuration de l'agent à l'aide du fichier de réponses silencieux

Le fichier de réponses silencieux contient les paramètres de configuration d'agent. Vous pouvez éditer le fichier de réponses silencieux pour modifier les valeurs de ces paramètres et exécuter le script de configuration pour créer une instance et mettre à jour les valeurs de configuration d'agent. Ce mode de configuration est également nommé le mode silencieux.

Pourquoi et quand exécuter cette tâche

Le fichier de réponses silencieux contient les paramètres de configuration d'agent dont certains comportent des valeurs par défaut. Vous pouvez modifier ce fichier pour spécifier des valeurs différentes pour les paramètres de configuration.

Après avoir mis à jour les valeurs de configuration dans le fichier de réponses, vous devez exécuter le script de configuration pour configurer l'agent avec ces valeurs mises à jour.

Procédure

Configurez l'Agent WebLogic en mode silencieux en effectuant les étapes ci-après.

1. Dans un éditeur de texte, ouvrez le fichier `weblogic_silent_config.txt` disponible à l'emplacement suivant :
   - Linux AIX *rép_install*`/samples/weblogic_silent_config.txt`
   - Windows *rép_install*`\samples\weblogic_silent_config.txt`

   où *rép_install* représente le chemin d'installation de l'agent.

   Exemple
   - Linux AIX `/opt/ibm/apm/agent/samples/weblogic_silent_config.txt`
   - Windows `C:\IBM\APM\samples\weblogic_silent_config.txt`
2. Dans le fichier `weblogic_silent_config.txt`, spécifiez des valeurs pour tous les paramètres obligatoires. Vous pouvez également modifier les valeurs par défaut d'autres paramètres.

   Pour obtenir une description de chaque paramètre de configuration, voir «Paramètres de configuration de l'Agent WebLogic», à la page 848.
3. Sauvegardez et fermez le fichier `weblogic_silent_config.txt` et exécutez la commande suivante :
   - Linux AIX *rép_install*`/bin/weblogic-agent.sh config` **nom_instance** *rép_install*`/samples/weblogic_silent_config.txt`
   - Windows *rép_install*`\bin\weblogic-agent.bat config` **nom_instance** *rép_install*`\samples\weblogic_silent_config.txt`

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom à affecter à l'instance d'agent.

   Les chemins d'accès *rép_install* par défaut sont répertoriés ici :
   - Linux AIX `/opt/ibm/apm/agent`
   - Windows `C:\IBM\APM\TMAITM6_x64`

   Important : Veillez à inclure le chemin d'accès absolu au fichier de réponses silencieux. Sinon, les données d'agent ne seront pas disponibles dans les tableaux de bord.

   Exemple
   - Linux AIX `/opt/ibm/apm/agent/bin/weblogic-agent.sh config example-inst01 /opt/ibm/apm/agent/samples/weblogic_silent_config.txt`
   - Windows `C:\IBM\APM\bin\weblogic-agent.bat config example-inst01 C:\IBM\APM\samples\weblogic_silent_config.txt`
4. Copiez les bibliothèques client de WebLogic dans le répertoire des fichiers binaires de l'Agent WebLogic.
   a. Localisez les fichiers `wlclient.jar` et `wljmxclient.jar` dans `ORACLE_HOME`.
   b. Copiez les fichiers de l'étape «5.a», à la page 847 dans le répertoire des fichiers binaires de l'Agent WebLogic.

- Linux AIX *rép_install*/bin.
- Windows *rép_install*\TMAITM6_x64

où *rép_install* représente le chemin d'installation de l'agent. Les chemins d'accès *rép_install* par défaut sont répertoriés ici :

- Linux AIX /opt/ibm/apm/agent
- Windows C:\IBM\APM\TMAITM6_x64

5. Exécutez la commande suivante pour démarrer l'agent :
   - Linux AIX *rép_install*/bin/weblogic-agent.sh start **nom_instance**
   - Windows *rép_install*\bin\weblogic-agent.bat start **nom_instance**

   où *rép_install* représente le chemin d'installation de l'agent et *nom_instance*, le nom de l'instance d'agent.

   Les chemins d'accès *rép_install* par défaut sont répertoriés ici :
   - Linux AIX /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64

   Exemple
   - Linux AIX /opt/ibm/apm/agent/bin/weblogic-agent.sh start example-inst01
   - Windows C:\IBM\APM\bin\weblogic-agent.bat start example-inst01

Paramètres de configuration de l'Agent WebLogic

Les paramètres de configuration de l'Agent WebLogic sont regroupés dans un tableau.

1. Paramètres de l'agent WebLogic - Paramètres de l'environnement de l'agent WebLogic.

Tableau 221. Paramètres de l'agent WebLogic

Nom du paramètre	Description	Nom du paramètre de fichier de configuration en mode silencieux
Nom du serveur WebLogic	Indiquez un nom pour identifier l'instance de l'agent du serveur WebLogic. Exemple : *wls1* **Remarque :** Cet alias vous permet de représenter l'instance de l'agent du serveur WebLogic avec les restrictions suivantes. Seuls les lettres, les chiffres arabes, le caractère souligné et le caractère moins peuvent être utilisés dans le nom de connexion. La longueur maximale d'un nom de connexion est de 25 caractères.	Chacun des paramètres suivants doit avoir un suffixe de nom d'instance qui sera le même pour chaque paramètre d'une instance d'agent. Les nouvelles instances d'agent doivent utiliser un nom d'instance unique pour son jeu de paramètres. Par exemple, une instance d'agent peut utiliser *.wls1* et une autre instance d'agent peut utiliser *.wls*2 à la place de *.nom_instance* dans les noms de paramètres ci-dessous.
Nom d'utilisateur	Nom d'utilisateur utilisé pour s'authentifier avec le serveur WebLogic.	**KWB_WLS_USERNAME.nom_instance**
Mot de passe	Mot de passe utilisé pour s'authentifier avec le serveur WebLogic.	**KWB_WLS_PASSWORD.nom_instance**
Hôte	Hôte utilisé pour s'authentifier avec le serveur WebLogic. Entrez le nom d'hôte qualifié complet ou l'adresse IP du serveur WebLogic.	**KWB_WLS_HOST.nom_instance**

Tableau 221. Paramètres de l'agent WebLogic (suite)		
Nom du paramètre	**Description**	**Nom du paramètre de fichier de configuration en mode silencieux**
Port	Port utilisé pour s'authentifier avec le serveur WebLogic.	**KWB_WLS_PORT.nom_instance**
Protocole	Protocole utilisé pour s'authentifier avec le serveur WebLogic. Les protocoles pris en charge sont *iiop* et *https*.	**KWB_WLS_PROTOCOL.nom_instance**

Configuration du suivi des transactions pour l'Agent WebLogic

La fonction de suivi des transactions de l'Agent WebLogic requiert des modifications dans le fichier des paramètres d'environnement de l'instance d'agent et le fichier de démarrage du serveur WebLogic. Un script est fourni pour vous aider à apporter ces modifications.

Avant de commencer

Linux AIX Vérifiez que la limite de ressource pour les fichiers ouverts est supérieure à 5 000 pour que le kit d'outils de suivi des transactions fonctionne correctement.

- Affichez le paramètre de limite de fichiers ouverts en cours. **ulimit -n**
- Exemple de paramètre définissant la limite de fichiers ouverts à 5 056. **ulimit -n 5056**

Exécutez l'Windows étape 1 ou l'Linux AIX étape 2 de l'«Configuration de la surveillance de WebLogic», à la page 840 avant de suivre cette procédure.

Remarque : La fonction de suivi des transactions est disponible pour l'Agent WebLogic dans l'offre Cloud APM, Advanced. Pour l'Agent WebLogic avec la fonction de base de surveillance des ressources, présente dans l'offre Cloud APM, Base, ignorez cette étape.

L'Agent WebLogic doit être installé en local sur le serveur WebLogic surveillé avec la fonction de suivi des transactions.

Le compte utilisateur qui exécute ce script doit disposer de droits en écriture aux répertoires et fichiers suivants :

1. Répertoire *WEBLOGIC_HOME*.
2. Répertoire *WEBLOGIC_HOME*/bin et ses fichiers.
3. Répertoire *rép_install*/config.
4. Fichier *rép_install*/config/*nom_hôte*_wb_*nom_instance*.cfg.

où

WEBLOGIC_HOME
Répertoire d'installation du serveur WebLogic.

rép_install
Chemin d'installation de l'agent. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux AIX /opt/ibm/apm/agent
- Windows C:\IBM\APM\TMAITM6_x64

hostname
Nom de l'ordinateur hôte sur lequel l'agent est installé.

nom_instance
Nom de l'instance d'agent affectée dans la rubrique sur la méthode de configuration de l'agent :

- Configuration de l'agent sur des systèmes Windows, étape «3», à la page 842
- Configuration de l'agent en répondant à des invites, étape «1», à la page 846

- Configuration de l'agent à l'aide du fichier de réponses silencieux, étape «2», à la page 847

Procédure

Exécutez le script **simpleConfig**.

1. Connectez-vous au serveur WebLogic sur lequel l'Agent WebLogic est installé.
2. Accédez au répertoire du répertoire d'installation de l'agent.
   - Linux AIX *rép_install*
   - Windows *rép_install*\TMAITM6_x64

   où *rép_install* représente le chemin d'installation de l'agent.

   Les chemins d'accès *rép_install* par défaut sont répertoriés ici :
   - Linux AIX /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64
3. Accédez au répertoire wbdchome/8.1.4.0.0/bin.
4. Exécutez le script d'installation.
   - Linux AIX ./simpleConfig.sh
   - Windows simpleConfig.bat
5. Suivez les invites pour entrer des paramètres pour votre environnement :
   a) Choisissez l'Agent WebLogic *nom_instance* et le sous-noeud à configurer dans la liste des combinaisons d'instance d'agent et de sous-noeud détectées, *nom_instance* représentant le nom de l'instance d'agent.
   b) Indiquez le numéro de la méthode de démarrage du serveur WebLogic.
   c) Indiquez le chemin de recherche racine du domaine WebLogic.

      Ce chemin d'accès est utilisé comme base pour la recherche de domaines WebLogic. Si la variable d'environnement *WEBLOGIC_HOME* est définie, sa valeur est offerte en tant que valeur par défaut.
   d) Indiquez le numéro du domaine WebLogic pour le serveur WebLogic à configurer.
   e) Entrez le numéro du nom de serveur WebLogic à configurer.

Linux Exemple de configuration avec une méthode de démarrage WebLogic Script de démarrage WebLogic.

```
./simpleconfig.sh

Les agents et sous-noeuds suivants ne sont pas encore configurés pour le suivi des
transactions :

1) wlinst1 Server1
2) wlinst1 Server2

Entrez le numéro qui correspond à l'instance d'agent et au sous-noeud que vous voulez
configurer.

Indiquez votre sélection ici (par exemple : 1) : 1

Les méthodes de démarrage WebLogic suivantes sont prises en charge :

1) Script de démarrage WebLogic
2) Gestionnaire de noeud WebLogic

Indiquez votre sélection ici (par défaut 1) : 1

Chemin d'accès pour commencer la recherche des domaines WebLogic.
Chemin de recherche du domaine WebLogic (par défaut) : /home/wlsadmin

Voici les chemins d'accès au domaine WebLogic trouvés :

1) /home/wlsadmin/oracle/user_projects/domains/ttdd

Entrez le numéro qui correspond au domaine WebLogic contenant le serveur WebLogic que
```

```
vous souhaitez configurer.

Entrez votre sélection ici (par exemple : 1) : 1

Les serveurs WebLogic suivants sont disponibles pour configuration :

1) AdminServer
2) Server1

Sélectionnez un nom de serveur WebLogic (par défaut : 2) : 2
INFO: [2000] Automatic configuration of agent environment file succeeded.
INFO: [3000] Automatic configuration of WebLogic start script succeeded.
INFO: [9000] Restart the WebLogic agent and WebLogic server for configuration to take effect.
```

6. Suivez ces étapes si `Gestionnaire de noeud WebLogic` est sélectionné comme **Méthode de démarrage du serveur WebLogic** à l'étape «5.b», à la page 850. Sinon, passez à l'étape «7», à la page 852.
   a) Ouvrez le fichier `weblogic_nodemanager_dc_opts` répertorié dans le message d'information numéro 3011 du texte de sortie à l'étape «5», à la page 850.

      Windows Exemple de sortie de configuration avec la méthode de démarrage WebLogic `Gestionnaire de noeud WebLogic`.

      ```
      INFO: [2000] Automatic configuration of agent environment file succeeded.
      INFO: [3010] Automatic configuration of WebLogic start script skipped.
      INFO: [3011] Please review C:\IBM\APM\TMAITM6_x64\wbdchome\8.1.4.0.0\runtime\ttdd_win
      \win_Server1\
      staging\weblogic_nodemanager_dc_opts.win for required WebLogic JVM start options.
      INFO: [9000] Restart the WebLogic agent and WebLogic server for configuration to take
      effect.
      ```

   b) Connectez-vous à la console WebLogic et sélectionnez **Environnement** > **Serveurs**.
   c) Sélectionnez le serveur à configurer.
   d) Sélectionnez l'onglet **Configuration** > **Server Start**.
   e) Copiez les arguments de démarrage du serveur à partir du fichier `weblogic_nodemanager_dc_opts` vers les arguments **Start Server** du serveur dans la console WebLogic et sauvegardez les modifications.

      Les arguments de démarrage du serveur correspondent à toutes les lignes qui suivent la ligne de commentaire `# Add the following lines to the server start arguments` dans le fichier `weblogic_nodemanager_dc_opts`.
   f) Vérifiez que le kit d'outils de suivi des transactions se trouve dans le chemin de la bibliothèque partagée lors de l'exécution.

      Choisissez une méthode.

      - Mettez à jour le script de démarrage du gestionnaire de noeud.

        Remarque : Tous les serveurs WebLogic démarrés par le gestionnaire de noeud ont ce chemin d'accès à la bibliothèque défini avec les bibliothèques de fichiers objets du kit d'outils de suivi des transactions incluses.

        1) Ouvrez le fichier `weblogic_nodemanager_dc_opts` répertorié dans le message d'information numéro 3011 du texte de sortie à l'étape «5», à la page 850.
        2) Définissez le chemin du kit d'outils de suivi des transactions dans le script de démarrage du gestionnaire de noeud. La commande permettant de définir le chemin est la ligne qui suit la ligne de commentaire `# Make sure that the executable path available to the WebLogic server includes the toolkit lib directory` dans le fichier `weblogic_nodemanager_dc_opts`.

           – Linux Copiez la ligne LD_LIBRARY_PATH line à partir du fichier `weblogic_nodemanager_dc_opts.linux` généré et copiez-la sous la ligne `export JAVA_OPTIONS` dans le script de démarrage du gestionnaire de noeud. Exemple : *WEBLOGIC_HOME*`/user_projects/domains/`*nom_domaine*`/bin/startNodeManager.sh`.

– Windows Copiez la ligne PATH à partir du fichier `weblogic_nodemanager_dc_opts.win` généré et copiez-la sous la ligne `export JAVA_OPTIONS` dans le script de démarrage du gestionnaire de noeud. Exemple : *WEBLOGIC_HOME*`\user_projects\domains\`*nom_domaine*`\bin\startNodeManager.bat`.

où *WEBLOGIC_HOME* représente le répertoire d'installation du serveur WebLogic et *nom_domaine*, le nom du domaine WebLogic.

- Mettez à jour l'environnement pour le compte utilisateur qui démarre le gestionnaire de noeud.

  Remarque : Toutes les applications démarrées par le compte utilisateur ont ce chemin d'accès à la bibliothèque défini avec les bibliothèques de fichiers objets du toolkit incluses.

  1) Modifiez les paramètres d'environnement pour l'utilisateur qui démarre le gestionnaire de noeud.

     – Linux AIX Modifiez le fichier de ressources de shell ou le fichier de profils de shell. Par exemple : `.bashrc` ou `.bash_profile`.

     – Windows Modifiez **Panneau de configuration** > **Système et sécurité** > **Système** > **Paramètres système avancés** > **Variables d'environnement** > **Variables utilisateur pour *nom_utilisateur*** > **Chemin**, *nom_utilisateur* représentant le nom du compte utilisateur utilisé pour démarrer le serveur WebLogic.

  2) Définissez le chemin du kit d'outils de suivi des transactions dans l'environnement du compte utilisateur. La commande permettant de définir le chemin est la ligne qui suit la ligne de commentaire `# Make sure that the executable path available to the WebLogic server includes the toolkit lib directory` dans le fichier `weblogic_nodemanager_dc_opts`.

     – Linux AIX Copiez la ligne `export LD_LIBRARY_PATH` à partir du fichier `weblogic_nodemanager_dc_opts.linux` généré. Si une ligne `export LD_LIBRARY_PATH` n'existe pas, ajoutez-la. Si elle existe, modifiez-la pour ajouter uniquement le chemin situé à droite du signe égal dans le chemin existant avec le délimiteur de chemin correct.

     – Windows Copiez la ligne `set PATH` à partir du fichier `weblogic_nodemanager_dc_opts.win` généré. Si une variable **Path** n'existe pas dans la section **User variables for *nom_utilisateur*** (*nom_utilisateur* représentant le nom du compte utilisateur utilisé pour démarrer le serveur WebLogic), ajoutez-la en entrant `Path` comme nom de variable et le chemin situé à droite du signe égal comme valeur. Si elle existe, modifiez la valeur pour ajouter uniquement le chemin situé à droite du signe égal dans le chemin existant avec le délimiteur de chemin correct.

  3) Rechargez l'environnement.

  Avertissement : Les scripts `startNodeManager` sont générés par l'utilitaire de configuration WebLogic. Vous risquez de perdre vos modifications lorsque la configuration WebLogic sera exécutée à nouveau.

7. Si le serveur WebLogic et l'agent sont en cours d'exécution, redémarrez-les.

Résultats

Fichiers du serveur WebLogic modifiés lors de la configuration du suivi des transactions :

- Script `startManagedWebLogic`.

  – Linux AIX *WEBLOGIC_HOME*`/bin/startManagedWebLogic.sh`

  – Windows *WEBLOGIC_HOME*`\bin\startManagedWebLogic.cmd`

  où *WEBLOGIC_HOME* représente le répertoire d'installation du serveur WebLogic.

Ce fichier est mis à jour avec les paramètres de configuration requis pour la fonction de suivi des transactions. Des repères de configuration sont insérés dans le fichier pour pouvoir être utilisés lorsque vous désactivez la fonction de suivi des transactions. Un fichier de sauvegarde est sauvegardé dans le répertoire *WEBLOGIC_HOME*/bin/bak/ avant que le script ajoute ou supprime les modifications des fonctions de suivi des transactions.

Fichiers de l'agent modifiés lors de la configuration du suivi des transactions :

- Fichier de configuration de l'instance d'agent
  - Linux AIX *rép_install*/config/*nom_hôte*_wb_*nom_instance*.cfg
  - Windows *rép_install*\TMAITM6_x64*nom_hôte*_WB_*nom_instance*.cfg
- Fichier des paramètres d'environnement de l'agent
  - Linux AIX *rép_install*/config/wb_*nom_instance*.environment
  - Windows *rép_install*\TMAITM6_x64\KWBENV_*nom_instance*

où

rép_install
Chemin d'installation de l'agent. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux AIX /opt/ibm/apm/agent
- Windows C:\IBM\APM\TMAITM6_x64

hostname
Nom de l'ordinateur hôte sur lequel l'agent est installé.

nom_instance
Nom de l'instance d'agent affectée dans la rubrique sur la méthode de configuration de l'agent :

- Configuration de l'agent sur des systèmes Windows, étape «3», à la page 842
- Configuration de l'agent en répondant à des invites, étape «1», à la page 846
- Configuration de l'agent à l'aide du fichier de réponses silencieux, étape «2», à la page 847

Désactivation du suivi des transactions pour une instance Agent WebLogic
La fonction de suivi des transactions de l'Agent WebLogic peut être supprimée. Un script est fourni pour supprimer la fonction de suivi des transactions pour une instance d'agent.

Avant de commencer

Assurez-vous que le serveur WebLogic et l'Agent WebLogic sont arrêtés.

Le compte utilisateur qui exécute ce script doit disposer de droits en écriture aux répertoires et fichiers suivants :

1. Répertoire *WEBLOGIC_HOME*.
2. Répertoire *WEBLOGIC_HOME*/bin et ses fichiers.
3. Répertoire *rép_install*/config.
4. Fichier *rép_install*/config/*nom_hôte*_wb_*nom_instance*.cfg.

Procédure

Exécutez le script **unconfig** avec l'option **remove**.

1. Connectez-vous au serveur WebLogic sur lequel l'Agent WebLogic est installé.
2. Accédez au répertoire du répertoire d'installation de l'agent.
   - Linux AIX *rép_install*
   - Windows *rép_install*\TMAITM6_x64

3. Accédez au répertoire wbdchome/8.1.4.0.0/bin.
4. Exécutez **unconfig** avec l'option **remove**, le nom de l'instance d'agent et le nom du sous-noeud.
   - Pour désactiver un sous-noeud d'une instance d'agent, utilisez le paramètre *nom_sous_noeud*.
     - Linux AIX `./unconfig.sh` **remove** *nom_instance nom_sous_noeud*
     - Windows `unconfig.bat` **remove** *nom_instance nom_sous_noeud*
   - Pour désactiver tous les sous-noeuds pour une instance d'agent, omettez le paramètre *nom_sous_noeud*.
     - Linux AIX `./unconfig.sh` **remove** *nom_instance*
     - Windows `unconfig.bat` **remove** *nom_instance*
5. Démarrez l'agent et le serveur WebLogic.

où

WEBLOGIC_HOME
Répertoire d'installation du serveur WebLogic.

hostname
Nom de l'ordinateur hôte sur lequel l'agent est installé.

nom_instance
Nom de l'instance d'agent affectée dans la rubrique sur la méthode de configuration de l'agent :

- Configuration de l'agent sur des systèmes Windows, étape «3», à la page 842
- Configuration de l'agent en répondant à des invites, étape «1», à la page 846
- Configuration de l'agent à l'aide du fichier de réponses silencieux, étape «2», à la page 847

nom_sous_noeud
Nom du sous-noeud de l'instance d'agent affecté au paramètre **Nom du serveur WebLogic** dans la rubrique sur la méthode de configuration de l'agent :

- Configuration de l'agent sur des systèmes Windows, étape «6», à la page 844
- Configuration de l'agent en répondant à des invites, étape «2», à la page 846
- Configuration de l'agent à l'aide du fichier de réponses silencieux, étape «2», à la page 847

rép_install
Chemin d'installation de l'agent. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux AIX `/opt/ibm/apm/agent`
- Windows `C:\IBM\APM\TMAITM6_x64`

Désinstallation du suivi des transactions pour l'Agent WebLogic
La fonction de suivi des transactions de l'Agent WebLogic peut être désinstallée. Un script est fourni pour supprimer la fonction de suivi des transactions de toutes les instances d'agent, ainsi que le kit d'outils de suivi des transactions.

Avant de commencer

Assurez-vous que le serveur WebLogic et toutes les instances d'Agent WebLogic sont arrêtés.

Le compte utilisateur qui exécute ce script doit disposer de droits en écriture aux répertoires et fichiers suivants :

1. Répertoire *WEBLOGIC_HOME*.
2. Répertoire *WEBLOGIC_HOME*/bin et ses fichiers.
3. Répertoire *rép_install*/config.
4. Fichier *rép_install*/config/*nom_hôte*_wb_*nom_instance*.cfg.

Procédure

Exécutez le script **unconfig** avec l'option **uninstall**.

1. Connectez-vous au serveur WebLogic sur lequel l'Agent WebLogic est installé.
2. Accédez au répertoire du répertoire d'installation de l'agent.
   - Linux AIX *rép_install*
   - Windows *rép_install*\TMAITM6_x64
3. Accédez au répertoire wbdchome/8.1.4.0.0/bin.
4. Exécutez **unconfig** avec l'option **uninstall**.
   - Linux AIX ./unconfig.sh **uninstall**
   - Windows unconfig.bat **uninstall**
5. Démarrez le serveur WebLogic et toutes les instances d'agent.

où

WEBLOGIC_HOME
Répertoire d'installation du serveur WebLogic.

hostname
Nom de l'ordinateur hôte sur lequel l'agent est installé.

nom_instance
Nom de l'instance d'agent affectée dans la rubrique sur la méthode de configuration de l'agent :

- Configuration de l'agent sur des systèmes Windows, étape «3», à la page 842
- Configuration de l'agent en répondant à des invites, étape «1», à la page 846
- Configuration de l'agent à l'aide du fichier de réponses silencieux, étape «2», à la page 847

rép_install
Chemin d'installation de l'agent. Les chemins d'accès par défaut à ces journaux sont les suivants :

- Linux AIX /opt/ibm/apm/agent
- Windows C:\IBM\APM\TMAITM6_x64

Configuration de votre Tableau de bord d'Application Performance pour l'affichage des données de suivi des transactions de l'Agent WebLogic

Pour afficher les données rassemblées par la fonction de suivi des transactions de l'Agent WebLogic, des modifications doivent être apportées à la configuration de votre Tableau de bord d'Application Performance.

Avant de commencer

Effectuez l'étape «Configuration du suivi des transactions pour l'Agent WebLogic», à la page 849 avant de suivre cette procédure.

Procédure

1. Activez les données de suivi des transactions dans le Tableau de bord d'Application Performance si vous disposez de l'Agent WebLogic avec la fonction de suivi des transactions, qui est disponible dans l'offre Cloud APM, Advanced et que vous souhaitez activer la fonction de suivi des transactions.
   a) A partir de la barre de navigation, cliquez sur **Configuration système** > **Configuration d'agent**.
   La page **Configuration d'agent** s'affiche.
   b) Sélectionnez l'onglet **WebLogic**.
   c) Sélectionnez les cases à cocher pour les instances de l'agent du serveur WebLogic que vous souhaitez surveiller et effectuez l'une des actions suivantes figurant dans la liste **Actions** :

- Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Enabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour sur *Enabled*.
- Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Disabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour sur *Disabled*.

2. Pour visualiser les tableaux de bord des données de suivi des transactions de l'Agent WebLogic, ajoutez l'instance de l'Agent WebLogic à une applications de votre Tableau de bord d'Application Performance.

   Pour plus d'informations sur l'éditeur d'applications, voir Gestion des applications.
3. Assurez-vous que des comptes utilisateur sont affectés à un rôle qui inclut les droits d'accès au Tableau de bord de diagnostic pour autoriser l'accès aux boutons suivants du Tableau de bord des applications pour le suivi des transactions de l'Agent WebLogic.

   Sinon, ces boutons sont désactivés pour ces utilisateurs dans le Tableau de bord des applications.

   a. Le bouton d'analyse détaillée **Diagnostiquer** sur le widget **Slowest 5 Response Time** (Temps de réponse - les 5 les plus lents).

   b. Le bouton **Inflight Requests** sur le widget **Applications**.

Configuration de la surveillance des applications WebSphere

La configuration de la surveillance des applications WebSphere implique la configuration d'un collecteur de données pour vos serveurs d'applications. Le collecteur de données peut être autonome ou imbriqué à l'Agent WebSphere Applications.

Collecteur de données imbriqué

La plupart des serveurs d'applications WebSphere peuvent être surveillés par le collecteur de données imbriqué, excepté pour le profil Liberty sur IBM Cloud. Le collecteur de données imbriqué peut fournir toutes les fonctions de surveillance disponibles.

Pour configurer le collecteur de données imbriqué, vous devez au préalable installer l'Agent WebSphere Applications sur le système sur lequel le serveur d'applications est en cours d'exécution. Après cela, utilisez les utilitaires de configuration fournis pour configurer le collecteur de données de manière interactive ou silencieuse.

Collecteur de données autonome

Le collecteur de données autonome s'applique uniquement à WebSphere Application Server Liberty sous Linux for System x et au profil WebSphere Liberty sur IBM Cloud.

Si vous choisissez de configurer un collecteur de données autonome, vous pouvez ignorer la procédure d'installation de l'agent et configurer directement le collecteur de données dans Liberty.

Toutefois, certaines données de diagnostic à la demande, telles que le cliché de tas à l'heure actuelle ou les informations sur les demandes en cours, ne seront pas collectées par le collecteur de données autonome. Cela signifie que vous pouvez uniquement activer le collecteur de données de manière à ce qu'il collecte automatiquement les informations de cliché de tas à des intervalles spécifiés et que vous ne pouvez pas prendre d'instantané de segment de mémoire lorsque vous le souhaitez à l'aide du bouton **Take Snapshot** de la console Cloud APM. Les tableaux de bord associés aux demandes en cours qui peuvent être fournis par le collecteur de données imbriqué sont tous indisponibles au collecteur de données autonome.

Utilisez Tableau 222, à la page 856 pour déterminer le collecteur de données approprié pour votre serveur d'applications.

Tableau 222. Applications WebSphere et collecteurs de données applicables

Application à surveiller	Collecteur de données applicable	Documentation
WebSphere Application Server Traditional	Collecteur de données imbriqué	«Configuration du collecteur de données pour l'Agent WebSphere Applications», à la page 857

Tableau 222. Applications WebSphere et collecteurs de données applicables (suite)		
Application à surveiller	**Collecteur de données applicable**	**Documentation**
WebSphere Application Server Liberty (sur site)	• Collecteur de données imbriqué • Collecteur de données autonome (Linux for System x uniquement)	• «Configuration du collecteur de données pour l'Agent WebSphere Applications», à la page 857 • «Configuration du collecteur de données Liberty pour les applications sur site», à la page 906
Profil WebSphere Liberty sur IBM Cloud	Collecteur de données autonome	«Configuration du collecteur de données Liberty pour les applications IBM Cloud», à la page 910
Profil WebSphere Liberty dans un conteneur Docker	Collecteur de données imbriqué	«Surveillance de WebSphere Application Server Liberty dans un conteneur Docker», à la page 891

Configuration du collecteur de données pour l'Agent WebSphere Applications

L'Agent WebSphere Applications n'a pas besoin d'être configuré après l'installation de l'agent, à moins que vous ne souhaitez modifier le port par défaut. Vous devez toutefois configurer le collecteur de données, qui est un composant de l'agent, pour configurer la surveillance pour votre environnement WebSphere.

Pourquoi et quand exécuter cette tâche

Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.

Procédure

- (Version accélérée) Si vous n'utilisez que l'Agent WebSphere Applications sans l'ITCAM Agent for WebSphere Applications du produit hérité dans votre environnement, pour configurer rapidement l'environnement pour la surveillance, voir une procédure de configuration simplifiée dans la section «Version accélérée : configuration du collecteur de données pour l'Agent WebSphere Applications», à la page 858.
- (Configuration simple) Pour une procédure de configuration complète pour un environnement IBM Cloud Application Performance Management pur, voir la section «Configuration du collecteur de données avec l'utilitaire de configuration simple», à la page 861.
- (Configuration complète) Pour configurer le collecteur de données avec plus d'options de personnalisation, utilisez les utilitaires de configuration complète. Pour obtenir des instructions, voir «Configuration ou reconfiguration du collecteur de données à l'aide des utilitaires de configuration complète», à la page 863.
- (Configuration en mode silencieux) Pour déployer la même surveillance pour plusieurs instances de serveur d'applications, configurez le collecteur de données en mode silencieux. Pour obtenir des instructions, voir «Configuration du collecteur de données en mode silencieux», à la page 872.
- (WebSphere Portal Server) Pour surveiller les instances WebSphere Portal Server, utilisez la procédure de configuration avancée. Pour obtenir des instructions, voir «Configuration ou reconfiguration du collecteur de données à l'aide des utilitaires de configuration complète», à la page 863.
- (Configuration manuelle) Si vous ne pouvez pas utiliser les utilitaires de configuration fournis pour configurer le collecteur de données pour l'Agent WebSphere Applications, configurez manuellement le collecteur de données dans la console d'administration WebSphere. Pour obtenir des instructions, voir

«Configuration manuelle du collecteur de données si les utilitaires de configuration échouent», à la page 879.

- (Coexistence des agents) Pour configurer le collecteur de données de sorte qu'il fonctionne dans un environnement de coexistence des agents où l'Agent WebSphere Applications et l'ITCAM Agent for WebSphere Applications sont installés, voir «(Coexistence d'agent) Configuration de l'Agent WebSphere Applications et du collecteur de données», à la page 883.
- (Surveillance de Docker) Pour surveiller WebSphere Application Server Liberty s'exécutant dans un conteneur Docker, voir «Surveillance de WebSphere Application Server Liberty dans un conteneur Docker», à la page 891.

Version accélérée : configuration du collecteur de données pour l'Agent WebSphere Applications
L'Agent WebSphere Applications n'a pas besoin d'être configuré après l'installation de l'agent. Vous devez toutefois configurer le collecteur de données, qui est un composant de l'agent, pour configurer la surveillance pour votre environnement WebSphere.

Avant de commencer

1. Installez l'Agent WebSphere Applications sur le système où le serveur d'applications à surveiller est installé et en cours d'exécution.
2. Vérifiez les exigences d'accès utilisateur.
   - Windows Utilisez l'ID administrateur utilisé pour installer le serveur d'applications pour configurer le collecteur de données. Assurez-vous que cet ID utilisateur dispose du droit complet en écriture sur le répertoire de base du collecteur de données, *rép_install*\dchome\7.3.0.14.08.
   - Linux AIX Utilisez l'ID utilisateur employé pour installer le serveur d'applications pour configurer le collecteur de données. Assurez-vous que cet ID utilisateur dispose de droits en lecture et en écriture sur les sous-répertoires suivants dans *rép_install*/yndchome/7.3.0.14.08 :
     - bin
     - data
     - runtime

Pourquoi et quand exécuter cette tâche

Un utilitaire de configuration simple, `simpleconfig`, est utilisé dans cette procédure pour fournir la configuration de base du collecteur de données.

L'utilitaire `simpleconfig` configure le collecteur de données avec les paramètres par défaut. Pour configurer le collecteur de données avec plus d'options de personnalisation, utilisez les utilitaires de configuration complète, `config`, dans le même répertoire. Pour obtenir des instructions, voir «Configuration ou reconfiguration du collecteur de données à l'aide des utilitaires de configuration complète», à la page 863.

Dans la plupart des cas, l'utilitaire `simpleconfig` suffit. Pour un environnement plus complexe, vous pouvez utiliser l'utilitaire de configuration `config` pour configurer le collecteur de données. Si l'utilitaire `simpleconfig` échoue, utilisez `config` à la place.

Procédure

1. Connectez-vous au système à l'aide de l'ID utilisateur utilisé pour installer le serveur d'applications.
2. Accédez au répertoire `bin` au sein du répertoire de base du collecteur de données.
   - Windows *rép_install*\dchome\7.3.0.14.08\bin
   - Linux AIX *rép_install*/yndchome/7.3.0.14.08/bin
3. Exécutez l'utilitaire de configuration simple suivant:
   - Windows **simpleconfig.bat**

- Linux AIX **./simpleconfig.sh**

4. Suivez les invites pour continuer la configuration du collecteur de données.

   Vous êtes tenu d'effectuer quelques-unes ou l'ensemble des actions suivantes selon les paramètres du serveur d'applications :

   - Pour un WebSphere Application Server traditionnel :
     - Sélectionnez le répertoire d'installation WebSphere découvert automatiquement ou indiquez-le manuellement.
     - Sélectionnez le profil WebSphere Application Server à surveiller.
     - Sélectionnez le profil des propriétés de sécurité à utiliser ou fournissez le nom d'utilisateur et le mot de passe de la console d'administration WebSphere (si la sécurité est activée pour le serveur d'applications).
   - Pour WebSphere Application Server Liberty :
     - Indiquez le chemin d'accès complet du répertoire de base Liberty qui contient les répertoires `bin` et `servers`. Par exemple, `/opt/ibm/wlp`.
     - Indiquez le répertoire de base du JRE qui est utilisé par Liberty.
5. Une fois que la configuration du collecteur de données est terminée, redémarrez le serveur d'applications.
   a) Accédez au répertoire `bin` situé sous le répertoire de base du profil de serveur d'applications. Par exemple, `opt/IBM/WebSphere/AppServer/profiles/`*`nom_profil`*`/bin`.
   b) Arrêtez le serveur d'applications en entrant la commande **stopServer** dans la console de commande.
      - Linux AIX `./stopServer.sh` *`nom_serveur`*
      - Windows `stopServer.bat` *`nom_serveur`*
   c) A l'invite, entrez l'ID utilisateur et le mot de passe de l'administrateur de la console d'administration WebSphere.
   d) Redémarrez le serveur d'applications en entrant la commande **startServer** dans la console de commande.
      - Linux AIX `./startServer.sh` *`nom_serveur`*
      - Windows `startServer.bat` *`nom_serveur`*
6. Connectez-vous à la console Cloud APM pour afficher les données dans les tableaux de bord.
   a) Accédez à la console en utilisant le lien fourni dans l'e-mail vous signalant que votre service est prêt. Vous pouvez également accéder à la console à partir du site Web IBM Marketplace. Pour des instructions détaillées, voir «Démarrage de la console Cloud APM», à la page 1003.
   b) Utilisez l'éditeur d'applications pour ajouter le serveur d'applications surveillé au Tableau de bord d'Application Performance. Vous pouvez l'ajouter en tant que nouveau composant à votre application existante ou créer une application à laquelle ajouter ce composant.

      Pour plus d'informations sur l'éditeur d'applications, voir «Gestion des applications», à la page 1129.

Résultats

Le collecteur de données permet de surveiller l'instance de serveur d'applications. Gardez à l'esprit que la collecte de données peut augmenter la surcharge du serveur d'applications. Vous pouvez contrôler la collecte de données avec des options de configuration plus avancées pour l'optimisation.

Vérification des exigences d'accès utilisateur

L'Agent WebSphere Applications a certaines exigences d'accès utilisateur pour l'ID utilisateur qui doit configurer le collecteur de données.

Pourquoi et quand exécuter cette tâche

Utilisez l'ID employé pour installer le serveur d'applications pour configurer le collecteur de données après avoir accordé les droits appropriés à l'ID d'installation du serveur d'applications.

Procédure

- Windows Utilisez l'ID administrateur utilisé pour installer le serveur d'applications pour configurer le collecteur de données. Assurez-vous que cet ID utilisateur dispose du droit complet en écriture sur le répertoire de base du collecteur de données, *rép_install*\dchome\7.3.0.14.08.
- Linux AIX Utilisez l'ID utilisateur employé pour installer le serveur d'applications pour configurer le collecteur de données. Assurez-vous que cet ID utilisateur dispose de droits en lecture et en écriture sur les sous-répertoires suivants dans *rép_install*/yndchome/7.3.0.14.08 :
  - bin
  - data
  - logs
  - runtime

  A faire : Si vous utilisez des ID utilisateur différents pour installer les serveurs d'applications, vous devrez peut-être faire de même pour configurer le collecteur de données. Après avoir configuré le collecteur de données pour la première fois, accordez le droit en écriture sur les fichiers suivants chaque fois que vous utilisez un ID utilisateur différent pour configurer le collecteur de données, où *nom_profil* correspond au nom de profil du serveur d'applications :
  - *rép_install*/yndchome/7.3.0.14.08/data/findservers.inputlist
  - *rép_install*/yndchome/7.3.0.14.08/data/*profile_name*.findservers.progress
  - *rép_install*/yndchome/7.3.0.14.08/data/config_inputlist
  - *rép_install*/yndchome/7.3.0.14.08/runtime/custom/connections.properties

Gestion d'un autre collecteur de données existant dans le serveur d'applications

Si un collecteur de données existe déjà dans le serveur d'applications, vous devez décider quoi en faire afin d'éviter un conflit avec le collecteur de données de l'Agent WebSphere Applications.

Pourquoi et quand exécuter cette tâche

Il est possible que les types de collecteur de données suivants existent déjà dans le serveur d'applications qui doit être surveillé :

- Le collecteur de données de l'Agent WebSphere Applications, qui est installé dans une version antérieure d'IBM Cloud Application Performance Management
- Le collecteur de données de l'ITCAM Agent for WebSphere Applications, qui est installé dans l'ancienne infrastructure IBM® Tivoli® Monitoring
- Tout autre collecteur de données qui n'est pas fourni par IBM

Procédure

Prenez les mesures appropriées afin d'éviter les conflits entre collecteurs de données.

- Pour une version antérieure du collecteur de données de l'Agent WebSphere Applications installée dans une version antérieure d'IBM Cloud Application Performance Management, vous avez les options suivantes :

  - Faites migrer le collecteur de données à l'aide de l'utilitaire de migration qui se trouve dans le répertoire de base du collecteur de données le plus récent. Pour obtenir des instructions, voir «Agent WebSphere Applications : migration du collecteur de données», à la page 1179.
  - Annulez la configuration la version antérieure du collecteur de données, puis configurez à nouveau le collecteur de données à l'aide de l'utilitaire de configuration qui se trouve dans le répertoire de base du collecteur de données le plus récent. Pour plus d'informations sur l'annulation de la configuration du collecteur de données, voir «Agent WebSphere Applications : Annulation de la configuration du collecteur de données», à la page 152.
- Pour le collecteur de données de l'ITCAM Agent for WebSphere Applications, effectuez les étapes suivantes si vous voulez déployer la surveillance dans un environnement de coexistence des agents :
  a) Désinstallez le collecteur de données de l'ITCAM Agent for WebSphere Applications.
  b) Ne configurez qu'un seul collecteur de données pour envoyer les données à la fois à l'Agent WebSphere Applications et à l'ITCAM Agent for WebSphere Applications. Pour obtenir des instructions, voir «(Coexistence d'agent) Configuration de l'Agent WebSphere Applications et du collecteur de données», à la page 883.
- Pour les autres collecteurs de données non fournis par IBM, évaluez s'il est nécessaire de les supprimer. Le collecteur de données de l'Agent WebSphere Applications utilise la manipulation du code d'octet Java pour collecter les données. Les autres collecteurs de données qui utilisent la même méthode de collecte des données peuvent être en conflit avec le collecteur de données de l'Agent WebSphere Applications.

Configuration du collecteur de données avec l'utilitaire de configuration simple
L'Agent WebSphere Applications démarre automatiquement après l'installation, mais vous devez configurer manuellement le collecteur de données, un composant de l'agent, pour surveiller des instances de serveur d'applications.

Avant de commencer

- Assurez-vous que les exigences relatives à l'accès utilisateur sont remplies dans votre environnement. Pour obtenir des instructions, voir «Vérification des exigences d'accès utilisateur», à la page 860.
- Si un autre collecteur de données existe dans le serveur d'applications qui doit être surveillé, prenez les mesures appropriées afin d'éviter des conflits entre collecteurs de données. Pour plus d'informations, voir «Gestion d'un autre collecteur de données existant dans le serveur d'applications», à la page 860.

Pourquoi et quand exécuter cette tâche

Important :

- Si vous souhaitez configurer le collecteur de données pour la surveillance de ressources uniquement ou pour définir des options supplémentaires, utilisez la procédure de configuration complète. Pour obtenir des instructions, voir «Configuration ou reconfiguration du collecteur de données à l'aide des utilitaires de configuration complète», à la page 863.
- Si vous souhaitez modifier le nom du serveur dans l'interface utilisateur de surveillance, reconfigurez le collecteur de données et indiquez un alias de serveur. Pour obtenir des instructions, voir «Configuration ou reconfiguration du collecteur de données à l'aide des utilitaires de configuration complète», à la page 863.

Pour l'Agent WebSphere Applications, les variables *base_cd* font référence au répertoire de base du collecteur de données. L'emplacement de la variable *rép_base_cd* sur chaque système d'exploitation est le suivant :

- Windows *rép_install*\dchome\7.3.0.14.08
- Linux AIX *rép_install*/yndchome/7.3.0.14.08

Procédure

1. Connectez-vous au système à l'aide de l'ID utilisateur utilisé pour installer le serveur d'applications.

2. Accédez au répertoire bin au sein du répertoire de base du collecteur de données.
   - Windows *rép_install*\dchome\7.3.0.14.08\bin
   - Linux AIX *rép_install*/yndchome/7.3.0.14.08/bin
3. Exécutez l'utilitaire de configuration simple suivant:
   - Windows simpleconfig.bat
   - Linux AIX ./simpleconfig.sh

   L'utilitaire **simpleconfig** reconnaît automatiquement les répertoires de base des serveurs d'applications.
4. Suivez les invites pour continuer la configuration du collecteur de données.

   Vous êtes tenu d'effectuer les actions suivantes selon les paramètres du serveur d'applications :
   - Pour un WebSphere Application Server traditionnel :
     - Sélectionnez le répertoire d'installation WebSphere découvert automatiquement ou indiquez-le manuellement.
     - Sélectionnez le profil WebSphere Application Server à surveiller.
     - Sélectionnez le profil des propriétés de sécurité à utiliser ou fournissez le nom d'utilisateur et le mot de passe de la console d'administration WebSphere (si la sécurité est activée pour le serveur d'applications).
   - Pour WebSphere Application Server Liberty :
     - Indiquez le chemin d'accès complet du répertoire de base Liberty qui contient les répertoires bin et servers (par exemple, /opt/ibm/wlp).
     - Indiquez le répertoire de base du JRE qui est utilisé par Liberty.
5. Si possible, redémarrez l'instance de serveur d'applications une fois que la configuration du collecteur de données est terminée.
   a) Accédez au répertoire bin situé sous le répertoire de base du profil de serveur d'applications. Par exemple, opt/IBM/WebSphere/AppServer/profiles/*nom_profil*/bin.
   b) Arrêtez le serveur d'applications en entrant la commande **stopServer** dans la console de commande.
      - Linux AIX ./stopServer.sh *nom_serveur*
      - Windows stopServer.bat *nom_serveur*
   c) A l'invite, entrez l'ID utilisateur et le mot de passe de l'administrateur de la console d'administration WebSphere.
   d) Redémarrez le serveur d'applications en entrant la commande **startServer** dans la console de commande.
      - Linux AIX ./startServer.sh *nom_serveur*
      - Windows startServer.bat *nom_serveur*

Résultats

- Le collecteur de données est configuré pour surveiller toutes les instances d'un profil ou, dans le cas de WebSphere Application Server Liberty, une instance unique ou plusieurs instances dans le même répertoire. Pour surveiller plusieurs profils ou instances, répétez la configuration.
- Il est configuré dans les instances de serveur, fournissant ainsi un niveau de surveillance maximal.
- Pour Cloud APM, Base, la surveillance des ressources est activée.
- Pour Cloud APM, Advanced, la surveillance des ressources, le suivi des transactions et les données de diagnostic sont activés.

Limitation connue : Lors de la surveillance de WebSphere Application Server Liberty, le collecteur de données ne peut pas générer d'événements JNDI (Java Naming and Directory Interface),

Que faire ensuite

- Connectez-vous à la console Cloud APM et utilisez l'éditeur d'applications pour ajouter le serveur d'applications surveillée au Tableau de bord d'Application Performance. Pour obtenir des instructions de démarrage de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir «Gestion des applications», à la page 1129.

  A faire : Si l'Agent WebSphere Applications est configuré pour surveiller WebSphere Portal Server, il est lié au composant d'application WebSphere Portal Server dans le Tableau de bord d'Application Performance, pas à WebSphere Application Server.
- Si l'interface utilisateur de surveillance de la Tableau de bord d'Application Performance ne fournit pas d'informations sur l'instance de serveur d'applications, redémarrez le composant agent de surveillance de l'Agent WebSphere Applications en procédant comme suit :
  - Windows

    ```
    cd rép_install\bin
    was-agent.bat stop
    was-agent.bat start
    ```
  - Linux AIX

    ```
    cd rép_install/bin
    ./was-agent.sh
    stop
    ./was-agent.sh start
    ```

Configuration ou reconfiguration du collecteur de données à l'aide des utilitaires de configuration complète

Si vous souhaitez définir des options de configuration supplémentaires, vous pouvez utiliser les utilitaires de configuration complète (en mode interactif ou silencieux) pour configurer le collecteur de données plutôt que l'utilitaire de configuration simple. Vous pouvez également utiliser ces utilitaires de configuration complète pour reconfigurer le collecteur de données déjà configuré. En outre, vous devez utiliser l'utilitaire de configuration complète pour configurer la surveillance pour les instances WebSphere Portal Server.

Avant de commencer

- Assurez-vous que les exigences relatives à l'accès utilisateur sont remplies dans votre environnement. Pour obtenir des instructions, voir «Vérification des exigences d'accès utilisateur», à la page 860.
- Si un autre collecteur de données existe dans le serveur d'applications qui doit être surveillé, prenez les mesures appropriées afin d'éviter des conflits entre collecteurs de données. Pour plus d'informations, voir «Gestion d'un autre collecteur de données existant dans le serveur d'applications», à la page 860.

Pourquoi et quand exécuter cette tâche

Les utilitaires de configuration et de reconfiguration se trouvent dans les répertoires suivants :

- Windows *rép_install*\dchome\7.3.0.14.08\bin
- Linux AIX *rép_install*/yndchome/7.3.0.14.08/bin

Procédure

- L'utilitaire de configuration se nomme **config**. La configuration du collecteur de données avec l'utilitaire de configuration complète peut s'avérer nécessaire dans les cas suivants :
  - L'utilitaire de configuration **simpleconfig** échoue.

- Vous souhaitez configurer la surveillance pour les instances WebSphere Portal Server.
- Vous souhaitez indiquer un alias de serveur qui s'affiche dans l'interface utilisateur de surveillance pendant la configuration du collecteur de données.
- Vous souhaitez disposer d'un contrôle plus précis des données à collecter. Par exemple, vous voulez n'utiliser que la surveillance des ressources et désactiver le suivi des données de diagnostics et des transactions.
- Vous ne voulez pas configurer tous les serveurs d'applications en même temps dans le même profil.
- Le collecteur de données n'est pas configuré dans le serveur d'applications et vous souhaitez le reconfigurer.

Pour plus d'informations sur l'utilitaire de configuration complète interactive, voir «Configuration du collecteur de données en mode interactif», à la page 864.

- L'utilitaire de reconfiguration se nomme **reconfig**. La reconfiguration du collecteur de données peut s'avérer nécessaire dans les cas suivants :
  - Vous voulez reconfigurer le collecteur de données après qu'il a été configuré en mode interactif ou en mode silencieux.

  Pour plus d'informations sur l'utilitaire de reconfiguration interactive, voir «Reconfiguration du collecteur de données en mode interactif», à la page 869.
- Pour une configuration en mode silencieux, voir «Configuration du collecteur de données en mode silencieux», à la page 872.

Configuration du collecteur de données en mode interactif

Utilisez l'utilitaire de configuration interactif (`config.sh` ou `config.bat`) pour configurer le collecteur de données lorsque l'utilitaire `simpleconfig` échoue. Vous pouvez utiliser l'utilitaire `config.sh` ou `config.bat` pour configurer le collecteur de données pour chaque instance de serveur d'applications que vous voulez surveiller.

Avant de commencer

Si vous configurez le collecteur de données pour surveiller WebSphere Application Server Liberty, définissez la variable d'environnement système **JAVA_HOME** sur la même machine JVM que celle utilisée pour le serveur d'applications. Par exemple, sur un système Windows, associez **JAVA_HOME** à la valeur `C:\Program Files\IBM\java`. Sur un système Linux, exécutez `export JAVA_HOME=/opt/IBM/java`.

Pourquoi et quand exécuter cette tâche

Utilisez l'utilitaire de configuration complète pour configurer le collecteur de données :

- Windows *rép_install*`\dchome\7.3.0.14.08\bin\config.bat`
- Linux AIX *rép_install*`/yndchome/7.3.0.14.08/bin/config.sh`

Procédure

Pour reconfigurer le collecteur de données en répondant aux invites, procédez comme suit :

1. Connectez-vous au système à l'aide de l'ID utilisateur utilisé pour installer le serveur d'applications.
2. Accédez au répertoire `bin` situé dans le répertoire de base du collecteur de données *base_cd*.
3. Démarrez l'utilitaire de configuration à l'aide de la commande suivante :
   - Windows `config.bat`
   - Linux AIX `./config.sh`

   L'utilitaire de configuration affiche les adresses IP et les noms d'hôte de toutes les cartes réseau qui sont détectées sur le système informatique local.

4. Entrez le nombre qui correspond à l'adresse IP et au nom d'hôte. Si l'adresse IP et le nom d'hôte que vous voulez utiliser ne figurent pas dans la liste, entrez l'adresse IP ou le nom d'hôte.
5. Indiquez le répertoire de base du serveur d'applications qui doit être surveillé.
   - Pour un serveur WebSphere Application Server traditionnel, entrez le nombre qui correspond à un répertoire de base de serveur d'applications reconnu automatiquement, ou indiquez le chemin d'accès complet d'un répertoire de base de serveur d'applications.
   - Pour WebSphere Application Server Liberty, entrez le chemin d'accès complet au répertoire de base de WebSphere Application Server Liberty qui contient les répertoires `bin` et `servers`, par exemple `/opt/ibm/wlp`.
6. Si vous configurez le collecteur de données pour WebSphere Application Server Liberty, vous êtes invité à indiquer le répertoire de base Java. Indiquez le répertoire de base Java qui est utilisé pour le serveur d'applications. Par exemple, `/opt/IBM/java`.
7. Lorsque l'utilitaire de configuration répertorie tous les profils sous le répertoire de base du serveur d'applications spécifié, entrez le nombre qui correspond au profil du serveur d'applications que vous souhaitez configurer.
   - Pour un serveur WebSphere Application Server traditionnel, l'utilitaire de configuration indique ensuite si WebSphere Global Security est activé pour le profil WebSphere Application Server que vous avez spécifié. Si la sécurité globale n'est pas activée, passez à l'étape «9», à la page 865.
   - Pour WebSphere Application Server Liberty, passez à l'étape «10», à la page 865.
8. Si la sécurité globale n'est pas activée pour le profil WebSphere Application Server, indiquez s'il faut récupérer les paramètres de sécurité dans le fichier de propriétés d'un client. Entrez 1 pour permettre à l'utilitaire de configuration d'extraire le nom d'utilisateur et le mot de passe à partir du fichier de propriétés de client approprié. Sinon, entrez 2 pour entrer le nom d'utilisateur et le mot de passe.

   Le collecteur de données communique avec les services d'administration de WebSphere en utilisant l'invocation RMI (Remote Method Invocation) ou le protocole SOAP. Si la sécurité globale est activée pour un profil de serveur d'applications, vous devez indiquer l'ID utilisateur et le mot de passe d'un utilisateur qui est autorisé à se connecter à la console d'administration de WebSphere Application Server pour ce profil. Vous avez également la possibilité de chiffrer le nom d'utilisateur et le mot de passe et de les stocker dans des fichiers de propriétés de client avant de configurer le collecteur de données. Vous devez utiliser le fichier `sas.client.props` pour une connexion RMI, ou le fichier `soap.client.props` pour une connexion SOAP.
9. Lorsque vous êtes invité à entrer le nom d'hôte de la console d'administration WebSphere, appuyez sur Entrée pour accepter les valeurs par défaut ou indiquez le nom d'hôte ou l'adresse IP de la console d'administration WebSphere. La valeur par défaut est `localhost`.

   A faire : Pour un environnement de déploiement réseau, entrez le nom d'hôte ou l'adresse IP de Deployment Manager.
10. Lorsque l'utilitaire de configuration affiche une liste de toutes les instances de serveur qui ne sont pas encore configurées pour la collecte de données, sélectionnez une ou plusieurs instances de serveur d'applications dans la liste. Entrez le nombre qui correspond à l'instance de serveur d'applications à configurer pour la collecte de données ou entrez un astérisque (*) pour configurer toutes les instances de serveur d'applications pour la collecte de données. Pour spécifier un sous-ensemble de serveurs, entrez les numéros qui représentent les serveurs, séparés par des virgules. Par exemple, `1,2,3`.

    A faire :
    - Pour un environnement autonome, les instances de serveur d'applications doivent s'exécuter pendant la configuration. (Une instance de WebSphere Application Server Liberty n'a pas besoin d'être en cours d'exécution).
    - Pour un environnement de déploiement réseau, Deployment Manager doit être en cours d'exécution.
    - Assurez-vous que les instances de serveur d'applications que vous sélectionnez sont les serveurs réels qui hébergent les applications ou les services que vous voulez surveiller.

11. Dans la section **Integration with Agent for WebSphere Applications**, indiquez si vous souhaitez intégrer le collecteur de données à l'Agent WebSphere Applications. Vous devez entrer 1 pour sélectionner cette option d'intégration, puis appuyer sur Entrée.

    Le serveur sélectionné sera enregistré pour la surveillance des ressources PMI.
12. Si vous configurez le collecteur de données pour un serveur WebSphere Application Server traditionnel, indiquez si vous souhaitez configurer le collecteur de données dans l'instance de serveur d'applications.

    - Entrez 1 pour configurer le collecteur de données dans le serveur d'applications. Avec cette option, le collecteur de données est intégré au serveur d'applications, ce qui est nécessaire à la collecte complète des données de surveillance opérationnelle et de diagnostic. Cependant, la configuration du collecteur de données dans le serveur d'applications nécessite de redémarrer ce dernier. En outre, le collecteur de données peut affecter les performances de serveur.
    - Entrez 2 pour ne pas configurer le collecteur de données dans le serveur d'applications et passez à l'étape «14», à la page 866. Avec cette option, le collecteur de données s'exécute comme un processus autonome et seule la surveillance des ressources peut être activée.
13. A l'invite, indiquez s'il faut activer ou non le collecteur de données pour les données de diagnostic. Entrez 1 pour activer la collecte des données de diagnostic. La valeur par défaut est 2.
14. Lorsque vous êtes invité à entrer le nom d'hôte de l'agent de surveillance V8, entrez le nom d'hôte ou l'adresse IP de l'Agent WebSphere Applications ou appuyez sur Entrée pour accepter la valeur par défaut. La valeur par défaut correspond au choix que vous avez effectué à l'étape 3.

    L'agent de surveillance V8 fait référence à l'Agent WebSphere Applications, qui est installé avec IBM Cloud Application Performance Management.
15. Lorsque vous êtes invité à entrer le numéro de port de l'agent de surveillance V8, entrez le numéro de port de l'Agent WebSphere Applications ou appuyez sur Entrée pour accepter la valeur par défaut. La valeur par défaut est 63335.
16. Lorsque vous êtes invité à indiquer si l'agent de surveillance V6 pour WebSphere Applications doit être configuré, appuyez sur Entrée pour accepter la valeur par défaut No.

    L'agent de surveillance V6 fait référence à l'ITCAM Agent for WebSphere Applications, qui est installé dans l'ancienne infrastructure IBM® Tivoli® Monitoring. La configuration de l'agent de surveillance V6 n'est requise que pour l'environnement de coexistence des agents.
17. Lorsque vous êtes invité à entrer l'alias de serveur, appuyez sur Entrée pour accepter la valeur par défaut ou entrez un autre alias. Si vous configurez plusieurs instances de serveur d'applications, l'utilitaire de configuration vous invite à indiquer un alias pour chaque instance.

    Important : L'alias ne peut contenir que les caractères suivants : A-Z, a-z, soulignement (_), tiret (-) et point (.). N'utilisez pas d'autres caractères dans l'alias.

    L'alias de serveur est le premier qualificateur du nom d'instance d'agent (également appelé MSN) affiché sur la console Cloud APM. La valeur par défaut est le nom du noeud combiné au nom du serveur. Par exemple, l'alias **node1server1** indique le serveur **server1** dans le noeud **node1**.
18. Lorsque vous êtes invité à entrer un numéro de port pour la surveillance des ressources PMI, appuyez sur Entrée pour accepter la valeur par défaut ou entrez un nouveau numéro. La valeur par défaut est 63355.

    Ce port est utilisé pour la communication interne entre les composants qui s'exécutent sur le même hôte. Si le port par défaut est utilisé, vous pouvez définir un numéro différent.
19. Dans la section **Prise en charge du suivi des transactions**, indiquez si vous souhaitez activer le suivi des transactions. Entrez 1 pour activer la prise en charge du suivi des transactions. Autrement, entrez 2 et passez à l'étape «22», à la page 867.
20. Lorsque vous êtes invité à indiquer le nom d'hôte ou l'adresse IP de Transaction Framework Extension, appuyez sur Entrée pour accepter la valeur par défaut ou entrez un autre nom d'hôte ou une autre adresse IP.

    Transaction Framework Extension est un composant interne de l'Agent WebSphere Applications qui recueille des mesures à partir du collecteur de données.

21. Lorsque vous êtes invité à entrer le numéro de port que le collecteur de données utilise pour se connecter à Transaction Framework Extension, appuyez sur Entrée pour accepter la valeur par défaut ou entrez un autre numéro de port. La valeur par défaut est 5457.
22. Indiquez si vous voulez intégrer le collecteur de données à Application Performance Diagnostics Lite. Appuyez sur Entrée pour accepter la valeur par défaut pour Non.
23. Dans la section **Paramètres avancés**, indiquez si vous souhaitez modifier le chemin du journal de la récupération de place. Entrez 1 pour sélectionner un chemin d'accès au journal de récupération de place. Autrement, entrez 2 et passez à l'étape «25», à la page 867. Pour utiliser le chemin d'accès au journal déjà indiqué dans l'argument JVM du serveur d'applications, entrez 2.
24. Indiquez le chemin de la collecte de récupération de place. Entrez un nom de fichier avec son chemin d'accès complet. Pour WebSphere Application Server Liberty, n'utilisez pas de variables dans le chemin d'accès. Le collecteur de données modifie automatiquement le nom du fichier journal en y ajoutant des informations sur l'instance de serveur.

    Par exemple, si vous indiquez `gc.log` comme nom de fichier, le nom réel est défini sur *`nom_profil.nom-cellule.nom_noeud.nom_serveur`*`.gc.log` pour chaque instance de serveur d'applications configurée.

    Important : Dans le chemin d'accès au journal de récupération de place, vous pouvez utiliser des variables WebSphere, telles que `${SERVER_LOG_ROOT}`. Cependant, n'utilisez pas de modèles, tels que `%pid`.
25. Consultez le récapitulatif de la configuration du collecteur de données à appliquer aux instances de serveur d'applications définies. Reconfigurez les parties de la configuration du collecteur de données avant d'appliquer les modifications, si nécessaire.
26. Entrez a pour accepter vos modifications.
27. A l'invite, indiquez si vous souhaitez créer une copie de sauvegarde de votre configuration en cours. Entrez 1 pour créer une sauvegarde de la configuration en cours. Sinon, entrez 2.

    L'utilitaire de configuration applique les modifications et présente un message d'état pour indiquer que la configuration du collecteur de données pour le profil est terminée .
28. Si vous configurez le collecteur de données pour le serveur WebSphere Application Server traditionnel, redémarrez les instances de serveur d'applications ou redémarrez l'agent, selon l'option que vous avez choisie à l'étape «12», à la page 866.
    - Si vous avez activé le collecteur de données dans le serveur d'applications, redémarrez les instances de serveur d'applications, comme indiqué par l'utilitaire de configuration.
    - Si vous avez activé la surveillance des ressources PMI sans activer le collecteur de données dans le serveur d'applications, redémarrez l'Agent WebSphere Applications en exécutant les commandes suivantes :
      – Windows

      ```
      cd rép_install\bin
      was-agent.bat stop
      was-agent.bat start
      ```

      – Linux AIX

      ```
      cd rép_install/bin
      ./was-agent.sh
      stop
      ./was-agent.sh start
      ```

    La configuration du collecteur de données entre en vigueur une fois que le serveur d'applications ou l'agent a redémarré.
29. Connectez-vous à la console Cloud APM pour afficher les données dans les tableaux de bord.
    a) Accédez à la console en utilisant le lien fourni dans l'e-mail vous signalant que votre service est prêt. Vous pouvez également accéder à la console à partir du site Web IBM Marketplace. Pour des instructions détaillées, voir «Démarrage de la console Cloud APM», à la page 1003.

b) Utilisez l'éditeur d'applications pour ajouter le serveur d'applications surveillé au Tableau de bord d'Application Performance. Vous pouvez l'ajouter en tant que nouveau composant à votre application existante ou créer une application à laquelle ajouter ce composant.

Pour plus d'informations sur l'éditeur d'applications, voir «Gestion des applications», à la page 1129.

Que faire ensuite

- Si l'ID utilisateur actuel utilisé pour configurer le collecteur de données n'est pas identique à l'ID de l'utilisateur qui exécute le serveur d'applications, vérifiez que l'ID utilisateur de configuration du collecteur de données dispose des droits en lecture et en écriture sur les répertoires `runtime` et `logs` dans le répertoire de base du collecteur de données. Ces deux sous-répertoires sont créés par l'ID de l'utilisateur qui exécute le serveur d'applications lorsque le serveur est redémarré.
- Connectez-vous à la console Cloud APM pour afficher les données de surveillance dans les tableaux de bord. Si les données de surveillance ne sont pas disponibles immédiatement, redémarrez l'Agent WebSphere Applications en exécutant les commandes suivantes :
  - Windows

    ```
    cd rép_install\bin
    was-agent.bat stop
    was-agent.bat start
    ```

  - Linux AIX

    ```
    cd rép_install/bin
    ./was-agent.sh
    stop
    ./was-agent.sh start
    ```

- La modification de l'alias de serveur entraîne la modification du nom d'instance de l'agent enregistré dans la console Cloud APM. Si ce n'est pas la première fois que vous configurez le collecteur de données et que vous avez modifié l'alias de serveur, vous devez vider certains fichiers cache en effectuant les opérations suivantes :
  1. Arrêtez l'agent de surveillance s'il est en cours d'exécution.
  2. Ouvrez le fichier *nom_hôte*`_yn.xml` dans le répertoire suivant avec un éditeur de texte, où *nom_hôte* est le nom de l'hôte où l'Agent WebSphere Applications est installé.
     - Windows *rép_install*`\TMAITM6_x64` (la valeur par défaut est `C:\IBM\APM\TMAITM6_x64`)
     - Linux AIX *rép_install*`/config` (la valeur par défaut est `/opt/ibm/apm/agent/config`)
  3. Recherchez la ligne qui commence par la chaîne suivante et qui contient le nom de serveur précédent. Par exemple, `was85.win4net01Cell02.win4net01Node02.AppSrv01.server1`, où `server1` est le nom précédent du serveur d'applications.

     ```
     <!ENTITY code_produit_was.nom_cellule.nom_noeud.nom_profil.nom_serveur
     ```

     où *code_produit_was* est le code produit de WebSphere Application Server ; *nom_cellule* est le nom de la cellule ; *nom_noeud* est le nom du noeud ; *nom_profil* est le nom du profil de serveur d'applications ; *nom_serveur* est le nom précédent du serveur d'applications.
  4. Dans le répertoire en cours, recherchez le fichier `.XML` indiqué sur la ligne et supprimez-le.
  5. Supprimez la ligne que vous avez recherchée à l'étape 3 dans le fichier *nomhôte*`_yn.xml`.
  6. A la fin du fichier *nom_hôte*`_yn.xml`, supprimez la ligne qui contient les noms de serveur précédents.
  7. Sauvegardez et fermez le fichier.
  8. Redémarrez l'agent de surveillance.

Reconfiguration du collecteur de données en mode interactif
Si vous avez configuré le collecteur de données pour surveiller une ou plusieurs instances de serveur d'applications, vous pouvez le reconfigurer à l'aide de l'utilitaire de reconfiguration (`reconfig.sh` ou `reconfig.bat`).

Avant de commencer

Si vous configurez le collecteur de données pour surveiller WebSphere Application Server Liberty, définissez la variable d'environnement système **JAVA_HOME** sur la même machine JVM que celle utilisée pour le serveur d'applications. Par exemple, sur un système Windows, associez **JAVA_HOME** à la valeur `C:\Program Files\IBM\java`. Sur un système Linux, exécutez `export JAVA_HOME=/opt/IBM/java`.

Pourquoi et quand exécuter cette tâche

Utilisez l'utilitaire de reconfiguration complète pour configurer le collecteur de données :

- Windows *rép_install*`\dchome\7.3.0.14.08\bin\reconfig.bat`
- Linux AIX *rép_install*`/yndchome/7.3.0.14.08/bin/reconfig.sh`

A faire : L'utilitaire **reconfig** n'est pas applicable dans les cas suivants. A la place, utilisez l'utilitaire de configuration **config**. Bien que cet utilitaire vous avertisse que le serveur est déjà configuré, il peut toujours effectuer toutes les modifications souhaitées.

- Le collecteur de données est déjà configuré pour la surveillance des ressources uniquement et vous voulez le reconfigurer.
- Vous voulez reconfigurer le collecteur de données pour WebSphere Portal Server.

Conseil : Dans les invites vous invitant à définir les paramètres de configuration d'agent, l'utilitaire de reconfiguration propose les valeurs actuellement configurées comme valeurs par défaut.

Procédure

Pour reconfigurer le collecteur de données en répondant aux invites, procédez comme suit :

1. Connectez-vous au système à l'aide de l'ID utilisateur utilisé pour installer le serveur d'applications.
2. Accédez au répertoire `bin` situé dans le répertoire de base du collecteur de données *base_cd*.
3. Démarrez l'utilitaire de reconfiguration à l'aide de la commande suivante :
   - Windows `reconfig.bat`
   - Linux AIX `./reconfig.sh`

   Conseil : L'exécution de cet utilitaire de reconfiguration a le même effet que l'exécution du script `config.bat` avec l'argument `-reconfig` sur les systèmes Windows, ou du script `config.sh` avec l'argument `-reconfig` sur les systèmes Linux ou AIX.

   L'utilitaire de reconfiguration affiche les adresses IP de toutes les cartes réseau qui sont détectées sur le système informatique local.
4. Entrez le nombre qui correspond à l'adresse IP à utiliser.

   L'utilitaire de reconfiguration recherche toutes les instances de serveur d'applications pour lesquelles le collecteur de données est configuré sur cet hôte et vous invite à sélectionner une ou plusieurs instances de serveur d'applications dans la liste.
5. Sélectionnez une ou plusieurs instances de serveur d'applications dans la liste. Entrez le nombre qui correspond à l'instance de serveur d'applications à reconfigurer pour la collecte de données ou entrez un astérisque (`*`) pour reconfigurer toutes les instances de serveur d'applications pour la collecte de données. Pour indiquer un sous-ensemble de serveurs, entrez les nombres, séparés par des virgules, qui représentent les serveurs. Par exemple : `1,2,3`.

   A faire :

- Pour un environnement autonome, les instances de serveur d'applications doivent s'exécuter pendant la configuration. (Une instance de WebSphere Application Server Liberty n'a pas besoin d'être en cours d'exécution).
- Pour un environnement de déploiement réseau, Deployment Manager doit être en cours d'exécution.
- Assurez-vous que les instances de serveur d'applications que vous sélectionnez sont les serveurs réels qui hébergent les applications ou les services que vous voulez surveiller.

6. Dans la section **Integration with Agent for WebSphere Applications**, indiquez si vous souhaitez intégrer le collecteur de données à l'Agent WebSphere Applications. Vous devez entrer 1 pour sélectionner cette option d'intégration, puis appuyer sur Entrée.
7. Si vous configurez le collecteur de données pour un serveur WebSphere Application Server traditionnel, indiquez si vous souhaitez configurer le collecteur de données dans l'instance de serveur d'applications.
   - Entrez 1 pour configurer le collecteur de données dans le serveur d'applications. Avec cette option, le collecteur de données est intégré au serveur d'applications, ce qui est nécessaire à la collecte complète des données de surveillance opérationnelle et de diagnostic. Cependant, la configuration du collecteur de données dans le serveur d'applications nécessite de redémarrer ce dernier. En outre, le collecteur de données peut affecter les performances de serveur.
   - Entrez 2 pour ne pas configurer le collecteur de données dans le serveur d'applications et passez à l'étape «9», à la page 870. Avec cette option, le collecteur de données s'exécute comme un processus autonome et seule la surveillance des ressources PMI peut être activée.
8. A l'invite, indiquez s'il faut activer ou non la collecte des données de diagnostic pour le collecteur de données. Entrez 1 pour oui ou 2 pour non.
9. Lorsque vous êtes invité à entrer le nom d'hôte, entrez le nom d'hôte ou l'adresse IP de l'Agent WebSphere Applications ou appuyez sur Entrée pour accepter la valeur par défaut. La valeur par défaut correspond au choix que vous avez effectué à l'étape «4», à la page 869.
10. Lorsque vous êtes invité à entrer le numéro de port, entrez le numéro de port de l'agent de surveillance ou appuyez sur Entrée pour accepter la valeur par défaut. La valeur par défaut est 63335.
11. Lorsque vous êtes invité à indiquer si l'agent de surveillance V6 pour WebSphere Applications doit être configuré, appuyez sur Entrée pour accepter la valeur par défaut No.

    L'agent de surveillance V6 fait référence à l'ITCAM Agent for WebSphere Applications, qui est installé dans l'ancienne infrastructure IBM® Tivoli® Monitoring. La configuration de l'agent de surveillance V6 n'est requise que pour l'environnement de coexistence des agents.
12. Lorsque vous êtes invité à entrer l'alias de serveur, appuyez sur Entrée pour accepter la valeur par défaut ou entrez un autre alias. Si vous configurez plusieurs instances de serveur d'applications, l'utilitaire de configuration vous invite à indiquer un alias pour chaque instance.

    Important : L'alias ne peut contenir que les caractères suivants : A-Z, a-z, soulignement (_), tiret (-) et point (.). N'utilisez pas d'autres caractères dans l'alias.

    L'alias de serveur est le premier qualificateur du nom d'instance d'agent (également appelé MSN) affiché sur la console Cloud APM. La valeur par défaut est le nom du noeud combiné au nom du serveur. Par exemple, l'alias **node1server1** indique le serveur **server1** dans le noeud **node1**.
13. Lorsque vous êtes invité à entrer un numéro de port pour la surveillance des ressources PMI, appuyez sur Entrée pour accepter la valeur par défaut ou entrez un nouveau numéro. La valeur par défaut est 63355.

    Ce port est utilisé pour la communication interne entre les composants qui s'exécutent sur le même hôte. Si le port par défaut est utilisé, vous pouvez définir un numéro différent.
14. Dans la section **Prise en charge du suivi des transactions**, indiquez si vous souhaitez activer le suivi des transactions. Entrez 1 pour activer la prise en charge du suivi des transactions. Autrement, entrez 2 et passez à l'étape «17», à la page 871.

15. Lorsque vous êtes invité à indiquer le nom d'hôte ou l'adresse IP de Transaction Framework Extension, appuyez sur Entrée pour accepter la valeur par défaut ou entrez un autre nom d'hôte ou une autre adresse IP.

    Transaction Framework Extension est un composant interne de l'Agent WebSphere Applications qui recueille des mesures à partir du collecteur de données.
16. Lorsque vous êtes invité à entrer le numéro de port que le collecteur de données utilise pour se connecter à Transaction Framework Extension, appuyez sur Entrée pour accepter la valeur par défaut ou entrez un autre numéro de port. La valeur par défaut est 5457.
17. Indiquez si vous voulez intégrer le collecteur de données à Application Performance Diagnostics Lite. Appuyez sur Entrée pour accepter la valeur par défaut pour Non.
18. Dans la section **Paramètres avancés**, indiquez si vous souhaitez modifier le chemin du journal de la récupération de place.

    Entrez 1 pour sélectionner un chemin d'accès au journal de récupération de place. Autrement, entrez 2 et passez à l'étape «20», à la page 871. Pour utiliser le chemin d'accès au journal déjà indiqué dans l'argument JVM du serveur d'applications, entrez 2.
19. Indiquez le chemin de la collecte de récupération de place. Entrez un nom de fichier avec son chemin d'accès complet. Pour WebSphere Application Server Liberty, n'utilisez pas de variables dans le chemin d'accès. Le collecteur de données modifie automatiquement le nom du fichier journal en y ajoutant des informations sur l'instance de serveur.

    Par exemple, si vous indiquez `gc.log` comme nom de fichier, le nom réel est défini sur *`nom_profil.nom-cellule.nom_noeud.nom_serveur`*`.gc.log` pour chaque instance de serveur d'applications configurée.

    Important : Dans le chemin d'accès au journal de récupération de place, vous pouvez utiliser des variables WebSphere, telles que `${SERVER_LOG_ROOT}`. Cependant, n'utilisez pas de modèles, tels que `%pid`.
20. Consultez le récapitulatif de la configuration du collecteur de données à appliquer aux instances de serveur d'applications définies. Reconfigurez les parties de la configuration du collecteur de données avant d'appliquer les modifications, si nécessaire.
21. Entrez a pour accepter vos modifications.
22. A l'invite, indiquez si vous souhaitez créer une copie de sauvegarde de votre configuration en cours. Entrez 1 pour créer une sauvegarde de la configuration en cours. Sinon, entrez 2.

    L'utilitaire de configuration applique les modifications et présente un message d'état pour indiquer que la configuration du collecteur de données pour le profil est terminée .
23. Si vous configurez le collecteur de données pour le serveur WebSphere Application Server traditionnel, redémarrez les instances de serveur d'applications ou redémarrez l'agent, selon l'option que vous avez choisie à l'étape «7», à la page 870.

    - Si vous avez activé le collecteur de données dans le serveur d'applications, redémarrez les instances de serveur d'applications, comme indiqué par l'utilitaire de configuration.
    - Si vous avez activé la surveillance des ressources PMI sans activer le collecteur de données dans le serveur d'applications, redémarrez l'Agent WebSphere Applications en exécutant les commandes suivantes :

      – Windows

      ```
      cd rép_install\bin
      was-agent.bat stop
      was-agent.bat start
      ```

      – Linux AIX

      ```
      cd rép_install/bin
      ./was-agent.sh stop
      ./was-agent.sh start
      ```

La configuration du collecteur de données entre en vigueur une fois que le serveur d'applications ou l'agent a redémarré.

Que faire ensuite

- La modification de l'alias de serveur entraîne la modification du nom d'instance de l'agent enregistré dans la console Cloud APM. Si vous avez modifié l'alias de serveur lors de la procédure de reconfiguration, vous devez effacer certains fichiers cache en effectuant les opérations suivantes :
  1. Arrêtez l'agent de surveillance s'il est en cours d'exécution.
  2. Ouvrez le fichier *nom_hôte*_yn.xml dans le répertoire suivant avec un éditeur de texte, où *nom_hôte* est le nom de l'hôte où l'Agent WebSphere Applications est installé.
     - Windows *rép_install*\TMAITM6_x64 (la valeur par défaut est C:\IBM\APM\TMAITM6_x64)
     - Linux AIX *rép_install*/config (la valeur par défaut est /opt/ibm/apm/agent/config)
  3. Recherchez la ligne qui commence par la chaîne suivante et qui contient le nom de serveur précédent. Par exemple, was85.win4net01Cell02.win4net01Node02.AppSrv01.server1, où server1 est le nom précédent du serveur d'applications.

     ```
     <!ENTITY code_produit_was.nom_cellule.nom_noeud.nom_profil.nom_serveur
     ```

     où *code_produit_was* est le code produit de WebSphere Application Server ; *nom_cellule* est le nom de la cellule ; *nom_noeud* est le nom du noeud ; *nom_profil* est le nom du profil de serveur d'applications ; *nom_serveur* est le nom précédent du serveur d'applications.
  4. Dans le répertoire en cours, recherchez le fichier .XML indiqué sur la ligne et supprimez-le.
  5. Supprimez la ligne que vous avez recherchée à l'étape 3 dans le fichier *nomhôte*_yn.xml.
  6. A la fin du fichier *nom_hôte*_yn.xml, supprimez la ligne qui contient les noms de serveur précédents.
  7. Sauvegardez et fermez le fichier.
  8. Redémarrez l'agent de surveillance.

Configuration du collecteur de données en mode silencieux

Si vous voulez configurer de nombreuses instances de serveur d'applications, il peut être plus pratique de configurer le collecteur de données en mode silencieux.

Pourquoi et quand exécuter cette tâche

Lorsque vous configurez le collecteur de données en mode silencieux, vous indiquez d'abord des options de configuration dans un fichier de propriétés. Un exemple de fichier de propriétés, sample_silent_config.txt, est fourni avec l'utilitaire de configuration. Le fichier est disponible dans les répertoires suivants, où *base_cd* est le répertoire dans lequel est installé le collecteur de données. Pour le chemin d'accès complet au répertoire *base_cd*, consultez l'introduction de Configuration du collecteur de données pour l'agent WebSphere Applications.

- Windows *base_cd*\bin
- Linux AIX *base_cd*/bin

Pour plus d'informations sur chaque propriété de configuration disponible dans ce fichier, voir «Fichier de propriétés pour la configuration en mode silencieux du collecteur de données», à la page 874.

Procédure

Exécutez les étapes suivantes pour effectuer une configuration en mode silencieux :

1. Spécifiez les options de configuration dans le fichier de propriétés. Vous pouvez copier l'exemple de fichier de propriétés et modifier les options obligatoires.
2. Définissez l'emplacement du répertoire de base Java avant d'exécuter l'utilitaire.

Exemple :

- Windows

```
set JAVA_HOME=C:\Program Files\IBM\WebSphere\AppServer80\java
```

- Linux AIX

```
export JAVA_HOME=/opt/IBM/AppServer80/java
```

Important : Si vous configurez la surveillance pour WebSphere Application Server Liberty, vous devez utiliser la même version de machine JVM que celle utilisée pour le serveur d'applications. Autrement, la surveillance peut échouer.

3. Accédez au répertoire suivant :
   - Windows *base_cd*\bin
   - Linux AIX *base_cd*/bin
4. Exécutez la commande pour configurer le collecteur de donnés en mode silencieux.
   - Windows Exécutez la commande suivante comme administrateur ayant installé WebSphere Application Server.

     ```
     config.bat -silent [dir_path]\silent file
     ```

   - Linux AIX Exécutez la commande suivante avec les privilèges de superutilisateur.

     ```
     config.sh -silent [dir_path]/silent file
     ```

   Conseil : Si l'utilisateur `wsadmin` a été utilisé pour installer le serveur d'applications, exécutez l'utilitaire `config` en tant qu'utilisateur `wsadmin` ou avec les privilèges de superutilisateur.
5. Après avoir configuré le collecteur de données pour surveiller des instances de serveur d'applications, si vous avez activé le collecteur de données dans le serveur d'applications, vous devez redémarrer les instances. La configuration du collecteur de données entre en vigueur une fois que les instances de serveur d'applications ont redémarré.
6. Si vous avez activé la surveillance des ressources PMI sans avoir activé le collecteur de données dans le serveur d'applications, il se peut que vous deviez redémarrer l'Agent WebSphere Applications pour démarrer la surveillance. Si les données de surveillance ne sont pas disponibles immédiatement, redémarrez l'agent de surveillance en exécutant les commandes suivantes :
   - Windows

     ```
     cd rép_install\bin
     was-agent.bat stop
     was-agent.bat start
     ```

   - Linux AIX

     ```
     cd rép_install/bin
     ./was-agent.sh stop
     ./was-agent.sh start
     ```

Que faire ensuite

Après une configuration en mode silencieux, pour modifier la configuration du collecteur de données, vous avez deux options :

- Reconfigurez-le de façon interactive à l'aide de l'utilitaire de reconfiguration **reconfig**. Pour obtenir des instructions, voir «Reconfiguration du collecteur de données en mode interactif», à la page 869.
- Annulez la configuration en mode silencieux, puis utilisez la même procédure pour la configurer de nouveau en mode silencieux. Pour obtenir des instructions, voir «Annulation de la configuration du collecteur de données en mode silencieux», à la page 154.

Référence associée

«Fichier de propriétés pour la configuration en mode silencieux du collecteur de données», à la page 874

Pour configurer le collecteur de données en mode silencieux, vous indiquez des options de configuration dans un fichier de propriétés, puis vous exécutez l'utilitaire de configuration.

Fichier de propriétés pour la configuration en mode silencieux du collecteur de données

Pour configurer le collecteur de données en mode silencieux, vous indiquez des options de configuration dans un fichier de propriétés, puis vous exécutez l'utilitaire de configuration.

Lorsque vous créez votre fichier de propriétés, tenez compte des remarques suivantes :

- Une ligne du fichier qui commence par un signe dièse (#) est considérée comme un commentaire et n'est pas traitée. Si le signe dièse est utilisé ailleurs dans la ligne, on ne le considère pas comme le début d'un commentaire.
- Chaque propriété est décrite sur une ligne distincte, dans le format suivant : *property* = *value*.

  property
  Nom de la propriété. La liste de propriétés valides que vous pouvez configurer est affichée dans le Tableau 223, à la page 874.

  value
  Valeur de la propriété. Des valeurs par défaut pour certaines propriétés sont déjà fournies. Vous pouvez supprimer des valeurs par défaut pour laisser des valeurs de propriété en blanc. Une valeur vide est traitée comme si la propriété n'était pas indiquée, par opposition à l'utilisation de la valeur par défaut. Si vous voulez utiliser des valeurs par défaut, vous pouvez mettre en commentaire la propriété dans le fichier.
- Les mots de passe sont en texte en clair.
- Les propriétés et leurs valeurs distinguent les majuscules et minuscules.

Le Tableau 223, à la page 874 décrit les propriétés qui sont disponibles lors de la configuration du collecteur de données en mode silencieux.

Important : Si vous configurez le collecteur de données pour une instance de WebSphere Application Server Liberty, certaines des propriétés ne sont pas utilisées.

Tableau 223. Propriétés disponibles pour exécuter l'utilitaire de configuration en mode silencieux

Propriété	**Commentaire**
default.hostip	Si le système informatique utilise plusieurs adresses IP, indiquez l'adresse IP que le collecteur de données doit utiliser.
Intégration du collecteur de données au serveur de gestion d'ITCAM for Application Diagnostics **Important :** Le serveur de gestion est uniquement disponible si vous avez ITCAM for Application Diagnostics. Pour une instance WebSphere Application Server Liberty ou dans un environnement Cloud APM, ces propriétés ne sont pas utilisées.	
ms.connect	Indique si le collecteur de données est configuré pour se connecter au serveur de gestion dans un environnement ITCAM for Application Diagnostics. Les valeurs valides sont `True` et `False`.
ms.kernel.host	Indique le nom de système hôte qualifié complet du serveur de gestion.
ms.kernel.codebase.port	Indique le port de codebase sur lequel le serveur de gestion est en mode écoute.
ms.am.home	Indique le répertoire de base du serveur de gestion.

Tableau 223. Propriétés disponibles pour exécuter l'utilitaire de configuration en mode silencieux (suite)

Propriété	Commentaire
ms.am.socket.bindip	Indique l'adresse IP ou le nom d'hôte que le collecteur de données doit utiliser pour communiquer avec le serveur de gestion. Si plus d'une interface réseau ou adresse IP est configurée sur le système informatique du collecteur de données, sélectionnez l'une d'entre elles.
ms.probe.controller.rmi.port	Si le collecteur de données est derrière un pare-feu ou si vous avez des exigences particulières de modification du port RMI de contrôleur du collecteur de données, définissez cette plage de numéros de port. Configurez ce numéro de port comme autorisé par le pare-feu pour l'hôte du collecteur de données. Par exemple : `ms.probe.controller.rmi.port=8300-8399` ou ms.probe.controller.rmi.port=8300.
ms.probe.rmi.port	Si le collecteur de données est derrière un pare-feu ou si vous avez des exigences particulières de modification du port RMI du collecteur de données, définissez cette plage de numéros de port. Configurez ce numéro de port comme autorisé par le pare-feu pour l'hôte du collecteur de données. Par exemple : `ms.probe.rmi.port=8200-8299` ou `ms.probe.rmi.port=8200`.
Prise en charge du suivi des transactions Pour visualiser les informations de suivi des transactions, vous devez avoir des vues de topologie disponibles dans la console Cloud APM et activer le suivi des transactions dans la fenêtre de configuration d'agent.	
ttapi.enable	Indique si le collecteur de données prend en charge le suivi des transactions. Les valeurs valides sont `True` et `False`.
ttapi.host	Indique l'hôte de Transaction Framework Extension, qui est le composant de Monitoring Agent for WebSphere Applications qui regroupe les mesures provenant du collecteur de données. Utilisez la valeur de l'hôte local, `127.0.0.1`.
ttapi.port	Indique le port de Transaction Framework Extension. Utilisez 5457.
Intégration du collecteur de données à ITCAM for SOA **Important :** Pour une instance WebSphere Application Server Liberty ou dans un environnement Cloud APM, cette propriété n'est pas utilisée.	
soa.enable	Indique si vous souhaitez intégrer le collecteur de données à ITCAM for SOA. L'agent ITCAM for SOA doit être installé pour que vous puissiez terminer la configuration.
Intégration du collecteur de données à Tivoli Performance Monitoring **Important :** Pour une instance WebSphere Application Server Liberty ou dans un environnement Cloud APM, cette propriété n'est pas utilisée.	
tpv.enable	Indique si vous souhaitez intégrer le collecteur de données à Tivoli Performance Monitoring lorsque le collecteur de données est inclus en tant qu'élément d'ITCAM for WebSphere Application Server version 8.5. Tivoli Performance Monitoring est accessible depuis la console d'administration de WebSphere Application Server. Les valeurs valides sont *True* et *False*.
Intégration du collecteur de données à Application Performance Diagnostics Lite **Important :** Pour une instance WebSphere Application Server Liberty, cette propriété n'est pas utilisée.	

Tableau 223. Propriétés disponibles pour exécuter l'utilitaire de configuration en mode silencieux (suite)

Propriété	Commentaire
de.enable	Indique s'il y a lieu de collecter des données de diagnostic qui sont requises pour Application Performance Diagnostics et Application Performance Diagnostics Lite. Les valeurs valides sont `True` et `False`. Activez cette intégration si vous disposez du produit Application Diagnostics ou si vous souhaitez l'acquérir ultérieurement. Dans ce cas, la collecte des données de diagnostic est activée au démarrage du serveur. Sinon, elle est désactivée au démarrage ; vous pouvez alors l'activer à l'aide de la page Configuration d'agent de l'interface utilisateur. Toutefois, si le serveur est redémarré, la collecte des données de diagnostic sera à nouveau désactivée. Ce paramètre active également l'intégration à Application Performance Diagnostics Lite, un outil conçu pour l'étude de diagnostic des applications exécutées sur WebSphere Application Server et WebSphere Portal Server. A l'aide de cet outil, vous pouvez analyser des données en temps réel ou vous pouvez sauvegarder les informations de diagnostic dans un fichier à des fins d'analyse ultérieure.
Surveillance des ressources PMI et du collecteur de données Le serveur sélectionné est toujours configuré pour la surveillance des ressources (PMI), sans aucun changement apporté au serveur d'applications. Cette option de surveillance fournit des métriques et des travaux limités seulement avec Agent WebSphere Applications, mais ne nécessite pas une relance du serveur d'application et ne peut pas affecter la performance.	
tema.appserver	Indique si vous souhaitez configurer le collecteur de données dans l'instance de serveur d'applications. Le collecteur de données de l'instance de serveur d'application est nécessaire pour obtenir l'éventail complet de mesures dans l'Agent WebSphere Applications et pour l'intégration à tous les autres produits. Cependant, la configuration du collecteur de données nécessite le redémarrage du serveur d'applications. En outre, le collecteur de données peut affecter les performances de serveur. Les valeurs valides sont `True` et `False`. Si ce paramètre a pour valeur `False`, les paramètres de configuration du collecteur de données pour une intégration à des produits autres que l'Agent WebSphere Applications ne sont pas pris en compte. Lorsque ce paramètre est défini sur `False`, les fonctions de diagnostic et de suivi des transactions sont indisponibles, et seules les données de surveillance des ressources sont collectées.
tema.jmxport	Le numéro du port TCP/IP pour la surveillance des ressources. Le port est utilisé pour la communication interne entre les composants qui s'exécutent sur le même hôte. Le port de défaut est 63355 ; si ce port est utilisé, vous pouvez définir un numéro différent.
Intégration du collecteur de données à l'Agent WebSphere Applications et Application Performance Diagnostics Lite	
temaconnect	Indique si le collecteur de données se connecte au composant agent de surveillance de l'Agent WebSphere Applications. Les valeurs valides sont `True` et `False`. **Important :** Vous devez utiliser la valeur `True` pour utiliser l'Agent WebSphere Applications.

Tableau 223. Propriétés disponibles pour exécuter l'utilitaire de configuration en mode silencieux (suite)

Propriété	Commentaire
tema.appserver	Indique si vous souhaitez configurer le collecteur de données dans l'instance de serveur d'applications. Le collecteur de données de l'instance de serveur d'application est nécessaire pour obtenir l'éventail complet de mesures dans l'Agent WebSphere Applications et pour l'intégration à tous les autres produits. Elle nécessite le redémarrage du serveur d'applications. En outre, le collecteur de données peut affecter les performances de serveur. Les valeurs valides sont `True` et `False`. Si ce paramètre est associé à la valeur `False`, les paramètres de configuration pour l'intégration du collecteur de données à des produits autres que l'Agent WebSphere Applications ne sont pas pris en compte, de même que les paramètres tema.host et tema.port suivants. Lorsque ce paramètre est défini sur `False`, les fonctions de diagnostic et de suivi des transactions sont indisponibles, et seules les données de surveillance des ressources sont collectées.
tema.host	Indique le nom d'hôte complet ou l'adresse IP du composant agent de surveillance de l'Agent WebSphere Applications. Utilisez l'adresse de l'hôte local (127.0.0.1).
tema.port	Indiquez le numéro de port du composant agent de surveillance de l'Agent WebSphere Applications. Ne modifiez pas la valeur par défaut 63335.
tema.jmxport	Le numéro du port TCP/IP pour la surveillance des ressources. Le port est utilisé pour la communication interne entre les composants qui s'exécutent sur le même hôte. Le port de défaut est 63355 ; si ce port est utilisé, vous pouvez définir un numéro différent.
Intégration du collecteur de données à ITCAM Agent for WebSphere Applications version 6 Utilisez les propriétés suivantes pour demander à un collecteur de données de collecter des données pour l'Agent WebSphere Applications et l'ITCAM Agent for WebSphere Applications version 6.	
config.tema.v6	Indique si le collecteur de données doit être intégré au composant agent de surveillance de l'ITCAM Agent for WebSphere Applications version 6. Les valeurs admises sont `True` et `False`. La valeur par défaut est `False`.
tema.host.v6	Indique si le collecteur de données doit être intégré au composant agent de surveillance de l'ITCAM Agent for WebSphere Applications version 6. Les valeurs admises sont `True` et `False`. La valeur par défaut est `False`.
tema.port.v6	Indique le numéro de port du composant agent de surveillance de l'ITCAM Agent for WebSphere Applications version 6. Ne modifiez pas la valeur par défaut 63336.
Copie de sauvegarde de WebSphere Application Server	
was.backup.configuration	Indique si la configuration en cours de WebSphere Application Server doit être sauvegardée avant que la nouvelle configuration soit appliquée. Les valeurs valides sont `True` et `False`.
was.backup.configuration.dir	Indique l'emplacement du répertoire de sauvegarde.
Paramètres de configuration avancés	
was.gc.custom.path	Indique si vous devez définir un chemin d'accès personnalisé pour le journal de récupération de place.

Tableau 223. Propriétés disponibles pour exécuter l'utilitaire de configuration en mode silencieux (suite)

Propriété	Commentaire
was.gc.file	Indique le chemin d'accès au journal de récupération de place personnalisé. Définissez cette valeur sur un nom de fichier avec son chemin d'accès complet. Le collecteur de données modifie automatiquement le nom du fichier journal en y ajoutant des informations sur l'instance de serveur. Par exemple, si vous indiquez `gc.log` comme nom de fichier, le nom réel est défini sur *`nom_profil.nom-cellule.nom_noeud.nom_serveur`*`.gc.log` pour chaque instance de serveur d'applications configurée. **Important :** Dans le chemin d'accès au journal de récupération de place, vous pouvez utiliser des variables WebSphere, telles que `${SERVER_LOG_ROOT}`. Cependant, n'utilisez pas de modèles, tels que %pid.
Paramètres de connexion de WebSphere Administrative Services	
was.wsadmin.connection.host	Indique le nom de l'hôte auquel l'outil wsadmin se connecte. Dans un environnement Network Deployment, spécifiez la connexion wsadmin au gestionnaire de déploiement. Dans un environnement autonome, indiquez la connexion wsadmin au serveur. **A faire :** Si la console d'administration WebSphere est sur le même système, la valeur de `localhost` est utilisée pour la connexion. Toutefois, dans certains cas, `localhost` n'est pas autorisé pour la communication en raison des paramètres de sécurité ou du réseau système. Dans ce cas, vous devez spécifier ce paramètre dans le fichier de réponses silencieux.
was.wsadmin.connection.type	Indique le port que l'outil wsadmin doit utiliser pour se connecter à WebSphere Application Server.
was.wsadmin.connection.port	Indique le port que l'outil wsadmin doit utiliser pour se connecter à WebSphere Application Server.
Paramètres de sécurité globale de WebSphere Application Server	
was.wsadmin.username	Spécifie l'ID utilisateur d'un utilisateur autorisé à se connecter à la console d'administration d'IBM WebSphere Application Server. Cet utilisateur doit posséder le rôle d'agent sur le serveur d'applications.
was.wsadmin.password	Indique le mot de passe qui correspond à l'utilisateur indiqué dans la propriété `was.wsadmin.username`.
was.client.props	Indique si les paramètres de sécurité doivent être extraits à partir d'un fichier de propriétés de client. Les valeurs valides sont `True` et `False`.
Paramètres WebSphere Application Server	
was.appserver.profile.name	Indique le nom du profil de serveur d'applications que vous voulez configurer. Pas utilisé pour WebSphere Application Server Liberty.
was.appserver.home	Indique le répertoire de base de WebSphere Application Server.
was.appserver.cell.name	Indique le nom de cellule de WebSphere Application Server. Pas utilisé pour WebSphere Application Server Liberty.
was.appserver.node.name	Indique le nom de noeud de WebSphere Application Server. Pas utilisé pour WebSphere Application Server Liberty.
Paramètres d'instance d'exécution de WebSphere Application Server	

Tableau 223. Propriétés disponibles pour exécuter l'utilitaire de configuration en mode silencieux (suite)	
Propriété	**Commentaire**
was.appserver.server.name	Indique l'instance du serveur d'applications dans le profil de serveur d'applications à configurer. **Conseil :** • Le fichier de réponses silencieux peut avoir plusieurs instances de cette propriété • Lors de l'ajout d'un deuxième serveur, supprimez la mise en commentaire de ce dernier (#[SERVER]) et ajoutez le nom du serveur.
tema.serveralias	Spécifie le nom du noeud dans l'interface utilisateur de surveillance qui contient les informations de surveillance pour cette instance du serveur d'applications. La valeur par défaut est le nom du noeud combiné au nom du serveur. **Important :** L'alias ne peut contenir que les caractères suivants : A-Z, a-z, soulignement (_), tiret (-) et point (.). N'utilisez pas d'autres caractères dans l'alias. **Conseil :** Le fichier de réponses silencieux peut avoir plusieurs instances de cette propriété. **A faire :** La modification de l'alias de serveur entraîne la modification du nom d'instance de l'agent enregistré dans la console Cloud APM. Si ce n'est pas la première fois que vous configurez le collecteur de données et que vous avez modifié l'alias de serveur, vous devez effacer certains fichiers cache. Pour plus d'instructions, voir la rubrique décrivant l'effacement des fichiers cache portant des anciens noms de serveur.

Configuration manuelle du collecteur de données si les utilitaires de configuration échouent
Si vous ne pouvez pas utiliser l'utilitaire de configuration fourni pour configurer le collecteur de données pour l'Agent WebSphere Applications, vous pouvez configurer manuellement le collecteur de données dans la console d'administration WebSphere.

Avant de commencer

- Installez l'Agent WebSphere Applications.
- Prenez connaissance du répertoire de base du collecteur de données, requis par la configuration du collecteur de données. Le répertoire par défaut est `/opt/ibm/apm/agent/yndchome/7.3.0.14.08` sur les systèmes Linux et UNIX ou `C:\IBM\APM\dchome\7.3.0.14.08` sur les systèmes Windows.
- Si vous souhaitez configurer le collecteur de données pour un serveur Liberty, prenez connaissance du répertoire de base du serveur Liberty. Par exemple, `/opt/ibm/was/liberty/usr/servers/defaultServer`.
- Assurez-vous qu'un fichier nommé `itcam_wsBundleMetaData.xml` existe dans le dossier *dc_home*`/runtime/wsBundleMetaData` et qu'il contient le contenu suivant. Si le dossier ou le fichier n'existe pas, créez-le manuellement.

  A faire : La valeur *plugins_dir_within_dc_home* doit être définie par le chemin absolu du dossier `plugins` dans le répertoire de base du collecteur de données. La valeur par défaut est `/opt/ibm/apm/agent/yndchome/7.3.0.14.08/plugins` sur les systèmes Linux et UNIX ou `C:\IBM\APM\dchome\7.3.0.14.08\plugins` sur les systèmes Windows.

```
<bundles>
  <directory path="plugins_dir_within_dc_home">
      <bundle>com.ibm.tivoli.itcam.bundlemanager_7.2.0.jar</bundle>
  </directory>
  <directory path="rép_plugins_dans_rép_principal_dc">
      <bundle>com.ibm.tivoli.itcam.classicsca_7.2.0.jar</bundle>
```

```
  </directory>
  <directory path="rép_plugins_dans_rép_principal_dc">
      <bundle>com.ibm.tivoli.itcam.toolkitsca.classicsca_7.2.0.jar</bundle>
  </directory>
</bundles>
```

Pourquoi et quand exécuter cette tâche

Important :

- Vous devez apporter des modifications manuelles à la configuration WebSphere Application Server pour les collecteurs de données en tant qu'administrateur WebSphere.
- Vous devez être un administrateur WebSphere expérimenté pour apporter des modifications manuelles à WebSphere Application Server en vue de la collecte de données. Toute erreur dans la modification manuelle de la configuration peut empêcher le démarrage du serveur d'applications.
- Après avoir configuré manuellement le collecteur de données pour surveiller les instances de serveur d'application, vous ne pouvez pas employer l'utilitaire d'annulation de configuration pour déconfigurer le collecteur de données. Vous devez à la place annuler manuellement la configuration du collecteur de données.

Procédure

- Pour configurer manuellement le collecteur de données pour WebSphere Application Server, voir «Configuration manuelle du collecteur de données pour WebSphere Application Server traditionnel», à la page 880.
- Pour configurer manuellement le collecteur de données pour le serveur Liberty, voir «Configuration manuelle du collecteur de données pour WebSphere Application Server Liberty», à la page 882.

Configuration manuelle du collecteur de données pour WebSphere Application Server traditionnel

Procédure

1. Connectez-vous à la console d'administration WebSphere en tant qu'administrateur.
2. Dans le panneau de navigation, cliquez sur **Servers**, développez **Server Types** et cliquez sur **WebSphere application servers**.
3. Dans la section **Server Infrastructure** de l'onglet Configuration, développez **Gestion des processus et Java** et cliquez sur **Process Definition**.
4. Dans la section **Propriétés supplémentaires**, cliquez sur **Machine virtuelle Java**.
5. Dans la zone **Arguments JVM génériques**, ajoutez les entrées suivantes :

   ```
   -agentlib:am_ibm_16=${WAS_SERVER_NAME} -Xbootclasspath/p:${ITCAMDCHOME}/
   toolkit/lib/bcm-bootstrap.jar -Djava.security.policy=${ITCAMDCHOME}/itcamdc/
   etc/datacollector.policy -verbosegc
   ```

   Lors de l'ajout de ces entrées, notez ce qui suit :

   - Toutes les entrées doivent se trouver sur une seule ligne.
   - Séparez les différents arguments par des espaces avant le signe moins (-). N'utilisez pas d'espaces ailleurs.
6. Cliquez sur **Apply**, puis enregistrez les changements apportés à la configuration principale.
   - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
   - Si vous êtes dans un environnement de déploiement réseau, vérifiez que **Synchroniser les modifications avec les noeuds** est sélectionné dans les **options de préférence de la console**, puis cliquez sur **Sauvegarder**.
7. Dans le panneau de navigation, cliquez sur **Servers**, développez **Server Types**, cliquez sur **WebSphere application servers**, puis cliquez sur le nom du serveur.

8. Dans l'onglet Configuration, accédez à **Infrastructure du serveur** > **Gestion des processus et Java** > **Définition des processus** > **Entrées d'environnement**.
9. Selon le système d'exploitation, la plateforme matérielle et la machine virtuelle Java de serveur d'applications utilisés, définissez l'entrée d'environnement suivante.

Tableau 224. Entrée d'environnement

Plateforme	Nom de l'entrée d'environnement	Valeur de l'entrée d'environnement
AIX R6.1 (machine virtuelle Java 64 bits)	LIBPATH	`/lib:${ITCAMDCHOME}/toolkit/lib/aix536`
AIX R7.1 (machine virtuelle Java 64 bits)	LIBPATH	`/lib:${ITCAMDCHOME}/toolkit/lib/aix536`
Solaris 10 (machine virtuelle Java 64 bits)	LIBPATH	`/lib:${ITCAMDCHOME}/toolkit/lib/sol296`
Solaris 11 (machine virtuelle Java 64 bits)	LIBPATH	`/lib:${ITCAMDCHOME}/toolkit/lib/sol296`
Linux Intel R2.6 (machine virtuelle Java 32 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/li6263`
Linux x86_64 R2.6 (machine virtuelle Java 64 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/lx8266`
Linux on Power Little Endian (machine virtuelle Java 64 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/lpl266`
Linux on System z (machine virtuelle Java 32 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/ls3263`
Linux on System z (machine virtuelle Java 64 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/ls3266`
Windows (machine virtuelle Java 32 bits)	PATH	`/lib;${ITCAMDCHOME}/toolkit/lib/win32`
Windows (machine virtuelle Java 64 bits)	PATH	`/lib;${ITCAMDCHOME}/toolkit/lib/win64`

10. Cliquez sur **Apply**, puis sauvegardez les changements apportés à la configuration principale.
    - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que **Synchroniser les modifications avec les noeuds** est sélectionné dans les **options de préférence de la console**, puis cliquez sur **Sauvegarder**.
11. Dans le panneau de navigation, cliquez sur **Environnement** > **Variables WebSphere**.
12. Définissez la portée sur un niveau serveur approprié et ajoutez la variable *ITCAMDCHOME*. Définissez la valeur de la variable *ITCAMDCHOME* sur le répertoire de base du collecteur de données. Par exemple, `/opt/ibm/apm/agent/yndchome/7.3.0.14.08`.
13. Cliquez sur **Apply**, puis enregistrez les changements apportés à la configuration principale.
    - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que **Synchroniser les modifications avec les noeuds** est sélectionné dans les **options de préférence de la console**, puis cliquez sur **Sauvegarder**.
14. Redémarrez le serveur d'applications.

Résultats

Vous pouvez à présent vérifier les données de l'Agent WebSphere Applications dans la console Cloud APM après avoir ajouté ce composant d'application à vos applications. Pour obtenir des instructions de démarrage de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003. Pour obtenir des instructions sur l'ajout ou l'édition d'une application, voir «Gestion des applications», à la page 1129.

Que faire ensuite

Après avoir configuré manuellement le collecteur de données, vous ne pouvez pas utiliser l'utilitaire `unconfig` fourni pour annuler la configuration du collecteur de données. Annulez plutôt la configuration du collecteur de données manuellement. Pour obtenir des instructions, voir «Annulation manuelle de la configuration du collecteur de données», à la page 158.

Configuration manuelle du collecteur de données pour WebSphere Application Server Liberty

Procédure

1. Accédez au répertoire de base du serveur Liberty. Par exemple, `/opt/ibm/wlp/usr/servers/defaultServer`.
2. Editez le fichier `jvm.options` en ajoutant les paramètres suivants, *base_cd* correspondant au répertoire de base du collecteur de données et *nom_serveur*, au nom du serveur Liberty. Si le fichier `jvm.options` n'existe pas, créez-le avec un éditeur de texte.

   ```
   -agentlib:am_ibm_16=nom_serveur
   –Xbootclasspath/p:base_cd/toolkit/lib/bcm-bootstrap.jar
   -Djava.security.policy=base_cd/itcamdc/etc/datacollector.policy
   -verbosegc
   ```

   Lors de l'ajout de ces entrées, notez ce qui suit :

   - Chaque entrée doit se trouver sur une ligne distincte.
   - Remplacez *nom_serveur* par le nom réel du serveur Liberty. Par exemple, `defaultServer`.
   - Remplacez *base_cd* par le répertoire de base réel du collecteur de données. Par exemple, `/opt/ibm/apm/agent/yndchome/7.3.0.14.08`.
3. Ouvrez le fichier `server.env` dans le même répertoire et ajoutez le chemin suivant à l'entrée d'environnement en fonction du système d'exploitation, où *base_cd* correspond au répertoire de base du collecteur de données. Si le fichier `server.env` n'existe pas, créez-le avec un éditeur de texte.

Tableau 225. Entrée d'environnement

Plateforme	Nom de l'entrée d'environnement	Valeur de l'entrée d'environnement
AIX R6.1 (machine virtuelle Java 64 bits)	LIBPATH	`/lib:base_cd/toolkit/lib/aix536`
AIX R7.1 (machine virtuelle Java 64 bits)	LIBPATH	`/lib:base_cd/toolkit/lib/aix536`
Solaris 10 (machine virtuelle Java 64 bits)	LIBPATH	`/lib:base_cd/toolkit/lib/sol296`
Solaris 11 (machine virtuelle Java 64 bits)	LIBPATH	`/lib:base_cd/toolkit/lib/sol296`
Linux x86_64 R2.6 (machine virtuelle Java 64 bits)	LD_LIBRARY_PATH	`/lib:base_cd/toolkit/lib/lx8266`
Linux Intel R2.6 (machine virtuelle Java 32 bits)	LD_LIBRARY_PATH	`/lib:base_cd/toolkit/lib/li6263`

Tableau 225. Entrée d'environnement (suite)		
Plateforme	**Nom de l'entrée d'environnement**	**Valeur de l'entrée d'environnement**
Windows (machine virtuelle Java 32 bits)	PATH	`/lib;`*`base_cd`*`/toolkit/lib/win32`
Windows (machine virtuelle Java 64 bits)	PATH	`/lib;`*`base_cd`*`/toolkit/lib/win64`

4. Ouvrez le fichier `server.xml` dans le même répertoire et ajoutez les lignes suivantes pour activer la fonction de surveillance :

```
<featureManager>
              <feature>webProfile-7.0</feature>
              <feature>monitor-1.0</feature>
              <feature>usr:itcam-730.140</feature>
   </featureManager>
```

5. Redémarrez le serveur Liberty.

Résultats

Vous pouvez à présent vérifier les données de l'Agent WebSphere Applications dans la console Cloud APM après avoir ajouté ce composant d'application à vos applications. Pour obtenir des instructions de démarrage de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003. Pour obtenir des instructions sur l'ajout ou l'édition d'une application, voir «Gestion des applications», à la page 1129.

Que faire ensuite

Après avoir configuré manuellement le collecteur de données, vous ne pouvez pas utiliser l'utilitaire `unconfig` fourni pour annuler la configuration du collecteur de données. Annulez plutôt la configuration du collecteur de données manuellement. Pour obtenir des instructions, voir «Annulation manuelle de la configuration du collecteur de données», à la page 158.

(Coexistence d'agent) Configuration de l'Agent WebSphere Applications et du collecteur de données

Dans l'environnement de coexistence d'agent où l'Agent WebSphere Applications et l'ITCAM Agent for WebSphere Applications sont installés, vous devez effectuer certaines étapes de configuration supplémentaires pour l'agent et procéder différemment pour configurer le collecteur de données.

Pourquoi et quand exécuter cette tâche

Dans l'environnement de coexistence d'agent, vous ne configurez qu'un seul collecteur de données pour envoyer les données à l'Agent WebSphere Applications et à l'ITCAM Agent for WebSphere Applications. Les deux agents doivent utiliser des ports différents pour écouter les demandes du collecteur de données.

Procédure

1. Si le collecteur de données de l'ITCAM Agent for WebSphere Applications, installé dans l'ancienne infrastructure IBM® Tivoli® Monitoring, est déjà présent dans votre environnement, désinstallez-le.
2. Installez l'Agent WebSphere Applications fourni dans IBM Cloud Application Performance Management 8.1.3 ou version ultérieure. Cela vous assure que la version 7.3.0.11.0 ou ultérieure du collecteur de données, qui est prise en charge pour la coexistence d'agent, est installée.
3. Assurez-vous que l'ID utilisateur employé pour configurer le collecteur de données et l'ID utilisateur employé pour installer le serveur d'applications disposent des droits d'utilisateur requis par l'agent. Pour obtenir des instructions, voir «Vérification des exigences d'accès utilisateur», à la page 860.
4. Assurez-vous que l'Agent WebSphere Applications et l'ITCAM Agent for WebSphere Applications utilisent des numéros de port différents pour écouter les demandes du collecteur de données. Les

numéros de port doivent être uniques de façon à ne pas pouvoir être utilisés par aucun autre composant de votre environnement. Configurez à nouveau l'agent pour modifier le port, si nécessaire.

- Pour plus d'informations sur la configuration de l'Agent WebSphere Applications, voir «Configuration de l'Agent WebSphere Applications», à la page 884.
- Pour plus d'informations sur la configuration de l'ITCAM Agent for WebSphere Applications, consultez la documentation d'ITCAM for Application Diagnostics ou d'ITCAM for Applications.

5. Utilisez l'utilitaire de configuration fourni pour configurer le collecteur de données. Pour plus d'informations, voir «Configuration du collecteur de données pour l'environnement de coexistence d'agent», à la page 886.

   Conseil : Si vous maîtrisez la configuration du collecteur de données, vous pouvez également configurer le collecteur de données en mode silencieux. Pour obtenir des instructions, voir «Configuration du collecteur de données en mode silencieux», à la page 872.

Configuration de l'Agent WebSphere Applications

Dans l'environnement de coexistence d'agent, le collecteur de données est partagé par l'Agent WebSphere Applications et l'ITCAM Agent for WebSphere Applications. Les deux agents doivent utiliser des ports différents pour écouter les demandes du collecteur de données. Vous devez configurer l'agent pour modifier le port, si nécessaire.

Pourquoi et quand exécuter cette tâche

- Sur les systèmes Linux ou AIX, vous pouvez configurer l'agent en mode interactif en exécutant le script de configuration, puis en répondant à des invites, ou en créant un fichier de réponses en mode silencieux et en exécutant le script de configuration sans interaction.
- Sur les systèmes Windows, vous pouvez configurer l'agent en créant le fichier de réponses silencieux et en exécutant le script de configuration, ou en lançant l'utilitaire Manage Monitoring Services. Pour plus d'informations sur Manage Monitoring Services sur des systèmes Windows, voir «Utilisation de la fenêtre IBM Cloud Application Performance Management sur les systèmes Windows», à la page 186.

Procédure

- Pour configurer l'agent en éditant le fichier de réponses silencieux et en exécutant le script sans intervenir, procédez comme suit :

  a) Créez un fichier `.txt` en tant que fichier de réponses silencieux.

  b) Indiquez les paramètres suivants dans le fichier de réponses silencieux. La syntaxe est *`nom_paramètre=valeur_paramètre`*.

  configure_type
  Indique le type de configuration. Ce paramètre est obligatoire.

  La valeur admise est `tema_configure` pour la configuration d'agent.

  KYN_ALT_NODEID
  Indique l'ID de noeud alternatif pour identifier l'agent. Ce paramètre est obligatoire.

  La valeur admise est une chaîne alphanumérique pouvant inclure jusqu'à 24 caractères.

  KYN_PORT
  Indique le port d'écoute utilisé par l'agent. Il s'agit de la connexion socket TCP que l'agent utilise pour écouter les demandes de connexion du collecteur de données. Ce paramètre est obligatoire.

  La valeur par défaut est 63335.

  A faire : Dans un environnement de coexistence d'agent, vérifiez que le numéro de port indiqué n'est pas utilisé par l'ITCAM Agent for WebSphere Applications.

Par exemple, ajoutez les lignes suivantes dans le fichier `.txt` que vous avez créé.

```
configure_type=tema_configure
KYN_ALT_NODEID=WASAgent
KYN_PORT=63335
```

c) Sauvegardez et fermez le fichier, puis entrez la commande suivante pour exécuter le script de configuration :

- Linux AIX *rép_install*/bin/was-agent.sh config *chemin_fichier_réponses*
- Windows *rép_install*\bin\was-agent.bat config *chemin_fichier_réponses*

où *rép_install* est le répertoire d'installation de l'agent. La valeur par défaut est `C:\IBM\APM` sur les systèmes Windows et `/opt/ibm/apm/agent` sur les systèmes Linux et AIX.

d) A l'issue de la configuration, redémarrez l'Agent WebSphere Applications s'il n'est pas encore en cours d'exécution à l'aide de la commande suivante :

- Linux AIX *rép_install*/bin/was-agent.sh start
- Windows *rép_install*\bin\was-agent.bat start

- Pour configurer l'agent en exécutant le script et en répondant aux invites, procédez comme suit :

a) A partir de la ligne de commande, accédez au répertoire *rép_install*/bin, où *rép_install* est le répertoire d'installation de l'agent.

La valeur par défaut est `/opt/ibm/apm/agent` sur les systèmes Linux et AIX.

b) Exécutez le script de configuration à partir du répertoire :

```
./was-agent.sh config
```

c) A l'invite du système, entrez 1 et appuyez sur Entrée pour modifier les paramètres de l'Agent WebSphere Applications.

d) Appuyez sur Entrée jusqu'à ce que le système vous invite à entrer l'ID de noeud alternatif pour identifier l'agent de surveillance.

e) Indiquez l'ID noeud et appuyez sur Entrée. La valeur admise est une chaîne alphanumérique pouvant inclure jusqu'à 24 caractères.

f) A l'invite du système, indiquez le port utilisé par l'agent pour écouter les demandes de connexion du collecteur de données et appuyez sur Entrée.

A faire : Pour des environnements de coexistence d'agent, vérifiez que le port indiqué n'est pas utilisé par l'ITCAM Agent for WebSphere Applications.

g) A l'issue de la configuration, redémarrez l'Agent WebSphere Applications.

Résultats
Vous avez configuré l'Agent WebSphere Applications.

Que faire ensuite
Vous devez ensuite configurer le collecteur de données. Lorsque vous configurez le collecteur de données, vous êtes invité à fournir le numéro de port que vous avez configuré pour l'Agent WebSphere Applications et l'ITCAM Agent for WebSphere Applications. Pour obtenir des instructions, voir «Configuration du collecteur de données pour l'environnement de coexistence d'agent», à la page 886.

Configuration du collecteur de données pour l'environnement de coexistence d'agent
Si votre environnement inclut à la fois l'Agent WebSphere Applications et l'ITCAM Agent for WebSphere Applications, vous ne pouvez configurer qu'un seul collecteur de données pour les deux agents.

Avant de commencer
Assurez-vous que d'avoir terminé les autres étapes qui sont documentées dans «(Coexistence d'agent) Configuration de l'Agent WebSphere Applications et du collecteur de données», à la page 883.

Pourquoi et quand exécuter cette tâche

Exécutez l'utilitaire de configuration interactif fourni pour configurer le collecteur de données pour un environnement où l'Agent WebSphere Applications et l'ITCAM Agent for WebSphere Applications existent et partagent le collecteur de données.

Limitation : L'intégration du collecteur de données aux composants ou aux produits suivants n'est pas prise en charge pour l'ITCAM Agent for WebSphere Applications :

- ITCAM for Application Diagnostics Managing Server
- ITCAM for Transactions
- Tivoli Performance Viewer

A faire : La surveillance de WebSphere Application Server Liberty n'est pas prise en charge par l'ITCAM Agent for WebSphere Applications. Pour surveiller WebSphere Application Server Liberty, utilisez uniquement l'Agent WebSphere Applications. Pour plus d'informations sur la configuration du collecteur de données pour la surveillance Liberty, voir «Configuration du collecteur de données en mode interactif», à la page 864 ou «Configuration du collecteur de données en mode silencieux», à la page 872.

Procédure

1. Connectez-vous au système à l'aide de l'ID utilisateur utilisé pour installer le serveur d'applications.
2. A partir de la ligne de commande, accédez au répertoire `bin` dans le répertoire *base_cd*. Le répertoire *base_cd* peut correspondre aux répertoires suivants :
   - Windows *rép_install*`\dchome\7.3.0.14.08`
   - Linux AIX *rép_install*`/yndchome/7.3.0.14.08`
3. Exécutez la commande suivante pour lancer l'utilitaire de configuration :
   - Windows `config.bat`
   - Linux AIX `./config.sh`

   L'utilitaire de configuration démarre et affiche les adresses IP de toutes les cartes réseau détectées sur le système informatique local.
4. Entrez le nombre qui correspond à l'adresse IP à utiliser et appuyez sur Entrée.

   L'utilitaire de configuration affiche les répertoires de base de WebSphere Application Server qui ont été détectés sur le système.
5. Lorsque vous êtes invité à entrer le répertoire de base du serveur d'applications, entrez le numéro correspondant au répertoire de base de WebSphere Application Server ou un chemin d'accès complet au répertoire de base du serveur d'applications et appuyez sur Entrée.

   L'utilitaire de configuration affiche tous les profils de serveur d'applications détectés sous le répertoire de base indiqué.
6. Lorsque vous êtes invité à indiquer le profil du serveur d'applications à configurer, entrez le numéro correspondant au profil WebSphere Application Server et appuyez sur Entrée.

   L'utilitaire de configuration indique si la sécurité globale de WebSphere est activée pour le profil WebSphere Application Server que vous avez indiqué. Si la sécurité globale n'est pas activée, passez à l'étape «8», à la page 887.

7. Spécifiez si vous voulez récupérer les paramètres depuis un fichier de propriétés de client. Entrez 1 pour permettre à l'utilitaire de configuration d'extraire le nom d'utilisateur et le mot de passe à partir du fichier de propriétés de client approprié. Sinon, entrez 2 pour entrer le nom d'utilisateur et le mot de passe WebSphere.

   Le collecteur de données communique avec les services d'administration de WebSphere en utilisant l'invocation RMI (Remote Method Invocation) ou le protocole SOAP. Si la sécurité globale est activée pour un profil de serveur d'applications, vous devez indiquer l'ID utilisateur et le mot de passe d'un utilisateur qui est autorisé à se connecter à la console d'administration de WebSphere Application Server pour ce profil. Vous avez également la possibilité de chiffrer le nom d'utilisateur et le mot de passe et de les stocker dans des fichiers de propriétés de client avant de configurer le collecteur de données. Vous devez utiliser le fichier `sas.client.props` pour une connexion RMI, ou le fichier `soap.client.props` pour une connexion SOAP.
8. Lorsque vous êtes invité à entrer le nom d'hôte de la console d'administration WebSphere, appuyez sur Entrée pour accepter les valeurs par défaut ou indiquez le nom d'hôte ou l'adresse IP de la console d'administration WebSphere. La valeur par défaut est `localhost`.
9. Lorsque l'utilitaire de configuration affiche une liste de toutes les instances de serveur qui ne sont pas encore configurées pour la collecte de données, sélectionnez une ou plusieurs instances de serveur d'applications dans la liste. Entrez le nombre qui correspond à l'instance de serveur d'applications à configurer pour la collecte de données ou entrez un astérisque (`*`) pour configurer toutes les instances de serveur d'applications pour la collecte de données, puis appuyez sur Entrée. Pour spécifier un sous-ensemble de serveurs, entrez les numéros qui représentent les serveurs, séparés par des virgules.
   Par exemple, `1,2,3`.

   A faire :

   - Pour un environnement autonome, les instances de serveur d'applications doivent s'exécuter pendant la configuration.
   - Pour un environnement de déploiement réseau, Deployment Manager doit être en cours d'exécution.
   - Assurez-vous que les instances de serveur d'applications que vous sélectionnez sont les serveurs réels qui hébergent les applications ou les services que vous voulez surveiller.

   L'utilitaire de configuration fournit une option pour intégrer le collecteur de données pour l'Agent WebSphere Applications.
10. Dans la section **Integration with Agent for WebSphere Applications**, indiquez si vous souhaitez intégrer le collecteur de données à l'agent de surveillance. Vous devez entrer 1 pour sélectionner cette option d'intégration, puis appuyer sur Entrée.

    Le serveur sélectionné sera enregistré pour la surveillance des ressources PMI.
11. Indiquez si vous souhaitez configurer le collecteur de données dans l'instance de serveur d'applications. Vous devez entrer 1 pour oui, puis appuyez sur Entrée.
12. Indiquez s'il faut activer ou non le collecteur de données pour les données de diagnostic. Entrez 1 pour oui ou 2 pour non.
13. Lorsque vous êtes invité à entrer le nom d'hôte de l'agent de surveillance V8, entrez le nom d'hôte ou l'adresse IP de l'Agent WebSphere Applications ou acceptez la valeur par défaut.
14. Lorsque vous êtes invité à entrer le numéro de port de l'agent de surveillance V8, entrez le numéro de port utilisé par l'Agent WebSphere Applications.

    A faire : La valeur par défaut peut ne pas être appropriée si elle est utilisée par un autre composant. Vous devez vous assurer que le port spécifié n'est pas utilisé par un autre composant dans votre environnement.
15. Indiquez si vous souhaitez configurer l'agent de surveillance V6. Entrez 1 pour configurer l'ITCAM Agent for WebSphere Applications et appuyez sur Entrée.
16. Lorsque vous êtes invité à entrer le nom d'hôte ou l'adresse IP de l'agent de surveillance V6, indiquez le nom d'hôte ou l'adresse IP de l'ITCAM Agent for WebSphere Applications.

17. Lorsque vous êtes invité à entrer le numéro de port de l'agent de surveillance V6, entrez le numéro de port utilisé par le composant agent de surveillance de l'ITCAM Agent for WebSphere Applications.

    A faire : La valeur par défaut peut ne pas être appropriée si elle est utilisée par un autre composant. Vous devez vous assurer que le port spécifié n'est pas utilisé par un autre composant dans votre environnement.
18. Lorsque vous êtes invité à entrer l'alias de serveur, n'utilisez pas la valeur par défaut et indiquez l'alias de serveur unique que vous souhaitez utiliser. Si vous configurez plusieurs instances de serveur d'applications, l'utilitaire de configuration vous invite à indiquer un alias pour chaque instance.

    Important : L'alias ne peut contenir que les caractères suivants : A-Z, a-z, soulignement (_), tiret (-) et point (.). N'utilisez pas d'autres caractères dans l'alias.

    L'alias de serveur est le premier qualificateur du nom d'instance d'agent (également appelé MSN) affiché sur la console Cloud APM. La valeur par défaut est le nom du noeud combiné au nom du serveur. Par exemple, l'alias **node1server1** indique le serveur **server1** dans le noeud **node1**.
19. Lorsque vous êtes invité à entrer le numéro de port TCP/IP pour la surveillance des ressources PMI, appuyez sur Entrée pour accepter la valeur par défaut ou entrez un nouveau numéro. La valeur par défaut est 63355.

    Le port est utilisé pour la communication interne entre les composants qui s'exécutent sur le même hôte. Si le port par défaut est déjà utilisé, définissez un numéro différent.
20. Dans la section **Prise en charge du suivi des transactions**, indiquez si vous souhaitez activer le suivi des transactions. Entrez 1 pour oui ou 2 pour non et passez à l'étape 22.

    A faire : Pour afficher les informations de suivi des transactions, vous devez activer le suivi des transactions dans la page Configuration d'agent de la console Cloud APM.
21. Acceptez le nom d'hôte ou l'adresse IP par défaut de Transaction Framework Extension, qui est un composant interne de l'Agent WebSphere Applications qui collecte les attributs depuis le collecteur de données.
22. Acceptez le numéro de port par défaut que le collecteur de données utilise pour se connecter à Transaction Framework Extension. La valeur par défaut est 5457.
23. Indiquez si vous voulez intégrer le collecteur de données à Application Performance Diagnostics Lite. Appuyez sur Entrée pour accepter la valeur par défaut pour Non.
24. Dans la section **Paramètres avancés**, indiquez si vous souhaitez modifier le chemin du journal de la récupération de place. Entrez 1 pour sélectionner un chemin d'accès au journal de récupération de place. Autrement, entrez 2 et passez à l'étape «26», à la page 888.
25. Indiquez le chemin de la collecte de récupération de place. Entrez un nom de fichier avec son chemin d'accès complet.

    Par exemple, si vous indiquez `gc.log` comme nom de fichier, le nom réel est défini sur *nom_profil*`.`*nom-cellule*`.`*nom_noeud*`.`*nom_serveur*`.gc.log` pour chaque instance de serveur d'applications configurée.

    Important : Dans le chemin d'accès au journal de récupération de place, vous pouvez utiliser des variables WebSphere, telles que `${SERVER_LOG_ROOT}`. Cependant, n'utilisez pas de modèles, tels que `%pid`.
26. Dans la section **Récapitulatif de la configuration du collecteur de données**, examinez le récapitulatif de la configuration du collecteur de données qui doit être appliquée aux instances de serveur d'applications indiquées. Si nécessaire, modifiez les paramètres de configuration.
27. Entrez a pour accepter les modifications.
28. A l'invite, indiquez si vous souhaitez créer une copie de sauvegarde de votre configuration en cours. Entrez 1 pour créer une sauvegarde de la configuration en cours. Sinon, entrez 2.
29. Redémarrez les instances du serveur d'applications, comme indiqué par l'utilitaire de configuration.
    a) Accédez au répertoire `bin` situé sous le répertoire de base du profil de serveur d'applications. Par exemple, `opt/IBM/WebSphere/AppServer/profiles/`*nom_profil*`/bin`.

b) Arrêtez le serveur d'applications en entrant la commande **stopServer** dans la console de commande.

- Linux AIX `./stopServer.sh` *nom_serveur*
- Windows `stopServer.bat` *nom_serveur*

c) A l'invite, entrez l'ID utilisateur et le mot de passe de l'administrateur de la console d'administration WebSphere.

d) Redémarrez le serveur d'applications en entrant la commande **startServer** dans la console de commande.

- Linux AIX `./startServer.sh` *nom_serveur*
- Windows `startServer.bat` *nom_serveur*

La configuration du collecteur de données entre en vigueur une fois que le serveur d'applications a redémarré.

30. Connectez-vous à la console Cloud APM pour afficher les données dans les tableaux de bord.

a) Accédez à la console en utilisant le lien fourni dans l'e-mail vous signalant que votre service est prêt. Vous pouvez également accéder à la console à partir du site Web IBM Marketplace. Pour des instructions détaillées, voir «Démarrage de la console Cloud APM», à la page 1003.

b) Utilisez l'éditeur d'applications pour ajouter le serveur d'applications surveillé au Tableau de bord d'Application Performance. Vous pouvez l'ajouter en tant que nouveau composant à votre application existante ou créer une application à laquelle ajouter ce composant.

Pour plus d'informations sur l'éditeur d'applications, voir «Gestion des applications», à la page 1129.

Que faire ensuite

- Si l'ID utilisateur actuel utilisé pour configurer le collecteur de données n'est pas identique à l'ID de l'utilisateur qui exécute le serveur d'applications, vérifiez que l'ID utilisateur de configuration du collecteur de données dispose des droits en lecture et en écriture sur les répertoires `runtime` et `logs` dans le répertoire de base du collecteur de données. Ces deux sous-répertoires sont créés par l'ID de l'utilisateur qui exécute le serveur d'applications lorsque le serveur est redémarré.
- Pour l'Agent WebSphere Applications, connectez-vous à la console Cloud APM pour afficher les données de surveillance dans les tableaux de bord. Pour l'ITCAM Agent for WebSphere Applications, connectez-vous à Tivoli Enterprise Portal pour afficher les données. Si les données de surveillance ne sont pas disponibles immédiatement, redémarrez l'agent de surveillance en exécutant les commandes suivantes :
  - Windows

    ```
    cd rép_install\bin
    was-agent.bat stop
    was-agent.bat start
    ```

  - Linux AIX

    ```
    cd rép_install/bin
    ./was-agent.sh
    stop
    ./was-agent.sh start
    ```

- La modification de l'alias de serveur entraîne la modification du nom d'instance de l'agent enregistré dans la console Cloud APM. Si ce n'est pas la première fois que vous configurez le collecteur de données et que vous avez modifié l'alias de serveur, vous devez vider certains fichiers cache en effectuant les opérations suivantes :

1. Arrêtez l'agent de surveillance s'il est en cours d'exécution.

2. Ouvrez le fichier *nom_hôte*_yn.xml dans le répertoire suivant avec un éditeur de texte, où *nom_hôte* est le nom de l'hôte où l'Agent WebSphere Applications ou l'ITCAM Agent for WebSphere Applications est installé.
   - Windows *rép_install*\TMAITM6_x64 (la valeur par défaut est C:\IBM\APM\TMAITM6_x64 pour l'Agent WebSphere Applications ou C:\IBM\ITM\TMAITM6_x64 pour l'ITCAM Agent for WebSphere Applications)
   - Linux AIX *rép_install*/config (La valeur par défaut est /opt/ibm/apm/agent/config pour l'Agent WebSphere Applications ou /opt/ibm/itm/agent/config pour l'ITCAM Agent for WebSphere Applications)
3. Recherchez la ligne qui commence par la chaîne suivante et qui contient le nom de serveur précédent. Par exemple was85.win4net01Cell02.win4net01Node02.AppSrv01.server1, où server1 est le nom précédent du serveur d'applications.

   ```
   <!ENTITY code_produit_was.nom_cellule.nom_noeud.nom_profil.nom_serveur
   ```

   où *code_produit_was* est le code produit de WebSphere Application Server ; *nom_cellule* est le nom de la cellule ; *nom_noeud* est le nom du noeud ; *nom_profil* est le nom du profil de serveur d'applications ; *nom_serveur* est le nom précédent du serveur d'applications.
4. Dans le répertoire en cours, recherchez le fichier .XML indiqué sur la ligne et supprimez-le.
5. Supprimez la ligne que vous avez recherchée à l'étape 3 dans le fichier *nomhôte*_yn.xml.
6. A la fin du fichier *nom_hôte*_yn.xml, supprimez la ligne qui contient les noms de serveur précédents.
7. Sauvegardez et fermez le fichier.
8. Redémarrez l'agent de surveillance.

Reconfiguration du collecteur de données en cas de modification du type d'offre sur le serveur Cloud APM

Si vous avez modifié le type d'offre que vous avez installé sur le serveur Cloud APM (de Cloud APM, Base à Cloud APM, Advanced) et que l'Agent WebSphere Applications a été installé et configuré avec l'offre Cloud APM, Base, vous devez, pour pouvoir utiliser les fonctions avancées de l'agent fournies dans l'offre Cloud APM, Advanced, désinstaller l'Agent WebSphere Applications précédent et réinstaller l'agent avec l'offre Cloud APM, Advanced. Vous pouvez aussi reconfigurer le collecteur de données pour que les fonctionnalités soient disponibles dans la nouvelle offre.

Pourquoi et quand exécuter cette tâche

La configuration de l'Agent WebSphere Applications est différente selon le package d'agent utilisé pour installer l'agent. Après avoir modifié le type d'offre sur le serveur Cloud APM, vous disposez de deux options pour activer les fonctionnalités d'agent de la nouvelle offre :

- Supprimez l'agent que vous avez installé avec l'offre précédente, puis installez l'agent de la nouvelle offre.
- Reconfigurez le collecteur de données pour utiliser les fonctionnalités de la nouvelle offre.

Procédure

- Supprimez l'agent que vous avez installé avec l'offre précédente, puis installez l'agent de la nouvelle offre.
  a) Annulez la configuration du collecteur de données. Pour obtenir des instructions, voir «Agent WebSphere Applications : Annulation de la configuration du collecteur de données», à la page 152.
  b) Désinstallez l'Agent WebSphere Applications que vous avez installé avec le package d'agent de l'offre précédente. Pour obtenir des instructions, voir «Désinstallation de vos agents», à la page 150.

c) Installez l'Agent WebSphere Applications avec le package d'agent de la nouvelle offre, puis reconfigurez le collecteur de données. Pour plus d'informations, voir «Configuration du collecteur de données avec l'utilitaire de configuration simple», à la page 861.

- Reconfigurez le collecteur de données pour utiliser les fonctionnalités de la nouvelle offre.

  a) Editez le fichier `offering.id` dans le répertoire de base du collecteur de données en remplaçant la valeur **IOFFERING** par l'une des valeurs suivantes, selon le nouveau type d'offre :

  BASE
  Si votre nouveau type d'offre est Cloud APM, Base Private.

  ADVANCED
  Si votre nouveau type d'offre est Cloud APM, Advanced Private.

  Le répertoire de base du collecteur de données est le suivant :

  – Windows *rép_install*\dchome\7.3.0.14.08

  – Linux AIX *rép_install*/yndchome/7.3.0.14.08

  b) Reconfigurez le collecteur de données pour activer les fonctions de diagnostic, de suivi des transactions ou les deux dans le collecteur de données, sur la base des fonctionnalités prises en charge dans le nouveau type d'offre. Pour savoir comment configurer le collecteur de données, voir «Configuration du collecteur de données avec l'utilitaire de configuration simple», à la page 861.

  c) Redémarrez WebSphere Application Server.

  d) Dans une page quelconque de la console Cloud APM, cliquez sur **Configuration du système** > **Configuration d'agent** pour ouvrir la page **Configuration d'agent**. Assurez-vous que le paramètre de suivi des transactions correspond aux fonctionnalités disponibles dans votre nouveau type d'offre. Sinon, mettez le paramètre à jour.

  Le paramètre de suivi des transactions doit être activé pour Cloud APM, Advanced, mais désactivé pour Cloud APM, Base.

Surveillance de WebSphere Application Server Liberty dans un conteneur Docker
Pour surveiller un profil Liberty dans un conteneur Docker, vous devez utiliser la commande **docker run** avec quelques options afin de configurer le collecteur de données pour que WebSphere Application Server Liberty puisse démarrer.

Avant de commencer
Vous devez installer Agent WebSphere Applications sur l'hôte Docker.

Pourquoi et quand exécuter cette tâche

Chaque profil Liberty qui s'exécute dans un conteneur Docker nécessite un collecteur de données pour collecter des mesures de ressource, des mesures de transaction et des données de diagnostic, puis transmettre les données à l'agent de surveillance qui s'exécute sur l'hôte Docker. Tous les collecteurs de données configurés sur le même hôte Docker se partagent le même agent de surveillance sur l'hôte.

Procédure

Pour configurer le collecteur de données pour un conteneur de profil Liberty, procédez comme suit :

1. Créez un fichier de réponses silencieux `.txt`, indiquez les options de configuration suivantes dans le fichier et enregistrez-le.

```
tema.host=hôte_agent
was.appserver.server.name=nom_profil_liberty
```

   où **tema.host** permet d'indiquer l'adresse IP de l'hôte de l'agent de surveillance et **was.appserver.server.name** le nom du profil Liberty.

Conseil : Un exemple de fichier de réponses silencieux (`sample_silent_liberty_config.txt`) est fourni dans le répertoire *<rép_install_agent>*`/agent/yndchome/7.3.0.14.08/bin`. Vous pouvez créer votre propre fichier de réponses en vous basant sur cet exemple.

2. Exécutez la commande suivante pour démarrer le nouveau conteneur Docker. Vous devez accepter la licence pour finaliser la configuration en définissant le paramètre **LICENSE** sur `accept`.

```
$docker run -d -e LICENSE=accept \
-e JAVA_HOME=<rép_base_java> \
-p <numéro_port>:<numéro_port> \
-v <rép_app_web>:<rép_install_liberty>/usr/servers/<nom_profil_liberty> \
-v <rép_install_agent>/agent/yndchome:<rép_install_agent>/agent/yndchome
websphere-liberty /bin/bash \
-c "<rép_install_agent>/agent/yndchome/<version_cd>/bin/config.sh -silent
<absolute_path_to_silent_response_file> && <rép_install_liberty>/bin/server
run <nom_profil_liberty>"
```

où :

- *<rép_base_java>* est le répertoire de l'environnement d'exécution Java qu'utilise le profil Liberty. Par exemple, `/opt/ibm/java/jre`.
- *<numéro_port>* est le numéro du port utilisé pour la communication entre le conteneur et l'hôte.
- *<rép_app_web>* est le répertoire dans lequel se trouve l'application Web.
- *<rép_install_liberty>* est le répertoire d'installation de WebSphere Application Server Liberty. Par défaut, il s'agit du répertoire `/opt/ibm/wlp`.
- *<nom_profil_liberty>* est le nom du profil Liberty.
- *<rép_install_agent>* est le répertoire d'installation de l'Agent WebSphere Applications. Par défaut, il s'agit du répertoire `/opt/ibm/apm`.
- *<version_cd>* est le numéro de version du collecteur de données pour l'Agent WebSphere Applications. Par exemple, 7.3.0.14.08.
- *<chemin_absolu_fichier_réponses_silencieux>* est le chemin d'accès absolu au fichier de réponses silencieux que vous avez créé.

Par exemple, la commande suivante configure le collecteur de données pour le profil Liberty nommé newitcam. L'Agent WebSphere Applications et le profil Liberty sont tous deux installés dans les répertoires par défaut. La version de l'agent de surveillance et du collecteur de données est 7.3.0.14.08.

```
$docker run -d -e LICENSE=accept \
-e JAVA_HOME=/opt/ibm/java/jre \
-p 9082:9082 \
-v /home/kub/liberty-docker/newitcam:/opt/ibm/wlp/usr/servers/newitcam \
-v /opt/ibm/apm/agent/yndchome:/opt/ibm/apm/agent/yndchome websphere-liberty
/bin/bash \
-c "/opt/ibm/apm/agent/yndchome/7.3.0.14.08/bin/config.sh -silent
/opt/ibm/wlp/usr/servers/newitcam/silent_config.txt && /opt/ibm/wlp/bin/server
run newitcam"
```

Résultats

Vous pouvez à présent vérifier que les données de l'Agent WebSphere Applications s'affichent dans la console Cloud APM. La colonne **Nom de la cellule** du widget **Informations WAS** affiche l'ID du conteneur Docker où s'exécute le profil Liberty.

Que faire ensuite

Pour annuler la configuration du collecteur de données de manière interactive, utilisez la commande suivante pour démarrer l'utilitaire d'annulation de configuration :

```
docker exec -i id_conteneur "<rép_install_agent>/yndchome/7.3.0.14.08/bin
/unconfig.sh"
```

Configuration manuelle du collecteur de données en vue de surveiller des serveurs de cluster dynamique

Vous pouvez configurer le collecteur de données pour surveiller des instances de serveur d'applications dans un cluster dynamique en ajoutant quelques paramètres de configuration de collecteur de données au modèle de serveur utilisé pour créer les instances de serveur de cluster dynamique. C'est une méthode alternative à la création de modèles de serveur spécifiques pour l'Agent WebSphere Applications pour configurer des instances de serveur de cluster dynamique.

Pourquoi et quand exécuter cette tâche

Pour configurer le collecteur de données pour la surveillance des clusters dynamiques, vous devez créer deux fichiers de paramètres, puis ajouter manuellement les paramètres dans la console d'administration WebSphere afin de modifier le modèle de serveur dynamique. Le répertoire d'`exécution` est créé automatiquement lorsque le collecteur de données est démarré pour l'instance de serveur d'applications. Toute mise à niveau du modèle de serveur supprime les modifications effectuées de cette manière.

Important :

- Le nom de cluster ne doit pas contenir d'espace.
- Vous devez apporter des modifications manuelles à la configuration WebSphere Application Server pour les collecteurs de données en tant qu'administrateur WebSphere.
- Vous devez être un administrateur WebSphere expérimenté pour apporter des modifications manuelles à WebSphere Application Server en vue de la collecte de données. Toute erreur dans la modification manuelle de la configuration peut empêcher le démarrage du serveur d'applications.
- Si vous configurez manuellement le collecteur de données pour surveiller des instances de serveur d'application, vous ne pouvez pas employer l'utilitaire d'annulation de configuration pour annuler la configuration du collecteur de données. Pour annuler la configuration du collecteur de données, vous devez rétablir manuellement les paramètres.

Procédure

1. Créez le fichier `dcManualInput.txt` dans le répertoire `runtime` du collecteur de données.

   Suivez les instructions décrites dans «Création du fichier dcManualInput.txt», à la page 893.
2. Créez le fichier `itcam_wsBundleMetaData.xml` dans le répertoire `wsBundleMetaData` du collecteur de données. Suivez les instructions décrites dans «Création du fichier itcam_wsBundleMetaData.xml», à la page 896.
3. Utilisez la console d'administration WebSphere pour modifier le modèle de serveur dynamique en ajoutant le paramètre de configuration du collecteur de données. Suivez les instructions décrites dans «Ajout de paramètres avec la console d'administration WebSphere», à la page 897.

   Conseil : Le nom de membre du cluster dynamique est utilisé comme qualificateur du milieu dans le nom d'instance de l'Agent WebSphere Applications affiché dans la console Cloud APM. Il est possible que le nom de membre du cluster soit tronqué en raison du nombre maximal de caractères dans le nom d'instance de l'agent. Dans ce cas, vous pouvez modifier le modèle du serveur dynamique en ajoutant une variable nommée *${MEP_NAME}* et en lui attribuant le nom de machine virtuelle Java pour chaque instance de serveur. Vous pouvez ensuite distinguer chaque membre du cluster à l'aide du nom de machine virtuelle Java réel dans la console Cloud APM. Pour obtenir des instructions, voir «Facultatif : Affichage du nom de machine virtuelle réel pour établir une distinction entre les membres du cluster», à la page 900.

Création du fichier dcManualInput.txt

Pourquoi et quand exécuter cette tâche

Le fichier `dcManualInput.txt` contient certaines valeurs obligatoires pour la configuration initiale du collecteur de données.

Procédure

Pour créer le fichier dcManualInput.txt, procédez comme suit :

1. Vérifiez s'il existe un fichier nommé *plateforme*_Template.DCManualInput.txt dans le répertoire suivant. S'il n'existe pas, créez-le.

   - Linux AIX *rép_install*/yndchome/7.3.0.14.08/runtime
   - Windows *rép_install*\dchome\7.3.0.14.08\runtime

   La variable *plateforme* dans le nom du fichier désigne l'architecture du système d'exploitation, par exemple, aix32, xLinux64.

   Vous pouvez attribuer au fichier le nom qui vous convient. Toutefois, *plateforme*_Template.DCManualInput.txt respecte les conventions d'attribution de nom lorsque le fichier est créé en exécutant le script configtemplate.sh. Vous devrez indiquer ce fichier pour le modèle de serveur avec la console d'administration WebSphere à la prochaine étape.
2. Copiez le contenu du fichier suivant dans le fichier .txt que vous avez trouvé ou créé à l'étape précédente.

   - Linux AIX *base_cd*/itcamdc/etc/was/dcInput_manual.properties
   - Windows *base_cd*\itcamdc\etc\was\dcInput_manual.properties
3. Editez le contenu du fichier .txt. Vous devez définir les paramètres de la section 1 du fichier en fonction des descriptions fournies dans Tableau 226, à la page 894.

   A faire :

   - Ne modifiez pas les paramètres de la section 2.
   - Certains des paramètres de configuration qu'utilise le collecteur de données pour créer les répertoires d'exécution sont toujours définis sur none. En effet, dans la surveillance des clusters dynamiques, le collecteur de données utilise la configuration de l'instance de serveur WebSphere pour créer les répertoires au démarrage de la machine virtuelle Java.

Tableau 226. Paramètres de configuration de la section 1

Paramètre	Valeur
local.hostname	Adresse IP ou nom de domaine qualifié complet du système local.
was.profile.home	Répertoire de base du profil. Toujours définir sur none pour un serveur de cluster dynamique
was.version	Numéro de version abrégé. Toujours définir sur none pour un serveur de cluster dynamique
itcam.home	Répertoire de base du collecteur de données. Exemple : /opt/ibm/apm/agent/yndchome/7.3.0.14.08
was.nodename	Nom du noeud. Toujours définir sur none pour un serveur de cluster dynamique

Tableau 226. Paramètres de configuration de la section 1 (suite)	
Paramètre	**Valeur**
was.servername	Nom du serveur. Toujours définir sur none pour un serveur de cluster dynamique
was.profilename	Nom du profil WebSphere. Toujours définir sur none pour un serveur de cluster dynamique
am.camtoolkit.gpe.dc.operation.mode	Mode de fonctionnement du collecteur de données. Les valeurs admises sont toute combinaison de WR, TT et DE, où : **WR** Intègre le collecteur de données à l'Agent WebSphere Applications. **TT** Intègre le collecteur de données à ITCAM for Transactions. **DE** Intègre le collecteur de données à l'outil de diagnostics d'ITCAM. L'outil est présent dans la version bêta d'ITCAM for Application Diagnostics. Vous ne devez indiquer que les modes de fonctionnement obligatoires. Par exemple, si vous connectez le collecteur de données uniquement à l'Agent WebSphere Applications, indiquez WR. Séparez les modes de fonctionnement avec une virgule. Exemple : `am.camtoolkit.gpe.dc.operation.mode=WR, DE`
interp	Code de plateforme. Exemple : `interp=win64` ou `interp=lx6266`
kwj.serveralias	Nom d'alias de WebSphere Application Server. Toujours définir sur none pour un serveur de cluster dynamique
temagclog.path	(Facultatif) Nom du chemin d'accès au fichier journal de récupération de place. Entrez un nom de fichier unique avec son chemin complet. Le nom de chemin ne doit pas contenir d'espaces.
tema.host	Nom d'hôte ou adresse IP de l'Agent WebSphere Applications. Obligatoire si le mode de fonctionnement inclut l'Agent WebSphere Applications (WR). En général, l'agent de surveillance est installé sur chaque système où le collecteur de données s'exécute et l'adresse de bouclage peut être indiquée. Exemple : `tema.host=127.0.0.1`

Tableau 226. Paramètres de configuration de la section 1 (suite)	
Paramètre	**Valeur**
tema.port	Port à utiliser pour communiquer avec l'Agent WebSphere Applications. Obligatoire si le mode de fonctionnement inclut l'Agent WebSphere Applications (WR). La valeur par défaut est 63335. Exemple : `tema.port=63335`
tt.connection.string	Nom d'hôte ou adresse IP et numéro de port du composant collecteur de transaction d'ITCAM for Transactions au format `tcp:`*`nom_hôte`*`(IP):`*`port`*. Obligatoire si le mode de fonctionnement inclut ITCAM for Transactions (TT). Exemple : `tt.connection.string=192.38.234.77:5455`

4. Ajoutez les lignes suivantes à la section 1 du fichier `.txt`.

```
bcm.helper=com.ibm.tivoli.itcam.was.bcm.websphere.DefaultWASBCMHelper
BCM_HELPER=@{bcm.helper}
```

5. Sauvegardez et fermez le fichier.

Création du fichier `itcam_wsBundleMetaData.xml`

Pourquoi et quand exécuter cette tâche

Le fichier `itcam_wsBundleMetaData.xml` contient certaines des valeurs obligatoires pour la configuration initiale du collecteur de données.

Procédure

Pour créer ce fichier, procédez comme suit :

1. Créez un répertoire nommé `wsBundleMetaData` dans le répertoire suivant :
   - Linux AIX *`rép_install`*`/yndchome/7.3.0.14.08/runtime`
   - Windows *`rép_install`*`\dchome\7.3.0.14.08\runtime`
2. Créez un fichier nommé `itcam_wsBundleMetaData.xml` et copiez dans ce fichier le contenu du fichier suivant :
   - Linux AIX *`rép_install`*`/yndchome/7.3.0.14.08/itcamdc/etc/was/itcam_wsBundleMetaData_template.xml`
   - Windows *`rép_install`*`\dchome\7.3.0.14.08\itcamdc\etc\was\itcam_wsBundleMetaData_template.xml`
3. Dans le fichier `itcam_wsBundleMetaData.xml`, remplacez la variable *@{CONFIGHOME}* par le chemin d'accès complet au répertoire de base de votre collecteur de données.

   Sur chaque système d'exploitation, le répertoire de base du collecteur de données est le suivant :
   - Linux AIX *`rép_install`*`/yndchome/7.3.0.14.08`
   - Windows *`rép_install`*`\dchome\7.3.0.14.08`
4. Placez le fichier `itcam_wsBundleMetaData.xml` dans le répertoire `wsBundleMetaData` créé à l'étape 1.

Ajout de paramètres avec la console d'administration WebSphere

Procédure

Pour modifier le modèle de serveur dynamique avec la console d'administration WebSphere, procédez comme suit :

1. Connectez-vous à la console d'administration WebSphere.
2. Cliquez sur **Serveurs**.
3. Développez **Clusters**, puis sélectionnez **Clusters dynamiques**.
4. Cliquez sur le nom du cluster de serveurs dynamiques à configurer avec le collecteur de données.
5. Dans la section **Propriétés supplémentaires**, cliquez sur **Modèle de serveur**.
6. Dans la section **Infrastructure du serveur**, développez **Gestion des processus et Java**, puis cliquez sur **Définition des processus**.
7. Dans la section **Propriétés supplémentaires**, cliquez sur **Machine virtuelle Java**.
8. Dans la zone **Arguments JVM génériques**, ajoutez les entrées suivantes :

   ```
   -agentlib:am_$jvm-vendor_$jvm-version=${WAS_SERVER_NAME}
   -Xbootclasspath/p:${ITCAMDCHOME}/toolkit/lib/bcm-bootstrap.jar
   -Djava.security.policy=${ITCAMDCHOME}/itcamdc/etc/datacollector.policy
   -verbosegc -Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=${ITCAMDCHOME}/runtime/
   $platform_Template_DCManualInput.txt
   -Dsun.rmi.dgc.client.gcInterval=3600000
   -Dsun.rmi.dgc.server.gcInterval=3600000
   -Dsun.rmi.transport.connectionTimeout=300000
   -Dws.bundle.metadata=${ITCAMDCHOME}/runtime/wsBundleMetaData
   –Ditcamdc.dyncluster=true
   ```

   Lors de l'ajout de ces entrées, notez les éléments suivants :

   - Toutes les entrées doivent se trouver sur une seule ligne.
   - Séparez les différents arguments par des espaces avant le signe `-`. N'utilisez pas d'espaces ailleurs.
   - Remplacez les variables suivantes par les noms réels :
     - *$jvm-vendor* : fournisseur de machine virtuelle Java utilisé.
     - *$jvm-version* : informations sur la version de machine virtuelle Java, telles que base 15 sur Java 5, base 16 sur Java 6 ou base 17 sur Java 7.
     - *$platform_Template_DCManualInput.txt* : fichier `.txt` créé à l'étape précédente.

     Exemple :

     ```
     -agentlib:am_ibm_16=${WAS_SERVER_NAME}
     -Xbootclasspath/p:${ITCAMDCHOME}/toolkit/lib/bcm-bootstrap.jar
     -Djava.security.policy=${ITCAMDCHOME}/itcamdc/etc/datacollector.policy
     -verbosegc -Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=${ITCAMDCHOME}/runtime/
     aix64_Template_DCManualInput.txt
     -Dsun.rmi.dgc.client.gcInterval=3600000
     -Dsun.rmi.dgc.server.gcInterval=3600000
     -Dsun.rmi.transport.connectionTimeout=300000
     -Dws.bundle.metadata=${ITCAMDCHOME}/runtime/wsBundleMetaData
     –Ditcamdc.dyncluster=true
     ```
9. Cliquez sur **Appliquer**.
10. Dans la boîte de dialogue Messages, cliquez sur **Sauvegarder**.
11. Dans la boîte de dialogue Sauvegarde dans la configuration principale, effectuez les opérations suivantes :
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que **Synchroniser les modifications avec les noeuds** est sélectionné, puis cliquez sur **Sauvegarder**.
    - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
12. Revenez dans **Clusters**, cliquez sur **Clusters dynamiques**, puis sur le même nom de serveur.

13. Dans l'onglet **Configuration**, accédez à **Infrastructure du serveur** > **Gestion des processus et Java** > **Définition des processus** > **Entrées d'environnement**.
14. Selon le système d'exploitation, la plateforme matérielle et la machine virtuelle Java de serveur d'applications utilisés, définissez l'entrée d'environnement suivante :

Tableau 227. Entrée d'environnement

Plateforme	Nom de l'entrée d'environnement	Valeur de l'entrée d'environnement
AIX R6.1 (machine virtuelle Java 32 bits)	LIBPATH	/lib:${ITCAMDCHOME}/toolkit/lib/aix533:${ITCAMDCHOME}/toolkit/lib/aix533/ttapi
AIX R6.1 (machine virtuelle Java 64 bits)	LIBPATH	/lib:${ITCAMDCHOME}/toolkit/lib/aix536:${ITCAMDCHOME}/toolkit/lib/aix536/ttapi
AIX R7.1 (machine virtuelle Java 32 bits)	LIBPATH	/lib:${ITCAMDCHOME}/toolkit/lib/aix533:${ITCAMDCHOME}/toolkit/lib/aix533/ttapi
AIX R7.1 (machine virtuelle Java 64 bits)	LIBPATH	/lib:${ITCAMDCHOME}/toolkit/lib/aix536:${ITCAMDCHOME}/toolkit/lib/aix536/ttapi
Linux x86_64 R2.6 (machine virtuelle Java 64 bits)	LD_LIBRARY_PATH	/lib:${ITCAMDCHOME}/toolkit/lib/lx8266:${ITCAMDCHOME}/toolkit/lib/lx8266/ttapi
Linux Intel R2.6 (machine virtuelle Java 32 bits)	LD_LIBRARY_PATH	/lib:${ITCAMDCHOME}/toolkit/lib/lx6263:${ITCAMDCHOME}/toolkit/lib/lx6263/ttapi
Linux ppc R2.6 (machine virtuelle Java 32 bits)	LD_LIBRARY_PATH	/lib:${ITCAMDCHOME}/toolkit/lib/lpp263:${ITCAMDCHOME}/toolkit/lib/lpp263/ttapi
Linux ppc R2.6 (machine virtuelle Java 64 bits)	LD_LIBRARY_PATH	/lib:${ITCAMDCHOME}/toolkit/lib/lpp266:${ITCAMDCHOME}/toolkit/lib/lpp266/ttapi
Windows (machine virtuelle Java 32 bits)	PATH	/lib;${ITCAMDCHOME}/toolkit/lib/win32;${ITCAMDCHOME}/toolkit/lib/win32/ttapi
Windows (machine virtuelle Java 64 bits)	PATH	/lib;${ITCAMDCHOME}/toolkit/lib/win64;${ITCAMDCHOME}/toolkit/lib/win64/ttapi

15. Définissez le nom d'entrée d'environnement NLSPATH sur la valeur suivante :

```
${ITCAMDCHOME}/toolkit/msg/%L/%N.cat
```

16. Cliquez sur **Appliquer**, puis sur **Sauvegarder**.
17. Dans la boîte de dialogue Sauvegarde dans la configuration principale, effectuez les opérations suivantes :
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que **Synchroniser les modifications avec les noeuds** est sélectionné, puis cliquez sur **Sauvegarder**.
    - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
18. Revenez dans **Clusters**, cliquez sur **Clusters dynamiques**, puis sur le même nom de serveur.
19. Dans l'onglet **Configuration**, accédez à **Infrastructure du serveur** > **Gestion des processus et Java** > **Définition des processus** > **Machine virtuelle Java** > **Propriétés supplémentaires : Propriétés personnalisées**.
20. Cliquez sur **Nouveau** pour ajouter les paires nom-valeur suivantes, puis cliquez sur **Appliquer**.
    - Créez une propriété `am.home` et définissez sa valeur sur le répertoire suivant :
      - Linux AIX *rép_install*`/yndchome/7.3.0.14.08/itcamdc`
      - Windows *rép_install*`\dchome\7.3.0.14.08\itcamdc`
    - Créez une propriété `am.orig.wascell` et définissez sa valeur sur le répertoire de cellule. Par exemple, `am.orig.wascell =cellname1`.
    - Créez une propriété `com.ibm.tivoli.itcam.toolkit.ai.runtimebuilder.enable.rebuild` et définissez sa valeur sur `true`.
    - Créez une propriété `ITCAM_DC_ENABLED` et définissez sa valeur sur `true`.
    - Créez une propriété `TEMAGCCollector.gclog.path`. Si l'argument `verlogsegclog` de la machine virtuelle Java générique est défini, définissez la propriété `TEMAGCCollector.gclog.path` sur la même valeur. Sinon, définissez la propriété `TEMAGCCollector.gclog.path` sur `None`.

      Conseil : Pour identifier la valeur de la propriété `verlogsegclog`, dans l'onglet **Configuration**, cliquez sur **Infrastructure du serveur** > **Gestion des processus et Java** > **Définition des processus** > **Machine virtuelle Java**. La valeur de `verlogsegclog` est indiquée dans la zone **Arguments JVM génériques**.
21. Dans la boîte de dialogue Messages, cliquez sur **Sauvegarder**.
22. Dans la boîte de dialogue Sauvegarde dans la configuration principale, effectuez les opérations suivantes :
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que **Synchroniser les modifications avec les noeuds** est sélectionné. Cliquez sur **Sauvegarder**.
    - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.
23. Dans le panneau de navigation, cliquez sur **Environnement** > **Variables WebSphere**.
24. Définissez les variables suivantes. Pour chaque variable, vous devez choisir le niveau de portée approprié, en fonction du répertoire d'installation du collecteur de données sur les divers systèmes. Si les systèmes ont différents répertoires d'installation pour le collecteur de données, ces variables doivent être correctement définies pour chaque portée de niveau noeud. S'ils ont tous le même répertoire d'installation, la portée peut être plus élevée, par exemple au niveau cluster.
    - Définissez *ITCAMDCHOME* sur le répertoire suivant :
      - Linux AIX *rép_install*`/yndchome/7.3.0.14.08/itcamdc`
      - Windows *rép_install*`\dchome\7.3.0.14.08\itcamdc`
    - Définissez *ITCAMDCVERSION* sur la version du collecteur de données, par exemple, 7.3.0.14.08.
25. Cliquez sur **Appliquer**, puis sur **Sauvegarder**.

26. Dans la boîte de dialogue Sauvegarde dans la configuration principale, effectuez les opérations suivantes :
    - Si vous êtes dans un environnement de déploiement réseau, vérifiez que **Synchroniser les modifications avec les noeuds** est sélectionné, puis cliquez sur **Sauvegarder**.
    - Si vous n'êtes pas dans un environnement de déploiement réseau, cliquez sur **Sauvegarder**.

    Une fois le modèle modifié, les valeurs sont synchronisées avec toutes les instances de serveur du cluster dynamique. Tout nouveau serveur créé de manière dynamique aura les mêmes paramètres de configuration de collecteur de données.
27. Redémarrez l'instance de serveur d'applications pour le collecteur de données à activer. Le collecteur de données lit les fichiers de paramètres et crée le répertoire d'exécution.

Facultatif : Affichage du nom de machine virtuelle réel pour établir une distinction entre les membres du cluster

Pourquoi et quand exécuter cette tâche

Sur la console Cloud APM, le nom d'instance de l'Agent WebSphere Applications prend la forme *nom_hôte*:*nom_serveur_was*:KYNS et contient 32 caractères au maximum. Dans un environnement cluster dynamique, les noms de membre du cluster dynamique sont utilisés comme qualificateurs du milieu *nom_serveur_was*.

Il est possible que les noms de membre du cluster soient tronqués en raison du nombre maximal de caractères. Dans ce cas, vous pouvez indiquer le nom de machine virtuelle Java réel à utiliser comme qualificateur du milieu dans le nom d'instance d'agent.

Procédure

Pour afficher le nom de machine virtuelle réel dans le nom d'instance de l'agent, procédez comme suit :

1. Connectez-vous à la console d'administration WebSphere pour mettre à jour les arguments génériques de machine virtuelle Java en ajoutant une nouvelle variable d'environnement *${MEP_NAME}* de la manière suivante :

    ```
    -agentlib:am_$jvm-vendor_$jvm-version=${MEP_NAME}${WAS_SERVER_NAME}
    -Xbootclasspath/p:${ITCAMDCHOME}/toolkit/lib/bcm-bootstrap.jar
    -Djava.security.policy=${ITCAMDCHOME}/itcamdc/etc/datacollector.policy
    -verbosegc -Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=${ITCAMDCHOME}/runtime/
    $platform_Template_DCManualInput.txt
    -Dsun.rmi.dgc.client.gcInterval=3600000
    -Dsun.rmi.dgc.server.gcInterval=3600000
    -Dsun.rmi.transport.connectionTimeout=300000
    -Dws.bundle.metadata=${ITCAMDCHOME}/runtime/wsBundleMetaData
    –Ditcamdc.dyncluster=true
    ```

    Exemple :

    ```
    -agentlib:am_ibm_16=${MEP_NAME}${WAS_SERVER_NAME}
    -Xbootclasspath/p:${ITCAMDCHOME}/toolkit/lib/bcm-bootstrap.jar
    -Djava.security.policy=${ITCAMDCHOME}/itcamdc/etc/datacollector.policy
    -verbosegc
    -Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=${ITCAMDCHOME}/runtime/
    aix64_Template_DCManualInput.txt
    -Dsun.rmi.dgc.client.gcInterval=3600000
    -Dsun.rmi.dgc.server.gcInterval=3600000
    -Dsun.rmi.transport.connectionTimeout=300000
    -Dws.bundle.metadata=${ITCAMDCHOME}/runtime/wsBundleMetaData
    –Ditcamdc.dyncluster=true
    ```
2. Sauvegardez et appliquez les modifications.
3. Dans le panneau de navigation, cliquez sur **Environnement** > **Variables WebSphere** pour définir la variable *${MEP_NAME}* pour chaque membre du cluster dynamique. Définissez la valeur en indiquant le nom réel de machine virtuelle réel du membre du cluster.
4. Sauvegardez et appliquez les modifications.
5. Redémarrez l'instance du serveur d'applications.

La console Cloud APM affiche une nouvelle instance de l'Agent WebSphere Applications dont le nom contient la valeur *${MEP_NAME}* que vous venez d'indiquer.

Configuration dynamique de la collecte des données sur la page Configuration d'agent
Une fois que vous avez activé la prise en charge du suivi des transactions ou de la collecte des données de diagnostic dans le collecteur de données, utilisez la page **Configuration d'agent** pour activer ou désactiver la collecte des données de manière dynamique.

Avant de commencer

- Vous devez installer et configurer Monitoring Agent for WebSphere Applications.
- Pour activer ou désactiver le suivi des transactions pour les serveurs d'applications surveillés, vous devez installer Suivi des transactions. Vous devez également activer la prise en charge du suivi des transactions sur l'agent, comme décrit dans «Configuration du collecteur de données en mode interactif», à la page 864. Si vous suivez la procédure de configuration simple, le collecteur de données est automatiquement configuré avec la prise en charge du suivi des transactions.
- Pour activer ou désactiver la collecte des données de diagnostic et notamment la trace de méthode, vous devez posséder Cloud APM, Advanced. Vous devez également activer la prise en charge de la collecte des données de diagnostic et des informations de trace de méthode dans le collecteur de données, comme décrit dans «Configuration du collecteur de données en mode interactif», à la page 864. (Non disponible pour Cloud APM, Base).

Conseil : La page **Configuration d'agent** affiche tous les serveurs surveillés par l'agent. Si un serveur manque, il risque de ne pas être correctement surveillé. Recherchez les messages d'erreur, par exemple de connexion, dans les fichiers journaux d'agent sur le système surveillé.

A faire : L'Agent WebSphere Applications ne prend en charge que Db2 et Oracle comme source de données. Pour les autres types de source de données, certaines valeurs d'indicateur clé de performance pourraient apparaître comme nulles dans les tableaux de bord de suivi des transactions et les widgets de groupe.

Procédure

Pour configurer la collecte des données pour chaque serveur, procédez comme suit :

1. A partir de la barre de navigation, cliquez sur **Configuration système** > **Configuration d'agent**.
   La page **Configuration d'agent** s'affiche.
2. Cliquez sur l'onglet **WebSphere Applications**.
3. Cochez les cases des serveurs sur lesquels vous voulez configurer la collecte de données et effectuez l'une des actions suivantes de la liste **Actions** :
   - Pour activer le suivi des transactions, cliquez sur **Activer le suivi des transactions**. Le statut dans la colonne **Suivi des transactions en cours** est mis à jour et indique Oui pour chaque serveur sélectionné.
   - Pour activer uniquement la collecte des données de diagnostic, cliquez sur **Activer le mode diagnostic**. Le statut dans la colonne **Mode diagnostic en cours** est mis à jour et indique Oui pour chaque serveur sélectionné.
   - Pour collecter à la fois les données de diagnostic et les informations de trace de méthode, cliquez sur **Activer le mode diagnostic et la trace de méthode**. Le statut dans les colonnes **Mode diagnostic en cours** et **Trace de méthode en cours** est mis à jour et indique Oui pour chaque serveur sélectionné.
   - Pour désactiver le suivi des transactions pour le serveur sélectionné, cliquez sur **Désactiver le suivi des transactions**. Le statut dans la colonne **Suivi des transactions en cours** est mis à jour et indique Non pour chaque serveur sélectionné.
   - Si seule la collecte des données de diagnostic est activée pour le serveur sélectionné, pour désactiver la collecte des données, cliquez sur **Désactiver le mode diagnostic**. Le statut dans la colonne **Mode diagnostic en cours** est mis à jour et indique Non pour chaque serveur sélectionné.

- Si les données de diagnostic et les données de trace de méthode sont activées pour le serveur sélectionné, pour désactiver la collecte des données, cliquez sur **Désactiver le mode diagnostic et la trace de méthode**. Le statut dans les colonnes **Mode diagnostic en cours** et **Trace de méthode en cours** est mis à jour et indique Non pour chaque serveur sélectionné.

A faire :

- A moins que le support du suivi des transactions ou de la collecte des données de diagnostic soit configuré dans le collecteur de données, les opérations sur la page **Configuration d'agent** n'activent pas la collecte des données et la valeur de la colonne est définie sur Non.
- Si le profil du serveur d'applications a été configuré pour utiliser `127.0.0.1` comme nom d'hôte, la colonne **Adresse IP** de la page **Configuration d'agent** affiche l'adresse IP de l'hôte où l'Agent WebSphere Applications est installé et en cours d'exécution.

Résultats
Vous avez configuré la collecte des données pour chaque serveur sélectionné. Les données de suivi des transactions et de diagnostic peuvent être affichées dans les tableaux de bord de topologie une fois que vous avez activé la collecte de données.

Important : Si un serveur d'application redémarre, il se peut que vous deviez réactiver le suivi des transactions ou la collecte des données de diagnostic pour le serveur.

Activation de la surveillance des fuites de mémoire
Pour que le tableau de bord Analyse de mémoire contienne des données, vous devez activer la surveillance des fuites de mémoire pour le collecteur de données. Si le JRE qui est utilisé par le serveur d'applications est pris en charge, la fonction de surveillance des fuites de mémoire est activée par défaut une fois que vous avez activé la collecte de données de diagnostic.

Avant de commencer

- Assurez-vous que `-Xtrace:none` n'est pas défini dans les arguments JVM pour le serveur d'applications.
- Lorsque la fonction de surveillance des fuites de mémoire est activée, les paramètres suivants sont définis dans les arguments JVM pour le serveur d'applications. Si vous avez défini ces paramètres dans vos arguments JVM en cours, assurez-vous que la configuration du collecteur de données peut les modifier.

```
-Xhealthcenter:level=inprocess
-Xgc:allocationSamplingGranularity=10000
```

- Assurez-vous que le JRE qui est utilisé par le serveur d'applications est l'une des versions suivantes :
  - IBM JRE 1.6.0 SR16 FP3 ou version supérieure
  - IBM JRE 1.6.1 SR8 FP3 ou version supérieure
  - IBM JRE 1.7.0 SR8 FP10 ou version supérieure
  - IBM JRE 1.7.1 SR2 FP10 ou version supérieure
  - IBM JRE 1.8 ou version supérieure
  - Autre IBM JRE d'une version supérieure à 1.6.0 SR7 avec le correctif temporaire pour l'APAR IV67574

Pourquoi et quand exécuter cette tâche

La fonction de surveillance des fuites de mémoire nécessite le composant IBM Health Center du JRE d'IBM. Vous devez vous assurer que le JRE qui est utilisé par le serveur d'applications est pris en charge par cette fonction.

- Sur les systèmes AIX ou Linux, lorsque vous configurez le collecteur de données de façon à activer la collecte de données de diagnostic, si le JRE en cours est pris en charge, l'utilitaire de configuration

vérifie automatiquement si le composant Health Center est admissible et le met à niveau s'il ne l'est pas.

- Sur les systèmes Windows, vous devez mettre à niveau le composant Health Center manuellement si la version en cours n'est pas prise en charge car l'utilitaire de configuration ne peut pas remplacer les fichiers pour un JRE en cours d'exécution.

A faire : La procédure suivante est requise uniquement sur les systèmes Windows. Pour les systèmes AIX ou Linux, pour activer la surveillance des fuites de mémoire, vous devez uniquement vous assurer que la version du JRE est prise en charge et que la collecte des données de diagnostic est activée. Pour les systèmes Solaris, le Centre de santé d'IBM JRE n'est pas pris en charge de sorte que la surveillance des fuites de mémoire ne peut pas être activée sur ces systèmes.

Procédure

1. Vérifiez que la version d'IBM Health Center qui est incluse dans le JRE est utilisée par le serveur d'applications.
   a) A l'invite de commande, accédez au répertoire `bin` qui se trouve dans le répertoire de base du JRE.
   b) Entrez `java -Xhealthcenter -version` et appuyez sur Entrée.

   La commande renvoie la version du JRE, ainsi que la version d'IBM Health Center. La fonction de surveillance des fuites de mémoire nécessite IBM Health Center version 3.0.11 ou supérieure.
2. Si la version d'IBM Health Center n'est pas admissible, effectuez une mise à niveau du JRE vers une version qui contient IBM Health Center version 3.0.11 ou supérieure.
3. Exécutez l'utilitaire de configuration ou de reconfiguration du collecteur de données pour activer la collecte de données de diagnostic.
   - Si vous n'avez pas configuré le collecteur de données, utilisez `simpleconfig` ou `config`.
   - Si vous avez configuré le collecteur de données, utilisez l'utilitaire `reconfig`.

   A faire : Si vous avez activé la collecte de données de diagnostic avant la mise à niveau du JRE, vous devez toujours exécuter de nouveau l'utilitaire de configuration de la collecte de données.

Configuration de l'infrastructure PMI
Pour afficher les données de performances dans des tableaux de bord de surveillance opérationnelle, l'infrastructure PMI (Performance Monitoring Infrastructure) de WebSphere Application Server doit être configurée pour collecter les données de performances.

Pourquoi et quand exécuter cette tâche

Utilisez la console d'administration WebSphere pour activer l'infrastructure PMI et définir le niveau PMI sur le système WebSphere Application Server.

L'infrastructure PMI fournit quatre niveaux prédéfinis suivants :

1. Aucun
2. De base
3. Etendu
4. Tous

Vous pouvez utiliser une option personnalisée pour sélectionner les statistiques individuelles que vous souhaiter activer ou désactiver. Chaque niveau inclut les statistiques du niveau immédiatement inférieur.

Pour afficher les données dans les tableaux de bord de surveillance des ressources, les attributs utilisés pour les calculs associés au tableau de bord doivent être inclus dans le niveau sélectionné.

Par défaut, l'Agent WebSphere Applications définit le niveau de l'infrastructure PMI à un niveau suffisamment élevé pour collecter les attributs obligatoires.

Restriction : Pour afficher les données dans certains widgets de groupe Process Server et Transaction Manager, vous devez définir manuellement le niveau PMI. Pour plus d'informations, consultez l'infobulle relative aux widgets de groupe.

Si vous modifiez le niveau PMI dans la console d'administration WebSphere, vous devez vérifier que le niveau est suffisamment élevé pour permettre la collecte des données requises.

Procédure

- Pour activer l'infrastructure PMI sur le serveur d'applications, procédez comme suit :
  a) Dans la console d'administration WebSphere, développez **Surveillance et optimisation**, puis sélectionnez **PMI (Performance Monitoring Infrastructure)**.
  b) Dans la liste des serveurs, cliquez sur le nom de votre serveur.
  c) Cliquez sur l'onglet Configuration, puis cochez la case **Activation de l'infrastructure PMI**.
  d) Cliquez sur **Appliquer** ou sur **OK**.
  e) Cliquez sur **Sauvegarder** pour activer l'infrastructure PMI.
- Pour définir l'infrastructure PMI sur le serveur d'applications, procédez comme suit :
  a) Dans la console d'administration WebSphere, développez **Surveillance et optimisation**, puis sélectionnez **Infrastructure PMI**.
  b) Dans la liste des serveurs, cliquez sur le nom de votre serveur.
  c) Cliquez sur l'onglet Configuration et sélectionnez ensuite l'ensemble de statistiques à utiliser : de base, étendu, tous ou personnalisé.
  d) Cliquez sur **Appliquer** ou sur **OK**.
  e) Cliquez sur **Sauvegarder** pour définir le niveau PMI.

  Pour plus d'informations sur le niveau PMI requis pour chaque attribut, voir la section "Dashboard attributes" dans le manuel Agent WebSphere Applications Reference. Les frais généraux de surveillance engendrés par l'activation de la collecte de chaque attribut sont affichés.

Restauration de la configuration du serveur d'applications depuis une sauvegarde
Si vous avez configuré une instance de serveur d'applications autonome pour la collecte de données, manuellement ou à l'aide de l'utilitaire de configuration ou de migration, et que le démarrage du serveur d'applications échoue, vous devez restaurer la configuration du serveur d'applications à partir d'une sauvegarde. Si vous n'avez pas créé de sauvegarde, contactez le support IBM.

Pourquoi et quand exécuter cette tâche

Dans un environnement Network Deployment, si vous avez configuré une instance de serveur d'applications pour la collecte de données manuellement ou avec l'utilitaire de migration ou de configuration et que le démarrage du serveur d'applications échoue, vous disposez des options suivantes :

- Vous pouvez restaurer la configuration du serveur d'applications à partir d'une configuration de sauvegarde. Si vous n'avez pas créé de sauvegarde, contactez le support IBM.
- Vous pouvez annuler manuellement la configuration du collecteur de données. Le gestionnaire de déploiement et l'agent de noeud doivent être démarrés sur le serveur d'applications. Pour plus d'informations, voir «Suppression manuelle de la configuration du collecteur de données depuis une instance de serveur d'applications», à la page 156.

Cette section concerne uniquement les systèmes d'exploitation Windows, UNIX et Linux.

Procédure

Pour appliquer la configuration de sauvegarde à l'aide de la commande **`restoreConfig`**, utilisez l'une des procédures suivantes :

- Dans un environnement de déploiement hors réseau, exécutez les étapes suivantes :
  a) Recherchez le fichier de configuration sauvegardé.

  Le répertoire par défaut est *rép_principal_cd*`/data`. S'il existe plusieurs fichiers de sauvegarde, vérifiez la date et l'heure de modification du fichier. Celui-ci doit porter la date et

l'heure de la configuration qui a échoué. Si vous n'avez terminé aucune autre configuration de collecteur de données sur le même hôte après l'échec de la configuration, utilisez le fichier le plus récent dans le répertoire.

b) Arrêtez toutes les instances du serveur d'applications.

c) Exécutez la commande **restoreConfig** à partir du répertoire *rép_principal_serveur_app*/profiles/*nom_profil*/bin.

La syntaxe de la commande est la suivante :

– Windows `restoreConfig.bat` *chemin_complet_vers_fichier_sauvegarde*

– Linux AIX `./restoreConfig.sh` *chemin_complet_vers_fichier_sauvegarde*

Pour plus d'informations sur les arguments de la commande **restoreConfig**, voir la rubrique correspondante dans le Knowledge Center WebSphere Application Server.

d) Redémarrez les instances du serveur d'applications.

- Dans un environnement de déploiement réseau, effectuez les étapes suivantes :

a) Recherchez le fichier de configuration sauvegardé.

Le répertoire par défaut est *rép_principal_cd*/data. S'il existe plusieurs fichiers de sauvegarde, vérifiez les date et heure de modification du fichier, qui doivent correspondre à celles de la configuration ayant échoué. Si vous n'avez terminé aucune autre configuration de collecteur de données sur le même hôte après l'échec de la configuration, utilisez le fichier le plus récent dans le répertoire.

b) Arrêtez toutes les instances du serveur d'applications.

c) Créez un répertoire temporaire dans n'importe quel chemin d'accès commode (*rép_temporaire*). Sur un système UNIX ou Linux, créez le répertoire temporaire sous le répertoire /tmp.

d) Exécutez la commande restoreConfig à partir du répertoire *rép_principal_serveur_app*/profiles/*nom_profil*/bin.

La syntaxe de la commande est la suivante :

– Windows `restoreConfig.bat` *chemin_complet_vers_fichier_sauvegarde*

– Linux AIX `./restoreConfig.sh` *chemin_complet_vers_fichier_sauvegarde*

La commande **restoreConfig** restaure la configuration du serveur d'applications d'origine dans le répertoire temporaire.

e) Copiez les fichiers server.xml, variables.xml et pmi-config.xml du répertoire temporaire dans le système Deployment Manager.

– Répertoire source : *répertoire_temp*/*rép_principal_configuration_restaurée*/cells/*nom_cellule*/nodes/*nom_noeud*/servers/*nom_serveur*

– Répertoire cible : *rép_principal_serveur_app*/profiles/*nom_profil*/config/cells/*nom_cellule*/nodes/*nom_noeud*/servers/*nom_serveur*

f) Effectuez une synchronisation de noeud à partir de la console d'administration du gestionnaire de déploiement associée au noeud.

g) Dans la console d'administration du gestionnaire de déploiement, sauvegardez les modifications dans la configuration principale.

h) Démarrez les instances du serveur d'applications.

Configuration du collecteur de données Liberty pour les applications sur site

Pour surveiller le profil Liberty sous Linux for System x, vous pouvez déployer directement un collecteur de données autonome dans votre répertoire Liberty local, sans installer Agent WebSphere Applications.

Avant de commencer

1. Téléchargez le module du collecteur de données `IBM_Data_Collectors_Install.tgz` à partir du site Web IBM Passport Advantage. Pour des instructions détaillées, consultez le site Web «Téléchargement de vos agents et de vos collecteurs de données», à la page 105.
2. Si vos règles de pare-feu n'autorisent pas les connexions HTTPS sortantes transparentes à des hôtes externes, vous pouvez configurer les collecteurs de données pour l'envoi du trafic à un proxy direct. Pour obtenir des instructions, voir «Configuration des collecteurs de données pour qu'ils communiquent via un proxy direct», à la page 167.
3. La fonction monitor-1.0 est requise par le collecteur de données. Vous pouvez télécharger cette fonction à partir du référentiel de fonctions Liberty à l'aide de la commande **`installUtility`**. Pour des instructions, consultez la section relative au téléchargement des actifs dans WebSphere Application Server Network Deployment Knowledge Center.
4. Pour que le tableau de bord Analyse de mémoire contienne des données, vous devez activer la collecte d'allocation de mémoire pour le collecteur de données au cours de la configuration. Cette fonction de diagnostic requiert IBM Health Center 3.0.8 ou version ultérieure. Si la version d'IBM Health Center n'est pas éligible, mettez à niveau l'environnement JRE utilisé par le serveur d'applications vers une version contenant IBM Health Center 3.0.8 ou version ultérieure.

   Conseil : Pour vérifier la version d'IBM Health Center incluse dans l'environnement JRE utilisé par le serveur d'applications, accédez au répertoire `bin` dans le répertoire de base JRE et lancez ensuite `java -Xhealthcenter -version`.

Pourquoi et quand exécuter cette tâche

Vous pouvez choisir de configurer manuellement le collecteur de données ou d'utiliser le script de configuration fourni pour configurer le collecteur de données.

Procédure

- Pour configurer manuellement le collecteur de données, extrayez les fichiers du collecteur de données du module de collecteur de données, puis modifiez des fichiers locaux pour le serveur Liberty.
  a) Exécutez la commande suivante pour extraire les fichiers du package de collecteur de données :

  ```
  tar -xzf IBM_Data_Collectors_Install.tgz
  ```

  Le module `liberty_datacollector_8.1.4.0.tgz` est inclus dans le répertoire extrait.

  b) Extrayez les fichiers du module `liberty_datacollector_8.1.4.0.tgz` dans un répertoire local à l'aide de la commande ci-dessous. Le répertoire extrait devient le répertoire de base du collecteur de données.

  ```
  tar -xzf liberty_datacollector_8.1.4.0.tgz
  ```

  Par exemple, pour extraire les fichiers dans le répertoire `/opt/ibm/apm/`, exécutez les commandes suivantes :

  ```
  cd /opt/ibm/apm
  tar -xzf liberty_datacollector_8.1.4.0.tgz
  ```

  Les fichiers extraits se trouvent dans le répertoire `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.08`. Ce répertoire est appelé répertoire de base du collecteur de données (*base_cd*) dans les étapes ci-après.

  c) Accédez au répertoire de base du serveur Liberty. Par exemple, `/opt/ibm/wlp/usr/servers/defaultServer`.

d) Editez le fichier `jvm.options` en ajoutant les paramètres ci-après. Si le fichier `jvm.options` n'existe pas, créez-le avec un éditeur de texte.

```
-agentlib:am_ibm_16=nom_serveur
-Xbootclasspath/p:base_cd/toolkit/lib/bcm-bootstrap.jar
-Djava.security.policy=base_cd/itcamdc/etc/datacollector.policy
-Dliberty.home=base_liberty
-Xhealthcenter:level=inprocess
-Xgc:allocationSamplingGranularity=10000
-verbosegc
-Xverbosegclog:chemin_accès_absolu_au_fichier_journal,1,10000
```

Lors de l'ajout de ces entrées, notez ce qui suit :

- Chaque entrée doit se trouver sur une ligne distincte.
- Remplacez *nom_serveur* par le nom du serveur Liberty.
- Remplacez *base_cd* par le répertoire de base du collecteur de données. Par exemple, `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.08`.
- Remplacez *base_liberty* par la racine du répertoire d'installation Liberty. Par exemple, `/opt/ibm/wlp`.
- Si le serveur Liberty fonctionne avec une lourde charge de travail, ajoutez le paramètre `-Xmx` pour allouer une taille de segment de mémoire de 512 Mo supplémentaire pour le collecteur de données. Par exemple, `-Xmx1024M`.
- Les lignes `-Xhealthcenter:level=inprocess` et `-Xgc:allocationSamplingGranularity=10000` sont facultatives. Ajoutez les deux lignes uniquement si vous souhaitez activer la collecte d'allocation de mémoire qui est désactivée par défaut. L'activation de cette fonction est nécessaire pour que le tableau de bord Analyse de mémoire contienne des données.
- La ligne `-Xverbosegclog:`*chemin_accès_absolu_au_fichier_journal*`,1,10000` est facultative ; elle indique le chemin d'accès au fichier journal de récupération de place redirigé. Si elle n'est pas indiquée, les journaux sont enregistrés dans un fichier qui est renouvelé tous les 10000 échecs d'allocation. Le fichier `stdout` ou `stderr` d'origine (`console.log`) peut être très volumineux lors de l'exécution du serveur. Ajoutez cette ligne si vous souhaitez sauvegarder les fichiers journaux de sortie de récupération de place dans un autre répertoire et limiter le nombre et la taille des fichiers journaux. Si le chemin d'accès indiqué n'est pas valide, cette ligne n'a pas d'effet et le fichier journal de récupération de place reste le fichier `stdout` ou `stderr`.

e) Ouvrez le fichier `server.env` dans le même répertoire et ajoutez le chemin ci-après à l'entrée d'environnement. Si le fichier `server.env` n'existe pas, créez-le avec un éditeur de texte.

```
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/lib:base_cd/toolkit/lib/lx8266:base_cd/
toolkit/lib/lx8266/ttapi
```

Lors de l'ajout de ces entrées, notez ce qui suit :

- Chaque entrée doit se trouver sur une ligne distincte.
- Remplacez *base_cd* par le répertoire de base du collecteur de données. Par exemple, `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.08`.

f) Modifiez le fichier `server.xml` dans le même répertoire pour activer la fonction de surveillance en ajoutant la ligne suivante à la section `<featureManager>` :

```
<feature>monitor-1.0</feature>
```

g) Redémarrez le serveur Liberty.

- Pour configurer le collecteur de données en répondant à des invites, utilisez le script de configuration fourni dans les packages de collecteur de données.

a) Exécutez la commande suivante pour extraire les fichiers du package de collecteur de données :

```
tar -xzf IBM_Data_Collectors_Install.tgz
```

Le module `liberty_datacollector_8.1.4.0.tgz` est inclus dans le répertoire extrait.

b) Extrayez les fichiers du module `liberty_datacollector_8.1.4.0.tgz` à l'aide de la commande ci-dessous.

```
tar -xzf liberty_datacollector_8.1.4.0.tgz
```

Par exemple,

```
cd /opt/ibm
tar -xzf liberty_datacollector_8.1.4.0.tgz
```

Les fichiers du collecteur de données extraits se trouvent dans le répertoire `liberty_dc`.

c) Accédez au répertoire `liberty_dc/.gdc/7.3.0.14.08/bin` et démarrez le script de configuration en exécutant la commande suivante :

```
./config_liberty_dc.sh
```

d) A l'invite de commande, entrez la racine de votre répertoire d'installation Liberty ou acceptez la valeur par défaut. Par exemple, `/opt/ibm/wlp`.

e) A l'invite, entrez le répertoire de base de la machine virtuelle Java qui est utilisé par le serveur d'applications ou acceptez le répertoire par défaut. Par exemple, `/opt/ibm/java`.

f) Le programme de configuration peut reconnaître et répertorier automatiquement les serveurs d'applications non configurés dans le répertoire spécifié. Entrez le numéro qui correspond au serveur Liberty à configurer. Pour sélectionner plusieurs serveurs, séparez les numéros par un espace ou entrez * pour sélectionner tous les serveurs.

g) Une fois que le programme de configuration a terminé de mettre à jour les fichiers de tous les serveurs Liberty, mettez à jour manuellement la taille de segment de mémoire de JVM afin d'allouer un segment de mémoire supplémentaire de 512 Mo pour le collecteur de données.

h) Redémarrez les serveurs pour que la configuration soit prise en compte.

Résultats

Le collecteur de données est configuré et il est connecté au serveur Cloud APM. La surveillance des ressources, le suivi des transactions et les données de diagnostic sont activées. Toutefois, la collecte de segments de mémoire et la collecte d'allocation de mémoire sont désactivées. Vous pouvez les activer avec les fichiers de propriétés du collecteur de données si vous avez besoin des données contenues dans les tableaux de bord Cliché de tas et Analyse de mémoire.

Que faire ensuite

- Pour afficher les données de surveillance de vos serveurs Liberty, démarrez la console Cloud APM. Pour les instructions, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.

  A faire : Lorsque vous ajoutez l'instance de collecteur de données Liberty sur le Tableau de bord des applications, sélectionnez **Liberty Runtime** au lieu de **WebSphere Application Server** dans la liste des composants.
- Pour que les tableaux de bord Cliché de tas et/ou Analyse de mémoire contiennent des données, vous devez également activer la collecte des données pour le collecteur d'instantané de segment de mémoire et/ou la collecte d'allocation de mémoire, ce qui est faisable dans les fichiers `.properties` du collecteur de données. Voir «Activation ou désactivation de la collecte des données de suivi des transactions et des données de diagnostic», à la page 918 .
- Si le fichier de clés ou le serveur Cloud APM est modifié, reconnectez le collecteur de données au serveur Cloud APM. Pour obtenir des instructions, voir «Reconnexion du collecteur de données au serveur Cloud APM», à la page 190.

Annulation de la configuration du collecteur de données pour les applications sur site
Si vous n'avez pas besoin de surveiller vos serveurs Liberty ou si vous souhaitez mettre à niveau le collecteur de données vers une nouvelle version, vous devez annuler la configuration du collecteur de données que vous avez déployé sur le serveur Liberty.

Pourquoi et quand exécuter cette tâche

Pour annuler la configuration du collecteur de données déployé sur le serveur Liberty, annulez les modifications apportées lors de la configuration du collecteur de données. Vous pouvez choisir de configurer le collecteur de données manuellement ou avec le script `unconfig_liberty_dc` fourni.

Procédure

- Pour annuler manuellement la configuration du collecteur de données, procédez comme suit :
  a) Accédez au répertoire de base du serveur Liberty. Par exemple, `/opt/ibm/wlp/usr/servers/defaultServer`.
  b) Modifiez le fichier `jvm.options` pour supprimer les paramètres ci-dessous.

```
-agentlib:am_ibm_16=nom_serveur
-Xbootclasspath/p:base_cd/toolkit/lib/bcm-bootstrap.jar
-Djava.security.policy=base_cd/itcamdc/etc/datacollector.policy
-Dliberty.home=base_liberty
-Xhealthcenter:level=inprocess
-Xgc:allocationSamplingGranularity=10000
-verbosegc
-Xverbosegclog:chemin_accès_absolu_au_fichier_journal,1,10000
```

  c) Modifiez le fichier `server.env` dans le même répertoire pour supprimer la valeur suivante pour **LD_LIBRARY_PATH**

```
/lib:base_cd/toolkit/lib/lx8266:base_cd/toolkit/lib/lx8266/ttapi
```

  où *base_cd* est le répertoire de base du collecteur de données. Par exemple, `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.08`.
  d) Modifiez le fichier `server.xml` dans le même répertoire pour supprimer `<feature>monitor-1.0</feature>` de la section `<featureManager>`.
  e) Redémarrez le serveur Liberty.
- Pour annuler la configuration du collecteur de données avec le script `unconfig_liberty_dc.sh`, procédez comme suit :
  a) Accédez au répertoire *base_cd*`/bin`. Par exemple, `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.08/bin`.
  b) Démarrez le script d'annulation de configuration en exécutant la commande suivante :

```
./unconfig_liberty_dc.sh
```

  c) A l'invite de commande, entrez la racine de votre répertoire d'installation Liberty ou acceptez la valeur par défaut. Par exemple, `/opt/ibm/wlp`.
  d) Le programme d'annulation de configuration peut reconnaître et répertorier automatiquement les serveurs d'applications configurés dans le répertoire spécifié. Entrez le numéro qui correspond au serveur Liberty dont vous souhaitez annuler la configuration. Pour sélectionner plusieurs serveurs, séparez les numéros par un espace ou entrez * pour sélectionner tous les serveurs.
  e) Une fois que le programme d'annulation de configuration a fini de mettre à jour les fichiers de tous les serveurs Liberty, redémarrez les serveurs pour que les modifications soient prises en compte.

Que faire ensuite

Une fois que vous avez configuré le collecteur de données, la console Cloud APM continue d'afficher le collecteur de données dans les applications auxquelles vous l'avez ajouté. La console Cloud APM indique qu'aucune donnée n'est disponible pour l'application et n'indique pas que le collecteur de données est

hors ligne. Pour plus d'informations sur la manière de supprimer le collecteur de données d'applications et de groupes de ressources, voir «Suppression de collecteurs de données de la console Cloud APM», à la page 193.

Vous pouvez également supprimer le répertoire de base du collecteur de données si vous n'en avez plus besoin.

Configuration du collecteur de données Liberty pour les applications IBM Cloud

Pour surveiller un profil Liberty exécuté dans l'environnement IBM Cloud, vous devez télécharger le package du collecteur de données à partir d'IBM Marketplace, déployer le collecteur de données sur vos fichiers d'application locaux, puis envoyer les mises à jour à IBM Cloud.

Avant de commencer

On suppose que l'application Liberty est envoyée à l'environnement IBM Cloud à l'aide des commandes Cloud Foundry. Le fichier `manifest.yml` et le répertoire de base Liberty (qui contient le fichier `server.xml`) existe déjà.

Si votre application Liberty est déployée sous forme de fichier WAR, vous devez modifier certains fichiers locaux de façon à mettre à jour l'application en envoyant un répertoire local contenant le fichier WAR et les fichiers de collecteur de données. Un exemple expliquant comment obtenir un répertoire principal de serveur Liberty local lorsque vous disposez uniquement du fichier WAR est fourni ici.

1. Exécutez la commande suivante pour exécuter l'application Liberty en local :

   ```
   mvn install liberty:run-server
   ```

   Dans le répertoire qui contient le fichier WAR Liberty, un sous-répertoire `/liberty/wlp/usr/servers/defaultServer` est créé. Ce répertoire peut servir de répertoire principal de serveur Liberty dans la procédure suivante.
2. Dans le répertoire racine qui contient le fichier WAR Liberty, copiez le dossier entier *nom_application*-SNAPSHOT dans le répertoire `/liberty/wlp/usr/servers/defaultServer`.
3. Dans le répertoire `/liberty/wlp/usr/servers/defaultServer`, éditez le fichier `bootstrap.properties` de façon à modifier le chemin **appLocation**. Le chemin **appLocation** doit être défini sur le chemin relatif du répertoire de l'application dans IBM Cloud.
4. Supprimez les dossiers `logs` et `workarea`. Il n'est pas nécessaire de les envoyer dans IBM Cloud.
5. Modifiez la valeur de **path** dans le fichier `manifest.yml` de façon à ce qu'elle pointe vers le répertoire `defaultServer`.

   Par exemple, `path: target/liberty/wlp/usr/servers/defaultServer`.

Procédure

Pour configurer le collecteur de données Liberty, procédez comme suit :

1. Téléchargez le module du collecteur de données `IBM_Data_Collectors_Install.tgz` à partir de IBM Marketplace. Pour des instructions détaillées, voir «Téléchargement de vos agents et de vos collecteurs de données», à la page 105.
2. Exécutez la commande suivante pour extraire les fichiers du module de collecteur de données :

   ```
   tar -xzf IBM_Data_Collectors_Install.tgz
   ```

   Le module `liberty_datacollector_8.1.4.0.tgz` est inclus dans le répertoire extrait.
3. Extrayez les fichiers à partir du module `liberty_datacollector_8.1.4.0.tgz` dans un répertoire temporaire.

   ```
   tar -xzf liberty_datacollector_8.1.4.0.tgz
   ```

   Par exemple,

```
cd /root/tmp
tar -xzf liberty_datacollector_8.1.4.0.tgz
```

Vous pouvez rechercher les fichiers extraits dans le répertoire `liberty_dc` dans le répertoire temporaire.

4. Copiez le répertoire `.gdc` du répertoire `liberty_dc` dans le répertoire de base de votre serveur Liberty sur lequel le fichier `server.xml` est stocké. Le répertoire de base du serveur Liberty est appelé *rép_principal_serveur_liberty* dans les étapes ci-après.

```
cp -rf rép_temp/liberty_dc/.gdc rép_principal_serveur_liberty
```

Par exemple,

```
cp -rf /root/tmp/liberty_dc/.gdc /opt/liberty855/wlp/usr/servers/defaultServer/
```

5. Copiez ou fusionnez le contenu des fichiers `jvm.options` et `server.env` du répertoire `liberty_dc/etc` dans le répertoire *rép_principal_serveur_liberty*.
   - Si les fichiers `jvm.options` et `server.env` ne se trouvent pas dans le répertoire *rép_principal_serveur_liberty*, copiez-les de *rép_temp*`/liberty_dc/etc` dans *rép_principal_serveur_liberty*.

     ```
     cp rép_temp/liberty_dc/etc/jvm.option rép_principal_serveur_liberty
     cp rép_temp/liberty_dc/etc/server.env rép_principal_serveur_liberty
     ```

   - Si le fichier `jvm.options` ou `server.env` existe dans le répertoire *rép_principal_serveur_liberty*, fusionnez son contenu avec les fichiers du répertoire *rép_temp*`/liberty_dc/etc`.
6. Si vos applications IBM Cloud ne peuvent pas se connecter directement au serveur Cloud APM en raison des paramètres de réseau ou de pare-feu, configurez le collecteur de données pour l'envoi du trafic par le biais d'un proxy direct. Pour cela, modifiez le fichier `jvm.options` de l'une des manières suivantes :
   - Si l'authentification n'est pas requise, ajoutez les lignes suivantes au fichier :

     ```
     -Dhttp.proxyHost=hôte_proxy_http
     -Dhttp.proxyPort=port_proxy_http
     -Dhttps.proxyHost=hôte_proxy_http
     -Dhttps.proxyPort=port_proxy_http
     -Djava.net.useSystemProxies=true
     ```

   - Si un nom d'utilisateur et un mot de passe sont requis pour accéder au serveur proxy direct, ajoutez les lignes suivantes au fichier :

     ```
     -Dhttp.proxyHost=hôte_proxy_http
     -Dhttp.proxyPort=port_proxy_http
     -Dhttp.proxyUser=utilisateur_proxy_http
     -Dhttp.proxyPassword=mot_de_passe_proxy_http
     -Dhttps.proxyHost=hôte_proxy_http
     -Dhttps.proxyPort=port_proxy_http
     -Dhttps.proxyUser=utilisateur_proxy_http
     -Dhttps.proxyPassword=mot_de_passe_proxy_http
     -Djava.net.useSystemProxies=true
     ```

7. Modifiez le fichier `server.xml` dans le répertoire de base du serveur Liberty pour activer la fonction de surveillance en ajoutant la ligne suivante à la section `<featureManager>` :

```
<featureManager>
              <feature>monitor-1.0</feature>
</featureManager>
```

8. Modifiez le fichier `manifest.yml` de votre application Liberty pour allouer 512 Mo de mémoire supplémentaire.
9. Ouvrez une invite de commande et accédez au répertoire local qui contient le fichier `manifest.yml` pour le serveur Liberty. Par exemple, `/opt/liberty855/`.
10. Connectez-vous à IBM Cloud et mettez à jour le profil Liberty avec la commande **cf push**.

Résultats
Le collecteur de données est configuré et il est connecté au serveur Cloud APM. La surveillance des ressources, le suivi des transactions et les données de diagnostic sont activées. Toutefois, la collecte de segments de mémoire et la collecte d'allocation de mémoire sont désactivées. Vous pouvez les activer avec les fichiers de propriétés du collecteur de données si vous avez besoin des données contenues dans les tableaux de bord Cliché de tas et Analyse de mémoire.

Que faire ensuite

- Pour afficher les données de surveillance de votre application IBM Cloud, démarrez la console Cloud APM. Pour les instructions, voir Démarrage de la console Cloud APM. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir Gestion des applications.

  A faire : Si vous souhaitez ajouter l'instance de collecteur de données Liberty sur le Tableau de bord des applications, sélectionnez **Liberty Runtime** au lieu de **WebSphere Application Server** dans la liste des composants.
- Pour que les tableaux de bord Cliché de tas et/ou Analyse de mémoire contiennent des données, vous devez également activer la collecte des données pour le collecteur d'instantané de segment de mémoire et/ou la collecte d'allocation de mémoire, ce qui est faisable dans les fichiers `.properties` du collecteur de données. Voir «Personnalisation du collecteur de données avec des fichiers de propriétés», à la page 914 .
- Si le fichier de clés ou le serveur Cloud APM est modifié, reconnectez le collecteur de données au serveur Cloud APM. Pour obtenir des instructions, voir «Reconnexion du collecteur de données au serveur Cloud APM», à la page 190.

Variables d'environnement pour la personnalisation du collecteur de données Liberty
Pour personnaliser le collecteur de données Liberty pour les applications IBM Cloud, utilisez l'interface utilisateur IBM Cloud pour ajouter les variables d'environnement prises en charge par le collecteur de données.

Conseil : Pour ajouter des variables d'environnement dans l'interface utilisateur IBM Cloud, connectez-vous d'abord à l'interface utilisateur IBM Cloud, puis cliquez sur votre application et sur **Exécution** > **Variable d'environnement**. Dans la section **définie par l'utilisateur**, ajoutez les variables d'environnement.

- Utilisez les variables répertoriées dans la rubrique Tableau 228, à la page 912 pour configurer la connexion entre le collecteur de données Liberty et le serveur Cloud APM.
- Utilisez la variable répertoriée dans Tableau 229, à la page 913 pour activer ou désactiver la trace de méthode pour vos applications IBM Cloud.
- Après avoir activé la méthode de traçage, utilisez les variables répertoriées dans Tableau 230, à la page 914 pour indiquer des seuils pour les différents types de demande, afin que des niveaux différents de données de surveillance puissent être collectés.

A faire : Après avoir ajouté ou modifié la variable d'environnement, redémarrez votre application pour que les modifications soient prises en compte.

Tableau 228. Variables d'environnement pour les connexions serveur

Nom de la variable	Valeurs admises	Description
APM_BM_GATEWAY_URL	• `https://` *`IP_ou_nom_d'hôte_du_serveur`*`:443` • `http://` *`IP_ou_nom_d'hôte_du_serveur`*`:80`	URL de la passerelle du serveur Cloud APM cible.

Tableau 228. Variables d'environnement pour les connexions serveur (suite)		
Nom de la variable	**Valeurs admises**	**Description**
APM_KEYFILE_PSWD	Mot de passe chiffré du fichier de clés	Le mot de passe chiffré du fichier de clés qui est apparié avec le fichier de clés. Si vous êtes un utilisateur Linux, vous pouvez utiliser la commande `echo -n <mot de passe du fichier de clés> | base64` pour chiffrer votre mot de passe. **A faire :** Définissez cette variable uniquement lorsque vous avez configuré la variable *APM_BM_GATEWAY_URL* pour utiliser HTTPS.
APM_KEYFILE_URL	`http://serveur_http_hébergé:port/keyfile.jks`	L'URL de téléchargement du fichier de clés. **A faire :** Définissez cette variable uniquement lorsque vous avez configuré la variable *APM_BM_GATEWAY_URL* pour utiliser HTTPS.

Tableau 229. Variable d'environnement pour la trace de méthode		
Nom de la variable	**Valeurs admises**	**Description**
METHOD_TRACE_ENABLE	• `true` • `false`	Cette variable permet d'activer ou de désactiver la méthode de traçage. La valeur `true` active cette fonction. La valeur par défaut est `false`.

Une fois que la trace de méthode a été activée, vous pouvez configurer des seuils pour les différents types de demande de façon à personnaliser la trace de méthode. Les méthodes suivantes, qui déclenchent la collecte de différents niveaux de données de surveillance, peuvent être configurées pour chaque type de demande :

Seuils principaux
Si vous configurez le seuil principal pour un type de demande, les informations temporelles de ce type de demande, telles que le temps UC et le temps de réponse, sont capturées. Par conséquent, si l'exécution d'une demande prend plus de temps que la durée spécifiée pour le seuil principal, le temps de la demande est capturé.

Seuils secondaires
Si vous configurez le seuil secondaire pour un type de demande, des données contextuelles approfondies sont capturées, par exemple les traces de pile et le code SQL pour les requêtes de base de données. Les données contextuelles capturées varient en fonction du type de demande. Si l'exécution d'une demande prend plus de temps que la valeur de seuil indiquée pour le seuil secondaire, ses données contextuelles sont capturées.

La variable d'environnement des différents seuils de demande est nommée *<type_demande>_<niveau seuil>*. Par exemple, pour configurer un seuil principal pour la demande JMS, ajoutez la variable JMS_PRIMARY et définissez sa valeur.

Le Tableau 230, à la page 914 répertorie les variables d'environnement correspondantes que vous pouvez ajouter pour les différents types de demande. Les valeurs sont exprimées en millisecondes.

Tableau 230. Variables d'environnement pour les différents seuils de demande	
Nom de la variable	**Valeur par défaut (en millisecondes)**
SERVLET_PRIMARY	20
SERVLET_SECONDARY	50
JDBC_PRIMARY	20
JDBC_SECONDARY	50
JNDI_PRIMARY	20
JNDI_SECONDARY	50
EJB_PRIMARY	20
EJB_SECONDARY	50
WEBSERVICES_PRIMARY	20
WEBSERVICES_SECONDARY	50
APP_METHODS_PRIMARY (méthodes d'application – non J2EE)	50
APP_METHODS _SECONDARY	1000
JCA_PRIMARY	50
JCA_SECONDARY	80
JMS_PRIMARY	40
JMS_SECONDARY	70

Personnalisation du collecteur de données avec des fichiers de propriétés
Par défaut, le suivi des transactions et des méthodes est activé pour le collecteur de données. La collecte des instantanés de segment de mémoire et la collecte d'allocation de mémoire sont désactivées. Vous pouvez personnaliser la collecte de données ou les intervalles auxquels les données de diagnostic sont collées en modifiant les fichiers `.properties` du collecteur de données.

Pourquoi et quand exécuter cette tâche

Les fichiers de propriétés du collecteur de données sont dans le répertoire *base_cd*, par exemple `/opt/liberty855/wlp/usr/servers/defaultServer/.gdc/7.3.0.14.08`. Utilisez les différents fichiers de propriétés pour personnaliser le collecteur de données pour atteindre les objectifs suivants :

- Activation ou désactivation du suivi des transactions.
- Activation ou désactivation de la collecte d'instantanés de segment de mémoire.
- Spécification de l'intervalle auquel le collecteur de données prend un instantané du cliché de tas.
- Activation ou désactivation de la surveillance de l'allocation de mémoire.
- Spécification de l'intervalle auquel le collecteur de données collecte les informations d'allocation de mémoire.
- Activation ou désactivation du suivi des méthodes.

A faire : Après avoir modifié les fichiers `.properties`, utilisez la commande **`cf push`** pour envoyer les mises à jour par push à l'environnement IBM Cloud.

Procédure

- Pour activer ou désactiver le suivi des transactions, définissez la propriété **com.ibm.tivoli.itcam.dc.bluemix.transaction.enabled** dans le fichier suivant sur `true` ou `false` :

  base_cd/ldc/etc/ldc.properties

  Si le suivi des transactions est activé, vous pouvez surveiller la pile d'application IBM Java dans les topologies.
- Pour activer ou désactiver la collecte des instantanés de segment de mémoire, définissez les propriétés **com.ibm.tivoli.itcam.hc.send.heap.enable** et **com.ibm.tivoli.itcam.hc.snapshot.automatic.enable** dans le fichier suivant sur `true` ou `false`.

  base_cd/healthcenter/etc/hc.properties

  Si la collecte d'instantanés de segment de mémoire est activée, le collecteur de données peut prendre un instantané de segment de mémoire à intervalles spécifiés. Les informations sur le cliché de tas peuvent être affichées dans le tableau de bord Cliché de tas.
- Pour modifier l'intervalle auquel l'instantané de segment de mémoire est pris par le collecteur de données, définissez la propriété **com.ibm.tivoli.itcam.hc.snapshot.automatic.interval** dans le même fichier sur un entier positif. L'unité de l'intervalle est la minute et la valeur par défaut est 360.

  base_cd/healthcenter/etc/hc.properties
- Pour activer ou désactiver la collecte d'allocation de mémoire, définissez la propriété **com.ibm.tivoli.itcam.hc.events.collection.automatic.enable** dans le fichier suivant sur `true` ou `false`.

  base_cd/healthcenter/etc/hc.properties

  A faire : Pour activer la collecte d'allocation de mémoire, assurez-vous également que les deux lignes suivantes sont ajoutées au fichier `jvm.options` du serveur Liberty.

  ```
  -Xhealthcenter:level=inprocess
  -Xgc:allocationSamplingGranularity=10000
  ```

  Une fois que la collecte d'allocation de mémoire est activée, les données sont disponibles dans le tableau de bord Analyse de la mémoire.
- Pour spécifier l'intervalle auquel les informations d'allocation de mémoire sont collectées, définissez la propriété **com.ibm.tivoli.itcam.hc.events.collection.automatic.interval** dans le même fichier sur un entier positif. L'unité de l'intervalle est la minute et la valeur par défaut est 15.

  base_cd/healthcenter/etc/hc.properties
- Pour activer ou désactiver le suivi des méthodes, définissez la propriété **dfe.enable.methoddata** dans le fichier suivant sur `true` ou `false`:

  base_cd/gdc/etc/gdc_dfe.properties

Que faire ensuite

- Une fois que le suivi des méthodes est activé, vous pouvez définir des seuils pour différents types de demande à l'aide des variables d'environnement, afin que des niveaux différents de données de surveillance puissent être collectés pour des demandes différentes. Pour les variables d'environnement applicables, voir Tableau 230, à la page 914.
- Si vous avez désactivé la collecte d'allocation de mémoire, n'oubliez pas de supprimer les lignes suivantes du fichier `jvm.options` du serveur Liberty :

  ```
  -Xhealthcenter:level=inprocess
  -Xgc:allocationSamplingGranularity=10000
  ```

Annulation de la configuration du collecteur de données pour les applications IBM Cloud

Si vous n'avez pas besoin de surveiller vos profils Liberty dans l'environnement IBM Cloud ou si vous souhaitez mettre à niveau le collecteur de données vers une nouvelle version, vous devez annuler la configuration du collecteur de données que vous avez déployé précédemment.

Pourquoi et quand exécuter cette tâche

Pour annuler la configuration du collecteur de données pour votre profil Liberty dans l'environnement IBM Cloud, annulez les modifications apportées aux fichiers `jvm.options`, `server.env` et `server.xml`, puis mettez à jour le profil Liberty dans IBM Cloud au moyen de la commande **`cf push`**.

Procédure

1. Dans votre répertoire local du profil Liberty, modifiez le fichier `jvm.options` pour supprimer les paramètres suivants. Vous pouvez supprimer le fichier s'il est vide après la modification.

```
-agentlib:am_ibm_16=defaultServer
-Xbootclasspath/p:../../../../.gdc/7.3.0.14.08/toolkit/lib/bcm-bootstrap.jar
-Djava.security.policy=../../../../.gdc/7.3.0.14.08/itcamdc/etc/datacollector
.policy
-Dliberty.home=/home/vcap/app/.liberty
-Xhealthcenter:level=inprocess
-Xgc:allocationSamplingGranularity=10000
-verbosegc
-Xverbosegclog:/home/vcap/app/wlp/usr/servers/defaultServer/logs/gc.log,1,10000
```

2. Dans le fichier `server.env`, supprimez la valeur suivante pour la variable d'environnement **`LD_LIBRARY_PATH`**. Vous pouvez supprimer le fichier s'il est vide après la modification.

```
LD_LIBRARY_PATH=:/lib:../../../../.gdc/7.3.0.14.08/toolkit/lib/lx8266
:../../../../.gdc/7.3.0.14.08/toolkit/lib/lx8266/ttapi
```

3. Modifiez le fichier `server.xml` pour supprimer la fonction monitor-1.0 en retirant la ligne suivante de la section `<featureManager>`

```
<feature>monitor-1.0</feature>
```

4. Supprimez le répertoire `.gdc` du répertoire de base Liberty.
5. Ouvrez une invite de commande, accédez au répertoire qui contient le fichier `manifest.yml` du serveur Liberty.
6. Connectez-vous à IBM Cloud et mettez à jour le profil Liberty avec la commande **`cf push`**.

Que faire ensuite

Une fois que vous avez configuré le collecteur de données, la console Cloud APM continue d'afficher le collecteur de données dans les applications auxquelles vous l'avez ajouté. La console Cloud APM indique qu'aucune donnée n'est disponible pour l'application et n'indique pas que le collecteur de données est hors ligne. Pour plus d'informations sur la manière de supprimer le collecteur de données d'applications et de groupes de ressources, voir «Suppression de collecteurs de données de la console Cloud APM», à la page 193.

Configuration avancée du collecteur de données

Vous pouvez éditer les fichiers de configuration du collecteur de données afin de modifier des paramètres de surveillance supplémentaires.

Fichiers de propriétés du collecteur de données Liberty

Divers fichiers de configuration sont fournis pour que vous puissiez contrôler davantage la configuration et le comportement du collecteur de données.

Une fois que vous avez extrait le package du collecteur de données dans un répertoire local, les fichiers du collecteur de données se trouvent dans le répertoire *`rép_local`*`/liberty_dc/.gdc/7.3.0.14.08`. Par exemple, `/opt/ibm/apm/.gdc/7.3.0.14.08`. Ce dossier devient le répertoire de

base du collecteur de données, qui est appelé *base_cd* dans les instructions qui suivent, par mesure de simplification.

Fichiers de propriétés du collecteur de données

Chaque instance de serveur d'applications surveillée par le collecteur de données possède son propre fichier de propriétés. Le collecteur de données crée automatiquement le fichier de propriétés. Le nom du fichier est *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/datacollector.properties.

Pour faciliter les mises à niveau ultérieures, ne modifiez pas ce fichier.

Ajoutez plutôt les paramètres que vous souhaitez modifier au fichier de propriétés personnalisées du collecteur de données. Ce fichier est nommé *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom/datacollector_custom.properties. Les paramètres du fichier de propriétés personnalisées du collecteur de données remplacent les valeurs du fichier de propriétés du collecteur de données.

Important : Si le fichier *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom/datacollector_custom.properties n'existe pas, créez-le lorsque vous souhaitez effectuer des modifications. Il se peut que vous deviez également créer le répertoire custom.

Fichier de propriétés du kit d'outils

Le fichier de propriétés du kit d'outils est automatiquement créé par le collecteur de données au démarrage, à l'aide de différents fichiers d'entrée. Il est unique pour chaque instance de serveur d'applications surveillée par le collecteur de données. Son nom est *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/toolkit.properties.

Ce fichier étant recréé à chaque démarrage du collecteur de données, **ne lui apportez pas de modifications** car elles seront remplacées.

Ajoutez plutôt les paramètres que vous souhaitez modifier au fichier de propriétés personnalisées du kit d'outils. Ce fichier est nommé *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom/toolkit_custom.properties. Les paramètres du fichier de propriétés personnalisées du kit d'outils remplacent les valeurs du fichier de propriétés du kit d'outils.

Vous pouvez également définir les propriétés du kit d'outils de toutes les instances de serveur d'applications surveillées par l'installation du collecteur de données. Pour cela, ajoutez les paramètres au fichier de propriétés personnalisées du kit d'outils global : *base_cd*/runtime/custom/toolkit_global_custom.properties. Cependant, si une propriété est définie dans le fichier toolkit_custom.properties propre à l'instance, elle remplace la valeur dans le fichier global pour cette instance.

Important : Si le fichier *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom/toolkit_custom.properties ou *base_cd*/runtime/custom/toolkit_custom.properties n'existe pas, créez-le lorsque vous souhaitez effectuer des modifications. Il se peut que vous deviez également créer le répertoire custom.

Autres fichiers de propriétés

Outre le fichier de propriétés du collecteur de données et le fichier de propriétés du kit d'outils, il existe d'autres fichiers de propriétés propres à chaque instance de serveur d'applications surveillée par le collecteur de données.

***base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom/gdc/gdc_custom.properties**
Définit les détails de collecte des données de diagnostic et de trace de méthode. Pour plus d'informations sur la modification de ce fichier, voir «Configuration de la collecte d'informations de diagnostic détaillées», à la page 920.

***base_cd*/runtime/*version_serveur_app.nom_noeud.nom_serveur*/hc.properties**
Définit les détails de la collecte d'instantanés de segment de mémoire et de la collecte d'allocation de mémoire. Pour plus d'informations sur la modification de ce fichier, voir «Configuration de la collecte d'informations de diagnostic détaillées», à la page 920.

***base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/cynlogging.properties**
Définit les détails des noms de fichier journal et de la consignation pour la portion Java du collecteur de données.

***base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/cyncclog.properties**
Définit les détails des noms de fichier journal et de la consignation pour la portion C++ du collecteur de données.

Fichiers de trace du collecteur de données

Les fichiers de trace du collecteur de données sont stockés par défaut dans les emplacements suivants :

- Windows *base_cd*\logs\CYN\logs.
- Linux AIX *base_cd*/logs/CYN/logs.

Activation ou désactivation de la collecte des données de suivi des transactions et des données de diagnostic

Par défaut, le suivi des transactions et des méthodes est activé pour le collecteur de données. La collecte des instantanés de segment de mémoire et la collecte d'allocation de mémoire sont désactivées. Vous pouvez personnaliser la collecte de données ou les intervalles auxquels les données de diagnostic sont collées en modifiant les fichiers `.properties` du collecteur de données.

Pourquoi et quand exécuter cette tâche

Les fichiers de propriétés du collecteur de données sont dans le répertoire *base_cd*, par exemple `/opt/ibm/apm/.gdc/7.3.0.14.08`. Utilisez les différents fichiers de propriétés pour personnaliser le collecteur de données pour atteindre les objectifs suivants :

- Activation ou désactivation du suivi des transactions.
- Activation ou désactivation de la collecte d'instantanés de segment de mémoire.
- Spécification de l'intervalle auquel le collecteur de données prend un instantané du cliché de tas.
- Activation ou désactivation de la surveillance de l'allocation de mémoire.
- Spécification de l'intervalle auquel le collecteur de données collecte les informations d'allocation de mémoire.
- Activation ou désactivation du suivi des méthodes.

A faire : Selon que vous avez redémarré le serveur Liberty après la configuration du collecteur de données, des fichiers `.properties` différents sont applicables. Si vous avez redémarré le serveur Liberty après la configuration du collecteur de données, un répertoire `runtime` est créé dans le répertoire *base_cd*. Après cela, vous pouvez utiliser uniquement les fichiers `.properties` dans le répertoire *base_cd*`/runtime/`*appserver_version.node_name.profile_name.server_name* pour personnaliser le collecteur de données pour chaque serveur d'applications.

Procédure

- Pour activer ou désactiver le suivi des transactions, définissez la propriété **com.ibm.tivoli.itcam.dc.bluemix.transaction.enabled** dans le fichier suivant sur `true` ou `false` :

  base_cd/runtime/*version_serveur_apps.nom_noeud.nom_serveur*/ldc.properties (si le répertoire `runtime` n'existe pas, utilisez *base_cd*/ldc/etc/ldc.properties)

  Une fois que le suivi des transactions est activé, vous pouvez surveiller la pile d'application IBM Java dans les topologies.
- Pour activer ou désactiver la collecte des instantanés de segment de mémoire, définissez les propriétés **com.ibm.tivoli.itcam.hc.send.heap.enable** et **com.ibm.tivoli.itcam.hc.snapshot.automatic.enable** dans le fichier suivant sur `true` ou `false`.

  base_cd/runtime/*version_serveur_apps.nom_noeud.nom_serveur*/hc.properties (si le répertoire `runtime` n'existe pas, utilisez *base_cd*/healthcenter/etc/hc.properties)

  Une fois que la collecte d'instantanés de segment de mémoire est activée, le collecteur de données peut prendre un instantané de segment de mémoire à intervalles spécifiés. Les informations sur le cliché de tas peuvent être affichées dans le tableau de bord Cliché de tas.
- Pour modifier l'intervalle auquel l'instantané de segment de mémoire est pris par le collecteur de données, définissez la propriété **com.ibm.tivoli.itcam.hc.snapshot.automatic.interval** dans le même fichier sur un entier positif. L'unité de l'intervalle est la minute et la valeur par défaut est 360.

  base_cd/runtime/*version_serveur_apps.nom_noeud.nom_serveur*/hc.properties (si le répertoire `runtime` n'existe pas, utilisez *base_cd*/healthcenter/etc/hc.properties)
- Pour activer ou désactiver la collecte d'allocation de mémoire, définissez la propriété **com.ibm.tivoli.itcam.hc.events.collection.automatic.enable** dans le fichier suivant sur `true` ou `false`.

  base_cd/runtime/*version_serveur_apps.nom_noeud.nom_serveur*/hc.properties (si le répertoire `runtime` n'existe pas, utilisez *base_cd*/healthcenter/etc/hc.properties)

  A faire : Pour activer la collecte d'allocation de mémoire, assurez-vous également que les deux lignes suivantes sont ajoutées au fichier `jvm.options` du serveur Liberty.

  ```
  -Xhealthcenter:level=inprocess
  -Xgc:allocationSamplingGranularity=10000
  ```

  Une fois que la collecte d'allocation de mémoire est activée, les données sont disponibles dans le tableau de bord Analyse de la mémoire.
- Pour spécifier l'intervalle auquel les informations d'allocation de mémoire sont collectées, définissez la propriété **com.ibm.tivoli.itcam.hc.events.collection.automatic.interval** dans le même fichier sur un entier positif. L'unité de l'intervalle est la minute et la valeur par défaut est 15.

  base_cd/runtime/*version_serveur_apps.nom_noeud.nom_serveur*/hc.properties (si le répertoire `runtime` n'existe pas, utilisez *base_cd*/healthcenter/etc/hc.properties)
- Pour activer ou désactiver le suivi des méthodes, définissez la propriété **dfe.enable.methoddata** dans le fichier suivant sur `true` ou `false`:

  base_cd/runtime/*appserver_version.node_name.profile_name.server_name*/custom/gdc/gdc_custom.properties (si le répertoire `runtime` n'existe pas, utilisez *base_cd*/gdc/etc/gdc_dfe.properties)

Résultats

Après avoir modifié les fichiers `.properties`, redémarrez le serveur Liberty pour que la modification soit prise en compte.

Pour plus d'informations sur les fichiers `.properties` du collecteur de données pour chaque serveur d'applications, voir «Fichiers de propriétés du collecteur de données Liberty», à la page 916.

Que faire ensuite

- Une fois que le suivi des méthodes est activé, vous pouvez définir des seuils pour différents types de demande, afin que des niveaux différents de données de surveillance puissent être collectés pour des demandes différentes. Pour plus d'informations, voir «Personnalisation des seuils de demande», à la page 922.
- Si vous avez désactivé la collecte d'allocation de mémoire, n'oubliez pas de supprimer les lignes suivantes du fichier `jvm.options` du serveur Liberty :

```
-Xhealthcenter:level=inprocess
-Xgc:allocationSamplingGranularity=10000
```

Configuration de la collecte d'informations de diagnostic détaillées

Si vous disposez d'IBM Cloud Application Performance Management, Advanced, vous pouvez utiliser le collecteur de données pour collecter des informations de diagnostic détaillées sur l'instance de serveur d'applications surveillée. Pour configurer le comportement de la collecte des données de diagnostic, notamment la quantité d'informations de diagnostic stocké par le collecteur de données, personnalisez le fichier de configuration `gdc_custom.properties`.

Pourquoi et quand exécuter cette tâche

Le fichier `gdc_custom.properties` se trouve dans le répertoire *rép_base_cd*`/runtime/`*version_serveurapp.nom_noeud.nom_profi.nom_serveur*`/custom/gdc`.

Les exemples suivants expliquent comment utiliser les propriétés du fichier de configuration `gdc_custom.properties` pour effectuer les opérations suivantes :

- Définition des limites relatives à la taille et au nombre des fichiers d'informations détaillés
- Définition de la collecte complète ou partielle des données de demande et des données de diagnostic de méthode

Vous pouvez également définir d'autres propriétés dans le fichier `gdc_custom.properties` pour personnaliser la collecte de données de diagnostic. Reportez-vous aux commentaires du fichier qui décrivent les propriétés.

A faire : Après avoir modifié le fichier `gdc_custom.properties`, vous devez redémarrer l'instance de serveur d'applications surveillée pour appliquer les modifications.

Définition des limites relatives à la taille et au nombre des fichiers d'informations détaillés

Pourquoi et quand exécuter cette tâche

Le collecteur de données stocke les informations de diagnostic dans un certain nombre des fichiers. Par défaut, il stocke 100 fichiers ; si 100 fichiers sont déjà stockés et qu'un nouveau fichier est créé, le fichier le plus ancien est supprimé. Le collecteur de données crée un nouveau fichier toutes les 15 minutes, ou lorsque la taille du fichier en cours dépasse 200 mégaoctets. Lorsque la taille totale du répertoire contenant les fichiers dépasse 2 gigaoctets, le collecteur de données supprime le fichier le plus ancien.

Procédure

Vous pouvez changer les paramètres suivants dans le fichier *rép_principal_collecteur_données*`/runtime/`*version_serveur_applications.nom_noeud.nom_profil.nom_serveur*`/custom/gdc/gdc_custom.properties` :

- Pour définir le nombre maximal de fichiers contenant des informations de diagnostic, définissez la propriété `com.ibm.itcam.gdc.dfe.filelimit`.
  Exemple :

```
com.ibm.itcam.gdc.dfe.filelimit=100
```

- Pour définir le délai, en minutes, après lequel le collecteur de données crée un nouveau fichier de données de diagnostic, définissez la propriété `com.ibm.itcam.gdc.dfe.frequency`.
  Par exemple :

  ```
  com.ibm.itcam.gdc.dfe.frequency=15
  ```

- Pour définir la taille maximale des fichiers de données de diagnostic, en mégaoctets, définissez la propriété `dfe.file.maxlimit`.
  Exemple :

  ```
  dfe.file.maxlimit=200
  ```

  Si les fichier de données de diagnostic en cours atteint cette taille, le collecteur de données crée un nouveau fichier de données de diagnostic.

- Pour définir la taille totale maximale de tous les fichiers de données, en mégaoctets, définissez la propriété `trace.dir.size.limit`.
  Exemple :

  ```
  trace.dir.size.limit=2147483648
  ```

  Si la somme des tailles de tous les fichiers de données de diagnostic dépasse cette valeur, le collecteur de données supprime le fichier de données le plus ancien. La taille totale minimale est de 25 mégaoctets.

Définition de la collecte complète ou partielle des données de demande et des données de diagnostic de méthode

Pourquoi et quand exécuter cette tâche

Le collecteur de données a les paramètres par défaut suivants :

- Le collecteur de données ne collecte les données de diagnostic que pour les demandes sélectionnées. La sélection (l'échantillon) des demandes vise à inclure toutes les erreurs et certaines demandes correctes.
- La collecte des données de méthode est désactivée au démarrage du serveur.
- Lorsque la collecte des données de méthode est activée, le collecteur de données récupère les données de méthode pour certaines demandes uniquement (de celles pour lesquelles les données de diagnostic sont collectées). Cette sélection avancée (échantillon) vise de nouveau à inclure toutes les erreurs et certaines demandes correctes.

Important : La modification de ces paramètres affecte le performance du serveur d'application. Sur les serveurs de production, la dégradation de la performance peut être critique.

Procédure

Vous pouvez modifier ces paramètres à l'aide des propriétés dans le fichier *rép_base_cd*`/runtime/`*version_serveurapplications.nom_noeud.nom_profil. nom_serveur*`/custom/gdc/gdc_custom.properties`.

- Pour activer la collecte des méthodes de données au démarrage du serveur, définissez la propriété de la manière suivante :

  ```
  dfe.enable.methoddata=true
  ```

  Conseil : Vous pouvez utiliser la page **Configuration d'agent** pour activer ou désactiver de manière dynamique la collecte des données de trace de méthode.

- Pour collecter les données de diagnostic pour toutes les demandes, désactivez l'échantillonnage en définissant la propriété de la manière suivante :

```
dc.sampling.enable=false
```

- Pour activer la collecte des données de méthode pour toutes les demandes dont les données de diagnostic sont collectées, définissez la propriété de la manière suivante :

```
dc.sampling.enable=false
dc.sampling.methsampler.enabled=false
```

A faire : La propriété `dc.sampling.methsampler.enabled` prend effet uniquement lorsque la collecte des données de méthode est activée dans la page de configuration d'agent ou par la propriété `dfe.enable.methoddata`.

Personnalisation des seuils de demande
Certaines demandes peuvent ne pas avoir suffisamment d'informations si les seuils par défaut sont élevés. Vous pouvez personnaliser les seuils de demande afin que davantage de demandes ou de données contextuelles de demande puissent être capturées par le collecteur de données.

Pourquoi et quand exécuter cette tâche

Chaque type de demande comporte deux types de seuil, qui sont nommés **perfThreshold** et **secondaryPerfThreshold**. Une demande est capturée par le collecteur de données uniquement quand elle est plus longue que la durée spécifiée pour le seuil **perfThreshold**. Les données contextuelles, comme la trace de la pile et l'instruction SQL, sont capturées uniquement lorsque la demande prend plus de temps que la durée spécifiée pour le seuil **secondaryPerfThreshold**. Vous pouvez ajuster ces valeurs de seuil en fonction de vos besoins.

Procédure

1. Accédez au répertoire *base_cd*`\gdc\etc`, *base_cd* correspondant au répertoire de base du collecteur de données.
2. Dans un éditeur de texte, ouvrez le fichier XML pour le type de demande que vous souhaitez personnaliser. Vous pouvez dire quel fichier est pour quel type de demande d'après le nom du fichier XML.
   Par exemple, le fichier `ejb.xml` concerne les demandes d'EJB, le fichier `custom.xml` concerne les demandes personnalisées et le fichier `appMethods.xml` concerne la classe et les méthodes lorsque la trace de méthode est activée.
3. Définissez les balises `<collectContextData>`, `<collectStackTrace>` et `<createDataRow>` sur `ifThresholdExceeded`.

```
<collectContextData>ifThresholdExceeded</collectContextData>
<collectStackTrace>ifThresholdExceeded</collectStackTrace>
<createDataRow>ifThresholdExceeded</createDataRow>
```

4. Définissez les balises `<perfThreshold>` et `<secondaryPerfThreshold>` sur les valeurs de seuil de votre choix. L'unité du seuil est la milliseconde.
   Par exemple, le fichier `ejb.xml` a les paramètres suivants pour les demandes d'EJB. En conséquence, seules les demandes d'EJB qui prennent plus de 1 seconde (1000 millisecondes) sont capturées par le collecteur de données. En outre, les données contextuelles liées à une demande d'EJB, comme la trace de la pile et l'accueil d'EJB, sont capturées uniquement lorsque la demande d'EJB prend plus de 1,5 secondes (1500 millisecondes).

```
<requestProbePoint id="EJB">
<interface>com.ibm.tivoli.itcam.toolkit.ai.boot.aspectmanager.ITurboEJBEventListener</
interface>
<family>EJB</family>
<collectContextData>ifThresholdExceeded</collectContextData>
<collectStackTrace>ifThresholdExceeded</collectStackTrace>
<perfThreshold>1000</perfThreshold>
<secondaryPerfThreshold>1500</secondaryPerfThreshold>
<dataToCollect>instanceAndSummary</dataToCollect>
<createDataRow>ifThresholdExceeded</createDataRow>
<requestType>EJB Method</requestType>
</requestProbePoint>
```

5. Sauvegardez vos changements, puis redémarrez le serveur d'applications.

Désactivation des divers types d'instrumentation par code intermédiaire des API Java EE
Dans BCI (Byte Code Instrumentation), le collecteur de données intercepte les appels des entrées et des sorties de différents types d'API Java Platform Enterprise Edition (Java EE) afin de créer un flux d'exécution pour chaque demande d'application. Des ressources sont utilisées pour la surveillance. Vous pouvez paramétrer le collecteur de données afin d'exclure certaines de ces API de la surveillance et réduire ainsi la consommation de ressources.

Pour désactiver la surveillance BCI pour les API Java EE, ajoutez les propriétés suivantes au fichier de propriétés personnalisées du kit d'outils. Pour plus d'informations sur ce fichier, voir «Fichier de propriétés du kit d'outils», à la page 917.

Tableau 231. Ajout de lignes au fichier de propriétés personnalisées du kit d'outils

Type d'API Java EE	**Ligne à ajouter au fichier `toolkit_custom.properties`**
Enterprise JavaBeans (EJB)	`com.ibm.tivoli.itcam.toolkit.ai.enableejb=false`
Java Connector Architecture (JCA)	`com.ibm.tivoli.itcam.toolkit.ai.enablejca=false`
JDBC (Java Database Connectivity)	`com.ibm.tivoli.itcam.toolkit.ai.enablejdbc=false`
Java Naming and Directory Interface (JNDI)	`com.ibm.tivoli.itcam.toolkit.ai.enablejndi=false`
Java Message Service (JMS)	`com.ibm.tivoli.itcam.toolkit.ai.enablejms=false`
Conteneurs Web pour Servlets/Pages JSP (JavaServer Pages)	`com.ibm.tivoli.itcam.dc.was.webcontainer=false`
Suivi du nombre de sessions HTTP	`com.ibm.tivoli.itcam.toolkit.ai.enablesessioncount=false`
CICS Transaction Gateway (CTG)	`com.ibm.tivoli.itcam.dc.ctg.enablectg=false`
IMS	`com.ibm.tivoli.itcam.dc.mqi.enableims=false`
Java Data Objects (JDO)	`com.ibm.tivoli.itcam.dc.mqi.enablejdo=false`
MQI (Message Queue Interface)	`com.ibm.tivoli.itcam.dc.mqi.enablemqi=false`
Service Web Axis	`com.ibm.tivoli.itcam.toolkit.ai.axis.enablewebservice=false`
RMI (Remote Method Invocation)	`am.ejb.rmilistener.enable=false`
Conteneur d'EJB WebSphere Application Server	`com.ibm.tivoli.itcam.dc.was.enableEJBContainer=false`

Désactivation du suivi des transactions pour un certain type de transactions
Lorsque le suivi des transactions est activé pour le collecteur de données, tous les types de transactions sont surveillés par défaut. Vous pouvez utiliser le fichier de propriétés du kit d'outils afin de désactiver le suivi des transactions pour des types de transactions spécifiques.

Pourquoi et quand exécuter cette tâche

Editez le fichier `toolkit_custom.properties` afin de personnaliser le suivi des transactions pour chaque serveur d'applications ou éditez le fichier `toolkit_global_custom.properties` pour toutes les instances de serveur d'applications.

Le fichier `toolkit_custom.properties` est utilisé dans la procédure suivante pour un serveur d'applications unique. Les propriétés sont également prises en charge dans le fichier `toolkit_global_custom.properties`. Pour plus d'informations sur les fichiers de propriétés du kit d'outils, voir Fichiers de propriétés du collecteur de données Liberty.

Procédure

1. Ouvrez le fichier `toolkit_custom.properties` du serveur d'applications à l'aide d'un éditeur de texte. Ce fichier se trouve dans le répertoire suivant :

   rép_principal_dc`/runtime/`
   version_serveur_app.node_name.nom_profil.nom_serveur`/custom`
2. Selon vos besoins, indiquez une ou plusieurs des propriétés suivantes, puis définissez la valeur de propriété sur `false` afin de désactiver le suivi des transactions pour un certain type de transactions.

   Pour les demandes CICS
   `com.ibm.tivoli.itcam.dc.ttapi.cics.enabled=false`

   Pour les demandes personnalisées
   `com.ibm.tivoli.itcam.dc.ttapi.ims.enabled=false`

   Pour les demandes EJB
   `com.ibm.tivoli.itcam.dc.ttapi.ejb.enabled=false`

   Pour les appels de client HTTP
   `com.ibm.tivoli.itcam.dc.ttapi.httpclient.enabled=false`

   Exception : Pour désactiver le suivi des transactions pour les appels de client HTTP Apache, spécifiez `com.ibm.tivoli.itcam.toolkit.dc.en able.apache.httpclient=false`.

   Pour les demandes IMS
   `com.ibm.tivoli.itcam.dc.ttapi.ims.enabled=false`

   Pour les demandes JDBC
   `com.ibm.tivoli.itcam.dc.ttapi.jdbc.enabled=false`

   Pour les demandes JMS
   `com.ibm.tivoli.itcam.dc.ttapi.jms.enabled=false`

   Pour les demandes JNDI
   `com.ibm.tivoli.itcam.dc.ttapi.jndi.enabled=false`

   Pour les demandes MQI
   `com.ibm.tivoli.itcam.dc.ttapi.mqi.enabled=false`

   Pour les demandes de portail
   `com.ibm.tivoli.itcam.dc.ttapi.portal=false`

   Pour les demandes RMI-IIOP
   `com.ibm.tivoli.itcam.dc.ttapi.rmiiiop.enabled=false`

   Pour les demandes de servlet
   `com.ibm.tivoli.itcam.dc.ttapi.arm.servlet.enabled=false`

   Pour les demandes de service Web
   `com.ibm.tivoli.itcam.dc.ttapi.webservice.enabled=false`

Conseil : Pour plus d'informations sur ces propriétés, voir le fichier *rép_principal_dc*/ttdc/etc/ttdc.properties.

3. Sauvegardez et fermez le fichier toolkit_custom.properties.
4. Pour que les modifications soient prises en compte, redémarrez le serveur d'applications.

Exclusion de classes de la surveillance
Vous pouvez personnaliser la collecte de données en excluant certaines classes de la surveillance. Pour effectuer cette personnalisation, utilisez le fichier de propriétés du kit d'outils.

Pourquoi et quand exécuter cette tâche

Editez le fichier toolkit_custom.properties afin de personnaliser le suivi des transactions pour chaque serveur d'applications ou éditez le fichier toolkit_global_custom.properties pour toutes les instances de serveur d'applications.

Le fichier toolkit_custom.properties est utilisé dans la procédure suivante pour un serveur d'applications unique. Les propriétés sont également prises en charge dans le fichier toolkit_global_custom.properties. Pour plus d'informations sur les fichiers de propriétés du kit d'outils, voir Fichiers de propriétés du collecteur de données Liberty.

Procédure

1. Ouvrez le fichier toolkit_custom.properties du serveur d'applications à l'aide d'un éditeur de texte. Ce fichier se trouve dans le répertoire suivant :

   rép_principal_dc/runtime/*version_serveur_app*.*node_name*.*nom_profil*.*nom_serveur*/custom
2. Editez le fichier pour ajouter la propriété suivante et sauvegardez vos modifications.

```
am.camtoolkit.gpe.customxml.exclude=excludes.xml
```

3. Dans le même répertoire custom, créez le fichier excludes.xml avec le contenu suivant, puis indiquez le nom de classe à exclure dans la balise <exclude>. Vous pouvez ajouter autant de classes que nécessaire et utiliser au besoin le caractère générique d'astérisque (*).

```
<gpe>
  <bci>
    <classExcludes>
      <exclude>nom_de_classe_à_exclure</exclude>
      <exclude>nom_de_classe_à_exclure</exclude>
    </classExcludes>
  </bci>
</gpe>
```

   Exemple :

```
<gpe>
  <bci>
    <classExcludes>
      <exclude>org.apache.struts.action.ActionServlet</exclude>
      <exclude>com.company.package.*</exclude>
    </classExcludes>
  </bci>
</gpe>
```

4. Redémarrez le serveur d'applications.

Que faire ensuite
Pour vérifier que la classe est bien exclue, examinez le fichier toolkit.xml ; le nom de la classe devrait s'afficher dans la section <classExcludes>.

A faire : Le fichier toolkit.xml contient les paramètres d'exécution et s'actualise chaque fois que le serveur d'applications est redémarré.

Personnalisation du mappage des informations des demandes
Dans certains cas, il peut être nécessaire de changer les informations qui identifient les demandes surveillées par l'agent. Ces informations incluent le nom de la demande et toutes les données qui peuvent être affichées pour la demande (par exemple, le texte de la requête pour une requête SQL). Pour modifier ces informations, vous devez définir une configuration d'associateur de demande personnalisée.

Pourquoi et quand exécuter cette tâche

Pour personnaliser le mappage des informations de demande, vous devez définir une configuration d'associateur de demande personnalisée dans un fichier XML.

Dans ce fichier, certains des *symboles* intégrés représentent les valeurs du contexte d'exécution de la demande. Vous pouvez créer des symboles supplémentaires, qui calculent de nouvelles valeurs. Le calcul peut inclure des valeurs de demande d'origine, des expressions, des appels à des méthodes Java (y compris les méthodes présentes dans l'application surveillée), des conditions et des itérations sur un ensemble de valeurs.

Puis, vous pouvez *mapper* le contenu des symboles dans les nouvelles données de demande qui sont fournies au serveur Cloud APM. Si une variable dans les données de demande n'est pas mappée, la valeur d'origine est conservée.

Dans la mesure où des données différentes sont collectées selon les types de demandes, une configuration d'associateur de demande personnalisée doit être spécifique à un type de demande donné. Vous pouvez configurer différents associateurs de demande pour différents types de demande sur le même collecteur de données.

Procédure

Pour définir une configuration d'associateur de demande personnalisée pour un type de demande, procédez comme suit :

1. Vous définissez une configuration d'associateur de demande personnalisée dans un fichier XML.
   Pour plus d'informations sur la syntaxe XML, voir «Syntaxe du fichier XML», à la page 926.
2. Placez le fichier XML dans le répertoire *base_cd*/runtime/custom pour l'employer pour toutes les instances du serveur d'applications, ou dans le répertoire *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom pour l'utiliser pour une instance de serveur d'applications.
3. Activez le mappage de demande personnalisée pour ce type dans le fichier de configuration personnalisée du kit d'outils, `toolkit_custom.properties` ou `toolkit_global_custom.properties`.
   Pour obtenir des instructions, voir «Activation d'un associateur de demande», à la page 937.
4. Mettez en référence le fichier XML que vous avez défini à partir du même fichier de configuration personnalisée du kit d'outils.
   Pour obtenir des instructions, voir «Activation d'un associateur de demande», à la page 937.

Syntaxe du fichier XML
Le fichier XML que vous créez pour la configuration de l'associateur de demande doit être un code XML valide et doit rester disponible lorsque la configuration est en cours d'utilisation. Placez le fichier XML dans le répertoire *base_cd*/runtime/custom pour l'employer pour toutes les instances du serveur d'applications, ou dans le répertoire *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom pour l'utiliser pour une instance de serveur d'applications.

Niveau supérieur

La balise de niveau supérieur est <gpe>. Dans cette balise, utilisez la balise >runtimeConfiguration<. Ces balises n'ont pas d'attributs.

Dans la balise <runtimeConfiguration>, créez une balise <requestMapperDefinition>. Cette balise doit avoir un attribut `type`. Définissez-la sur le nom du type d'associateur de demande pour le type de demande requis. Pour plus d'informations, voir Tableau 233, à la page 939.

Dans la balise <requestMapperDefinition>, les deux balises suivantes doivent être présentes :

<symbolDefinitions>
Contient toutes les définitions des symboles. Les symboles représentent les valeurs que calcule l'agent chaque fois qu'une demande de ce type est détectée.

<selection>
Contient le mappage des clés de contexte aux valeurs. Les clés représentent les données personnalisées envoyées à l'agent. Elles sont prédéfinies pour chaque type de demande. Le mappage peut être conditionnel.

Pour plus d'informations sur les propriétés d'activation et les noms de type de l'associateur de demande, voir Tableau 233, à la page 939.

En outre, dans la balise <runtimeConfiguration>, vous pouvez créer une balise <requestMapperClassPath>. Cette dernière permet de définir des fichiers .jar. Dans ces fichiers .jar, vous pouvez référencer des classes Java dans des définitions d'associateur de demande.

Définition d'une expression
Pour définir des symboles, vous devez utiliser des expressions. L'agent évalue les expressions pour affecter des valeurs aux symboles.

Utilisation de données dans une expression
Une expression peut utiliser les données suivantes :

- Les symboles de données d'entrée pour le type de demande
- D'autres symboles décrits dans la même définition d'associateur de demande
- Des constantes numériques
- Des constantes de type chaîne (délimitées par ", par exemple `"string"`)
- Des constantes booléennes (`true`, TRUE, `false`, FALSE)
- La constante `null`

Pour plus d'informations sur les symboles de données d'entrée, voir Tableau 234, à la page 940.

Si la valeur d'un symbole est une instanciation d'une classe Java, les expressions peuvent contenir des références à des zones et à des méthodes qui sont définies dans la classe. Pour faire référence à une zone, utilisez *`symbole.nom_zone`*. Pour faire référence à une méthode, utilisez *`symbole.nom_méthode(paramètres)`*. L'appel de méthode doit renvoyer une valeur. Par exemple, vous pouvez utiliser les méthodes de chaîne Java avec un symbole ayant une valeur de type chaîne.

Pour faire référence à une zone statique ou à la méthode d'une classe, vous pouvez également utiliser *`nom_classe.nom_zone`* et *`nom_classe.nom_méthode(paramètres)`*.

Si un symbole fait référence à un objet de type tableau, l'expression peut sélectionner un élément (*`symbole[sélecteur]`*) et déterminer la longueur du tableau (*`symbole`*`.length`).

Opérateurs

Vous pouvez utiliser les opérateurs suivants dans une expression :

- Opérateurs booléens : AND, &, OR, |, NOT, !
- Comparaison : ==, !=, GT, >, LT, <, GE, >=, LE, <=
- Opérateurs numériques : +, -, *, /
- Parenthèses pour forcer l'ordre d'évaluation : (,)

Important : Vous devez mettre en échappement les symboles <, > et & dans le code XML. A défaut, vous pouvez utiliser les opérateurs GT (supérieur à), GE (supérieur ou égal à), LT (inférieur à), LE (inférieur ou égal à) et AND.

L'expression peut évaluer si une valeur est une instance d'une classe, en utilisant l'opérateur `instanceof` :

```
expression instanceof nom.classe.java
```

Cet opérateur, semblable à l'opérateur Java `instanceof`, génère une valeur booléenne. Dans cet exemple, la valeur est true si la classe à laquelle la valeur *expression* appartient remplit l'une des conditions suivantes :

- Se nomme *nom.classe.java*
- Est une sous-classe directe ou indirecte de la classe identifiée par *nom.classe.java*.
- Implémente, directement ou indirectement, l'interface identifiée par *nom.classe.java*.

L'expression peut également instancier un nouvel objet d'une classe Java en utilisant l'opérateur new. Cet opérateur est similaire à l'opérateur Java new :

```
new nom.classe.java(expression1, expression2, ... expressionN)
```

Ordre de priorité des opérateurs
Les opérateurs sont évalués selon un ordre de priorité. Les opérateurs ayant le même niveau de priorité sont évalués de gauche à droite. Vous pouvez modifier l'ordre d'évaluation en utilisant des parenthèses (et).

L'ordre de priorité est le suivant :

1. . opérateur (appel de méthode ou référence de zone)
2. [ ] (sélecteur d'élément de tableau)
3. new
4. !, NOT
5. *, /
6. +, -
7. GT, >, LT, <, GE, >=, LE, <=, instanceof
8. ==, !=
9. AND, &
10. OR, |

Exemple

```
$s1 >= ( 2 * ($s2.sampMethod($s3, true) + 1))
```

L'agent évalue cette expression de la manière suivante :

1. Le symbole $s1 est évalué. Il doit renvoyer une valeur numérique.
2. Le symbole $s2 est évalué. Il doit renvoyer un objet Java.
3. Le symbole $s3 est évalué.
4. La méthode sampMethod est appelée pour l'objet qui résulte de l'évaluation de $s2. Le résultat de l'évaluation de $s3 est transmis en tant que premier paramètre et la valeur booléenne true est transmise en tant que second paramètre. L'appel de la méthode sampMethod doit renvoyer une valeur numérique.
5. 1 est ajouté au résultat de l'étape «4», à la page 928.
6. Le résultat de l'étape «5», à la page 928 est multiplié par 2.

7. Le résultat de l'étape «1», à la page 928 est comparé au résultat de l'étape «6», à la page 928. Si le résultat de l'étape «1», à la page 928 est supérieur ou égal au résultat de l'étape «6», à la page 928, `true` est renvoyé. Sinon, c'est la valeur `false` qui est renvoyée.

Définition des symboles de base
Pour définir des symboles, vous devez utiliser des expressions. L'agent évalue les expressions pour affecter des valeurs aux symboles.

Dans la balise <symbol>, utilisez les balises suivantes :

<name>
Nom du symbole. Il s'agit d'une chaîne qui doit commencer par le caractère $.

<eval>
Expression que l'agent doit évaluer pour produire la valeur de ce symbole. Pour plus d'informations sur la définition des expressions, voir «Définition d'une expression», à la page 927.

<type>
Type de la valeur renvoyée par le symbole. Entrez cette valeur sous la forme d'un nom de classe Java complet ou d'une primitive Java. La définition du type de symbole est facultative. S'il n'est pas défini, l'associateur de demande essaye d'établir le type de zone en fonction de l'expression. Si l'associateur de demande ne peut pas déterminer le type de symbole avant qu'il évalue l'expression, les performances sont affectées. Pour optimiser les performances, il est donc préférable de spécifier le type.

<args>
Arguments associés au symbole. Cette balise est facultative ; si elle est définie, des arguments doivent être fournis pour calculer le symbole. Pour plus d'informations, voir «Définition des arguments de symbole», à la page 929.

Exemple

```
<symbol>
   <name>$doubles1</name>
   <eval>$s1*2</eval>
   <type>int</type>
</symbol>
```

Ce symbole renvoie le double de la valeur d'un autre symbole, `$s1`.

Définition des arguments de symbole
Dans la balise <args> de la définition d'un symbole, vous pouvez définir les types d'arguments du symbole.

Dans cette balise, utilisez la balise <type> pour définir les types d'arguments. Entrez cette valeur sous la forme d'un nom de classe Java complet ou d'une primitive Java. Vous pouvez indiquer plusieurs balises <type> qui définissent chacune un argument.

Dans ce cas, le symbole doit être référencé avec des arguments entre parenthèses, comme suit :

```
$symbol(argument1,argument2...)
```

Le nombre d'arguments doit être identique au nombre de définitions de type d'argument.

Dans la définition de symbole, le premier argument correspond à `$p0`, le second argument correspond à `$p1`, etc.

Un symbole avec des arguments fonctionne comme une méthode Java. L'expression utilise les arguments comme des entrées et renvoie une valeur qui dépend des valeurs des arguments.

Exemple

```
<symbol>
   <name>$double</name>
   <eval>$p0*2</eval>
```

```
    <type>int</type>
    <args>
        <type>int</type>
    </args>
</symbol>
```

Ce symbole renvoie le double de la valeur de l'argument. Pour l'évaluer, indiquez un argument numérique : `$double(2)`, `$double($s1)`.

Définition de symboles d'itération
Dans la balise <symbolDefinitions>, vous pouvez définir un symbole d'itération à l'aide de la balise <iterationSymbol>. Un symbole d'itération représente une valeur qui est acquise par itération à travers un ensemble d'objets dans un tableau, une énumération ou une collection Java. Pour chacun des membres, l'associateur de demande évalue une ou plusieurs expressions de condition. Si une expression renvoie `true`, l'associateur de demande utilise le membre pour calculer la valeur de retour. Quand un membre respecte l'expression de condition, l'associateur de demande n'évalue pas le reste des membres.

Dans la balise <iterationSymbol>, insérez les balises suivantes :

<name>
Nom du symbole. Il s'agit d'une chaîne qui doit commencer par le caractère $.

<type>
Type de la valeur renvoyée par le symbole. Entrez cette valeur sous la forme d'un nom de classe Java complet ou d'une primitive Java. La définition du type de symbole est facultative. S'il n'est pas défini, l'associateur de demande essaye d'établir le type de zone en fonction de l'expression. Si l'associateur de demande ne peut pas déterminer le type de symbole avant qu'il évalue l'expression, les performances sont affectées. Pour optimiser les performances, il est donc préférable de spécifier le type.

<args>
Arguments associés au symbole. Cette balise est facultative ; si elle est définie, des arguments doivent être fournis pour calculer le symbole. Pour plus d'informations, voir «Définition des arguments de symbole», à la page 929.

<iterate over="*expression*">
Définit l'objet (tableau, énumération ou collection) qui contient les membres à itérer. L'expression doit renvoyer un objet du même type. L'associateur de demande itère sur ses membres jusqu'à ce que l'un d'entre eux provoque une expression de condition pour renvoyer `true`, ou qu'il ne reste plus de membre. Définissez les expressions d'itération dans les balises imbriquées dans cette balise, comme suit :

<test>
Définissez la condition et l'expression de retour dans cette balise. Une balise <iterate> peut contenir plusieurs balises <test>. Dans ce cas, l'associateur de demande les évalue tous. Si une expression de condition est vraie, le symbole retourne une valeur en utilisant l'expression de résultat dans la même balise <test> et aucune autre évaluation n'est exécutée.

<castTo>
Facultatif : si cette balise est présente, indiquez-y le nom d'un type Java sous la forme d'un nom de classe Java complet ou d'une primitive Java. L'associateur de demande transtype l'élément itéré dans ce type avant d'évaluer les expressions de condition et de retour. Si cette balise n'est pas présente, l'associateur de demande transtype un membre d'un tableau sur le type de base du tableau, et un membre d'une énumération ou d'une collection sur `java.lang.Object`. Pour un membre de tableau, le type de base du tableau est généralement le bon choix ; donc utilisez cette balise pour que l'associateur de demande itère sur une énumération ou une collection.

<condition>
Expression qui doit renvoyer une valeur booléenne. Utilisez `$iterElement` pour faire référence à l'élément itéré.

<return>
Si l'expression de la balise <condition> renvoie `true`, l'associateur de demande évalue l'expression dans la balise <return>. Le symbole d'itération renvoie la valeur que cette expression génère. Utilisez `$iterElement` pour faire référence à l'élément itéré.

<defaultValue>
Facultatif. Si l'associateur de demande a itéré sur tous les membres de l'objet, mais aucune expression de condition n'a renvoyé `true`, l'associateur de demande évalue l'expression dans la balise >defaultValue<. Le symbole d'itération retourne la valeur qui génère l'expression. Si cette balise est absente, la valeur par défaut renvoyée est `null`.

Exemples

```
<iterationSymbol>
  <name>$userNameCookieValue</name>
  <iterate over="$httpServletRequest.getCookies()">
     <test>
        <condition>$iterElement.getName().equals("nomUtilisateur")</condition>
        <return>$iterElement.getValue()</return>
     </test>
   </iterate>
</iterationSymbol>
```

Ce symbole recherche le cookie "nomutilisateur" et renvoie sa valeur. `$httpServletRequest.getCookies()` renvoie un tableau, dans quel cas l'élément <castTo> est inutile.

```
<iterationSymbol>
  <name>$headerNameStartingWithA</name>
  <iterate over="$httpServletRequest.getHeaderNames()">
    <test>
       <castTo>java.lang.String</castTo>
       <condition>$iterElement.startsWith("A")</condition>
       <return>$iterElement</return>
    </test>
  </iterate>
</iterationSymbol>
```

Ce symbole recherche l'en-tête dont le nom commence par "A" et renvoie son nom. `$httpServletRequest.getHeaderNames()` renvoie une énumération, dans quel cas l'élément <castTo> est obligatoire.

```
<iterationSymbol>
  <name>$determined_gender</name>
  <iterate over="$children">
    <test>
       <castTo>java.lang.String</castTo>
       <condition>$iterElement.equals("garçon")</condition>
       <return>"C'est un garçon"</return>
    </test>
    <test>
       <castTo>java.lang.String</castTo>
       <condition>$iterElement.equals("fille")</condition>
       <return>"C'est une fille"</return>
    </test>
  </iterate>
  <defaultValue>"inconnu"</defaultValue>
</iterationSymbol>
```

Ce symbole itère `$children`, qui doit être un tableau, une énumération ou une collection de chaînes. Si l'une des chaînes contient "garçon", l'expression renvoie "c'est un garçon". Si l'une des chaînes contient "fille", l'expression renvoie "c'est une fille". Enfin, si aucune chaîne dans l'objet `$children` ne contient "garçon" ou "fille", l'expression renvoie "inconnu".

Définition de symboles conditionnels
Dans la balise <symbolDefinitions>, vous pouvez définir un symbole conditionnel à l'aide de la balise <conditionalSymbol>. Un symbole conditionnel représente une valeur acquise en évaluant une série d'expressions conditionnelles. Si une expression renvoie `true`, l'associateur de demande utilise le

membre pour calculer la valeur de retour. Lorsqu'un membre rencontre l'expression de condition, l'associateur de demande évalue une expression de retour correspondante et renvoie le résultat. Une fois que l'associateur de demande trouve un résultat à renvoyer, il n'évalue pas d'autres d'expressions.

Dans la balise <conditionalSymbol>, utilisez les balises suivantes.

<name>
Nom du symbole. Il s'agit d'une chaîne qui doit commencer par le caractère $.

<type>
Type de la valeur renvoyée par le symbole. Entrez cette valeur sous la forme d'un nom de classe Java complet ou d'une primitive Java. La définition du type de symbole est facultative. S'il n'est pas défini, l'associateur de demande essaye d'établir le type de zone en fonction de l'expression. Si l'associateur de demande ne peut pas déterminer le type de symbole avant qu'il évalue l'expression, les performances sont affectées. Pour optimiser les performances, il est donc préférable de spécifier le type.

<args>
Arguments associés au symbole. Cette balise est facultative ; si elle est définie, des arguments doivent être fournis pour calculer le symbole. Pour plus d'informations, voir «Définition des arguments de symbole», à la page 929.

<if condition="*expression*">
L'attribut `condition` définit une expression de condition à calculer. L'expression doit renvoyer une valeur booléenne. Si la valeur est `true`, l'associateur de demande utilise le contenu de la balise <if> pour essayer de déterminer la valeur de retour. La balise <if> doit contenir l'un ou l'autre des contenus suivants, mais pas les deux :

- Une balise <return>. Cette balise contient une expression. Si l'expression de condition est vraie, l'associateur de demande évalue l'expression et renvoie le résultat.
- N'importe quel nombre de balises <if> imbriquées dans la balise <if>. Si l'expression de condition est vraie, l'associateur de demande traite les balises <if> imbriquées de la même manière qu'une balise <if> de haut niveau. En d'autres termes, il calcule l'expression dans l'attribut `condition` et si l'expression est vraie, il utilise le contenu de la balise et tente de déterminer la valeur de retour.

Important : Si une valeur de retour est déterminée, l'associateur de demande n'évalue pas d'autres expressions. Cependant, si une expression de condition contenue dans une balise <if> est satisfaite mais qu'elle contient d'autres balises <if> imbriquées et qu'aucune des expressions de condition associées n'est vérifiée, l'agent ne renvoie alors aucune valeur. Dans ce cas, l'associateur de demande continue à évaluer les expressions suivantes.

<defaultValue>
Facultatif. Si l'associateur de demande a évalué toutes les expressions de condition, mais qu'aucune n'a renvoyé `true`, l'associateur de demande évalue l'expression de la balise <defaultValue>. Le symbole conditionnel renvoie la valeur produite par l'expression. Si cette balise est absente, la valeur par défaut renvoyée est `null`.

Exemple

```
<symbol>
  <name>$GET</name>
  <eval>"GET"</eval>
</symbol>
<symbol>
  <name>$PUT</name>
  <eval>"PUT"</eval>
</symbol>
<conditionalSymbol>
  <name>$sessionAttribute</name>
  <if condition="$httpServletRequest.getSession(false) != null>
     <if condition="$httpServletRequest.getSession(false).getAttribute($GET)
!= null">
       <return>$httpServletRequest.getSession(false).getAttribute($GET)</return>
     </if>
     <if condition="true">
       <return>$httpServletRequest.getSession(false).getAttribute($PUT)</return>
      </if>
```

```
  </if>
</conditionalSymbol>
```

Ce symbole est supposé être une partie de l'associateur de demande de servlet. Tout d'abord, il vérifie si une session HTTP existe pour le servlet, sinon, le symbole renvoie `null`. Si une session est présente, le symbole vérifie si le servlet possède un attribut GET et renvoie la valeur de cet attribut. Sinon, il renvoie la valeur de l'attribut PUT. Si la deuxième expression de condition a pour résultat true, cette valeur est utilisée comme une clause else. Si la première condition est true, l'associateur de demande n'évalue pas d'autres expressions ; sinon, il poursuit vers la deuxième expression.

Définition des symboles de classe externe
Dans la balise <symbolDefinitions>, vous pouvez définir une classe externe à l'aide de la balise <externalClassSymbol>. Un symbole de classe externe représente une classe Java externe. La définition d'un symbole de classe externe est facultative car vous pouvez utiliser des classes Java externes directement dans les expressions. Toutefois, il pourrait améliorer la lisibilité de la configuration de l'associateur de demande.

Dans la balise <externalClassSymbol>, insérez les balises suivantes :

<name>
Nom du symbole. Il s'agit d'une chaîne qui doit commencer par le caractère $.

<className>
Nom de la classe définie par le client.

Important : Pour faire référence à une classe Java dans la configuration de l'associateur de demande, que ce soit dans une définition de symbole de classe externe ou dans une expression, vous devez ajouter le chemin complet et le nom du fichier JAR qui contient la classe à la balise <requestMapperClassPath> dans la balise <runtimeConfiguration>.

Une fois que vous avez défini un symbole de classe externe, vous pouvez faire référence à cette classe par le nom du symbole. Vous pouvez également consulter les méthodes et les zones statiques de la classe en utilisant le symbole.

Exemple

```
<externalClassSymbol>
  <name>$rand</name>
  <className>user.class.Random</className>
</externalClassSymbol>
```

Ce symbole fait référence à une classe écrite par l'utilisateur en générant un nombre aléatoire. Le chemin d'accès complet et le nom du fichier JAR qui contient cette classe doivent être présents dans la balise <requestMapperClassPath> au sein de la balise <runtimeConfiguration>.

Pour faire référence à la méthode statique `user.class.Random.generate()` dans une expression, vous pouvez utiliser le symbole externe :

```
$rand.generate()
```

Mappage de valeurs à des clés de contexte
Dans la balise <requestMapperDefinition>, mappez des valeurs aux clés de contexte à l'aide de la balise <selection>. Ce mappage fournit les modifications dans les informations de surveillance.

Vous pouvez mapper des valeurs aux clés de sortie définies pour le type de demande. Pour plus d'informations, voir Tableau 233, à la page 939.

Si aucune valeur n'est mappée à une clé après l'évaluation de la configuration de l'associateur de demande, ITCAM utilise la valeur d'origine extraite de la demande.

Dans la balise <selection>, insérez les balises suivantes.

<matchCriteria>
Expression qui doit renvoyer une valeur booléenne. Le mappage qui est défini dans cette balise est uniquement utilisé si cette expression renvoie `true`.

<mapTo>
Définit une clé et la valeur à lui associer. Dans cette balise, une balise <key> contient la clé et une balise <value> contient la valeur.

<selection>
Vous pouvez imbriquer des balises <selection> les unes dans les autres.

Si des balises <selection> sont imbriquées, le mappage imbriqué est uniquement utilisé si à la fois la première expression <matchCriteria> et les expressions imbriquées renvoient `true`.

Vous pouvez utiliser plusieurs balises <selection> dans une balise <requestMapperDefinition> ou dans une autre balise <selection>. Si une même clé est associée plusieurs fois dans plusieurs balises <selection> au même niveau d'imbrication (c'est-à-dire dans la même balise parent), le premier mappage pour lequel l'expression <matchCriteria> a retourné `true` est utilisé.

Ne mappez pas la même clé à la fois dans la balise <selection> de niveau supérieur et dans les balises imbriquées.

En règle générale, utilisez la valeur <matchCriteria> `true` comme valeur "else" pour la dernière balise "selection" dans un niveau d'imbrication. Si vous souhaitez mapper des valeurs différentes pour différents cas, utilisez plusieurs balises <selection> dans la balise externe ; chacune peut contenir des critères et des valeurs propres à chaque cas particulier. La dernière balise, avec la valeur `true`, prévoit les cas où les informations disponibles ne satisfont aucun des critères.

Exemples

```
<selection>
   <matchCriteria>true</matchCriteria>
   <mapTo>
      <key>Result</key>
      <value>$s1</value>
   </mapTo>
</selection>
```

Dans cette configuration de mappage, `Result` est mappé à la valeur du symbole `$s1`.

```
<matchCriteria>true</matchCriteria>
   <selection>
      <matchCriteria>$b1</matchCriteria>
      <mapTo>
         <key>Result</key>
         <value>1</value>
      </mapTo>
   </selection>
   <selection>
      <matchCriteria>true</matchCriteria>
      <mapTo>
         <key>Result</key>
         <value>2</value>
      </mapTo>
</selection>
```

Dans cette configuration de mappage, le symbole `$b1` doit renvoyer une valeur booléenne. `Result` a pour valeur 1 si `$b1` renvoie `true` et a pour valeur 2 si `$b1` renvoie `false`. Si `$b1` renvoie `true`, l'associateur de demande utilise le mappage pour `Result` dans la première balise <selection> ; le mappage de la même clé dans la seconde balise n'est pas utilisé.

Définition de demandes personnalisées
Par défaut, seuls certains types de méthodes et de classes Java sont surveillés par le collecteur de données en tant que demandes. Les servlets, les pages JSP, les méthodes métier à base d'EJB et

certaines API Java EE standard sont reconnues comme des demandes. Vous pouvez désigner des classes et méthodes supplémentaires en tant que *demandes personnalisées*.

Pourquoi et quand exécuter cette tâche

Pour activer la surveillance des demandes personnalisées par le collecteur de données, définissez celles-ci dans un fichier XML et définissez la propriété `am.camtoolkit.gpe.customxml.custom` dans le fichier de propriétés personnalisées du kit d'outils.

Par exemple, le collecteur de données ne reconnaît pas les classes Struts Action en tant que demandes par défaut. Toutefois, vous pouvez configurer des définitions de demande personnalisées afin que les actions soient reconnues comme des demandes imbriquées.

Procédure

Pour activer la surveillance des demandes personnalisées et désigner une ou plusieurs méthodes en tant que demandes personnalisées, procédez comme suit :

1. Effectuez une copie du fichier *base_cd*`/itcamdc/etc/custom_requests.xml` dans un emplacement temporaire. Ouvrez ensuite la copie du fichier dans un éditeur de texte.
2. Modifiez les paramètres dans le fichier.

   Le tableau suivant décrit les paramètres modifiables :

Tableau 232. Paramètres du fichier de configuration des demandes personnalisées

Nom de la balise	Description
`edgeRequest`	Identifie une ou plusieurs méthodes d'application qui doivent être de type BCI (Byte-Code-Instrumented) pour le traitement des demandes personnalisées. La modification des balises `requestName`, `Matches`, `type` et `methodName` dans la balise `edgeRequest` permet de personnaliser la sélection. Chaque balise `edgeRequest` doit contenir précisément une balise `methodName` et une ou plusieurs balises `Matches`. Plusieurs balises `edgeRequest` peuvent être indiquées.
`requestName`	Définit un nom unique pour cette demande. Le nom de la demande s'affiche pour l'utilisateur lorsque les entrées et les sorties de la méthode sont tracées.
`Matches`	Identifie une ou plusieurs classes contenant les méthodes qui doivent être de type BCI (Byte-Code-Instrumented) pour le traitement des demandes personnalisées. Il peut y avoir plusieurs balises `Matches` dans une seule balise `edgeRequest`.
`type`	Indique si une classe doit être une classe système ou une classe d'application pour concorder avec la balise `edgeRequest`.
`methodName`	Identifie les noms des méthodes dans l'une des classes identifiées par la balise `Matches` et qui doivent être de type BCI (Byte-Code-Instrumented) pour le traitement des demandes personnalisées. Une seule balise `methodName` peut être indiquée dans chaque balise `edgeRequest`.
`requestMapper`	Facultatif. Si cette balise est indiquée, le collecteur de données utilise un associateur de demande afin de déterminer les informations qui identifient la demande. Vous pouvez définir des méthodes non standard pour extraire ces informations. Pour plus d'informations sur l'activation et la définition des associateurs de demande, voir «Personnalisation du mappage des informations des demandes», à la page 926.

Tableau 232. Paramètres du fichier de configuration des demandes personnalisées (suite)

Nom de la balise	Description
A faire : Les balises `Matches` et `methodName` peuvent inclure des caractères génériques. Le mécanisme des caractères génériques est décrit ci-après : • L'astérisque (*) représente zéro, une ou plusieurs occurrences d'un caractère quelconque lorsqu'il est utilisé seul. S'il est imbriqué dans une séquence de caractères (par exemple, `java.*.String`), il représente zéro, une ou plusieurs occurrences d'un caractère quelconque excepté le séparateur de module (.). • Deux points (..) peuvent être utilisés pour définir tous les sous-packages. Ils correspondent à toute suite de caractères commençant et finissant par le séparateur de module (.). Par exemple, `java..String` correspond à `java.lang.String` et `com.ibm..*` correspond à toute déclaration commençant par `com.ibm`.	

Par exemple, une application dont le nom de module est `com.mycompany.myapp` doit remplir les conditions suivantes :

- Dans la classe `Customer`, la méthode `creditCheck()` doit être traitée comme une demande personnalisée appelée `CreditCheck`.
- Dans la classe `Supplier`, la méthode `inventoryCheck()` doit être traitée comme une demande personnalisée appelée `SupplyCheck`.

Le contenu du fichier `custom_requests.xml` personnalisé qui permet de satisfaire ces conditions est le suivant :

```
<customEdgeRequests>
      <edgeRequest>
              <requestName>CreditCheck</requestName>
              <Matches>com.mycompany.myapp.Customer</Matches>
              <type>application</type>
              <methodName>creditCheck</methodName>
      </edgeRequest>
      <edgeRequest>
              <requestName>SupplyCheck</requestName>
              <Matches>com.mycompany.myapp.Supplier</Matches>
              <type>application</type>
              <methodName>inventoryCheck</methodName>
      </edgeRequest>
</customEdgeRequests>
```

3. Effectuer l'une des étapes suivantes :
   - Sauvegardez le fichier dans le répertoire *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom. Ensuite, dans le fichier de propriétés personnalisées de la boîte à outils, définissez la propriété `am.camtoolkit.gpe.customxml.custom` avec le nom (sans chemin d'accès) du fichier que vous avez modifié à l'étape «2», à la page 935.
   - Sauvegardez le fichier dans l'un des répertoires de votre ordinateur. Ensuite, dans le fichier de propriétés personnalisées de la boîte à outils, définissez la propriété `am.camtoolkit.gpe.customxml.custom` avec le nom et le chemin d'accès du fichier que vous avez modifié à l'étape «2», à la page 935.

Pour plus d'informations sur le fichier de propriétés personnalisées du kit d'outils, voir «Fichier de propriétés du kit d'outils», à la page 917.

Activation d'un associateur de demande

Pour activer un associateur de demande pour un type de demande, modifiez le fichier de configuration personnalisée du kit d'outils ou le fichier de configuration personnalisée globale du kit d'outils. Les procédures sont différentes pour les demandes communes et pour les demandes personnalisées.

Avant de commencer

Définissez la configuration de l'associateur de demande dans un fichier XML. Ensuite, placez ce fichier XML dans le même répertoire que le fichier de propriétés du kit d'outils.

- Pour activer l'associateur de demande pour toutes les instances du serveur d'applications, placez-le dans le répertoire *base_cd*/runtime/custom.
- Pour activer l'associateur de demande pour une instance du serveur d'applications, placez-le dans le répertoire *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom/.

Pour plus d'informations sur la syntaxe du fichier XML, voir «Syntaxe du fichier XML», à la page 926.

Pourquoi et quand exécuter cette tâche

Editez le fichier toolkit_custom.properties ou le fichier toolkit_global_custom.properties pour activer l'associateur de demande pour une ou toutes les instances du serveur d'applications.

Procédure

- Pour activer un associateur de demande pour des demandes communes, procédez comme suit :
  a) Dans un éditeur de texte, ouvrez un des fichiers de configuration personnalisée suivants du kit d'outils :
     – Pour activer l'associateur de demande pour toutes les instances de serveur d'applications, ouvrez le fichier *base_cd*/runtime/custom/toolkit_global_custom.properties.
     – Pour activer l'associateur de demande pour une instance de serveur d'applications, ouvrez le fichier *base_cd*/runtime/*version_serveur_app.nom_noeud.nom_profil.nom_serveur*/custom/toolkit_custom.properties.
  b) Editez le fichier de propriétés du kit d'outils comme suit :
     – Ajoutez une ligne définissant la propriété d'activation pour ce type de demande sur true. Pour plus d'informations, voir Tableau 233, à la page 939.
     – Ajoutez une ligne définissant la propriété am.camtoolkit.gpe.customxml.* sur le nom du fichier XML de l'associateur. Utilisez des valeurs uniques au lieu du symbole "*". Pour plus d'informations, voir «Syntaxe du fichier XML», à la page 926.
  c) Sauvegardez et fermez le fichier de propriétés.

  Exemple :

  Pour activer un associateur de demande qui est défini dans renameDataSource.xml pour le type de demande SQL, ajoutez les lignes suivantes dans le fichier de configuration personnalisée du kit d'outils ou dans le fichier de configuration personnalisée globale du kit d'outils :

```
com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper=true
am.camtoolkit.gpe.customxml.renameDataSource=renameDataSource.xml
```

- Pour activer un associateur de demande pour des demandes personnalisées, effectuez les étapes suivantes :
  a) Sous la balise <edgerequest> dans le fichier XML de définition de demandes personnalisées, créez la balise >requestMapper<. Insérez un nom de type d'associateur de demande unique dans cette balise. Pour plus d'informations sur la définition des demandes personnalisées, voir «Définition de demandes personnalisées», à la page 934.

b) Dans le fichier XML de l'associateur de demande, utilisez le nom unique de type d'associateur de demande dans l'attribut `type` de la balise >requestMapperDefinition<.

c) Dans un éditeur de texte, ouvrez un des fichiers de configuration personnalisée suivants du kit d'outils :

- Pour activer l'associateur de demande pour toutes les instances de serveur d'applications, ouvrez le fichier *base_cd*`/runtime/custom/toolkit_global_custom.properties`.
- Pour activer l'associateur de demande pour une instance de serveur d'applications, ouvrez le fichier *base_cd*`/runtime/`*version_serveur_app.nom_noeud.nom_profil.nom_serveur*`/custom/toolkit_custom.properties`.

d) Editez le fichier de propriétés du kit d'outils pour ajouter une ligne définissant la propriété `am.camtoolkit.gpe.customxml.*` sur le nom du fichier XML de l'associateur. Utilisez des valeurs uniques au lieu du symbole "*". Pour plus d'informations, voir «Syntaxe du fichier XML», à la page 926.

e) Sauvegardez et fermez le fichier de propriétés.

Exemple :

Pour activer un associateur de demande qui est défini dans `customMapper.xml` pour le type de demande personnalisée `SupplyCheck` qui est défini dans le fichier `custom_requests.xml`, effectuez les étapes suivantes :

1. Utilisez la définition suivante dans le fichier `custom_requests.xml` :

```
<customEdgeRequests>
  <edgeRequest>
    <requestName>SupplyCheck</requestName>
    <Matches>com.mycompany.myapp.Supplier</Matches>
    <type>application</type
    <methodName>inventoryCheck</methodName>
    <requestMapper>customMapper</requestMapper>
  </edgeRequest>
</customEdgeRequests>
```

2. Dans le fichier `customMapper.xml`, assurez-vous que le nom du type est défini :

```
<requestMapperDefinition type="customMapper">
```

3. Ajoutez la ligne suivante dans le fichier de configuration personnalisée du kit d'outils ou dans le fichier de configuration personnalisée globale du kit d'outils :

```
am.camtoolkit.gpe.customxml.customMapper=customMapper.xml
```

Noms et données d'entrée et de sortie de l'associateur de demande

Les tableaux suivants répertorient les informations nécessaires pour configurer et activer des associateurs de demande pour les différents types de demande.

La signification de chaque en-tête de tableau est expliquée comme suit :

Type de demande
Type de la demande.

Propriété d'activation
Pour activer l'associateur de demande, affectez à cette propriété la valeur `true` dans le fichier `toolkit_custom.properties` ou `toolkit_global_custom.properties`.

Important : Si vous copiez cette valeur depuis le tableau, supprimez les espaces et les retours à la ligne.

Nom de type d'associateur de demande
Affectez cette valeur à l'attribut `type` de la balise <requestMapperDefinition> dans le fichier XML de définition de l'associateur de demande.

Noms des symboles de données d'entrée
Symboles représentant les informations de demande. Vous pouvez utiliser ces symboles dans les expressions des définitions de l'associateur de demande. Pour plus d'informations, voir «Définition d'une expression», à la page 927.

Clés de contexte des données de sortie
Pour apporter des modifications aux informations de surveillance, vous pouvez attribuer des valeurs à ces clés dans la définition de l'associateur de demande. Pour plus d'informations, voir «Mappage de valeurs à des clés de contexte», à la page 933.

Tableau 233. Propriétés d'activation et noms de type de l'associateur de demande

Type de demande	Propriété d'activation	Nom de type d'associateur de demande
Servlet	`com.ibm.tivoli.itcam.toolkit.ai.enable.servletrequestmapper`	`servlet`
JNDI	`com.ibm.tivoli.itcam.toolkit.ai.enable.jndirequestmapper`	`jndiLookup`
Demande personnalisée		Définie par l'utilisateur dans la définition edgeRequest
EJB	`com.ibm.tivoli.itcam.toolkit.ai.enable.ejbrequestmapper`	`ejb`
JCA	`com.ibm.tivoli.itcam.toolkit.ai.enable.jcarequestmapper`	`jca`
Source de données JDBC	`com.ibm.tivoli.itcam.toolkit.ai.enable.datasourcerequestmapper`	`dataSource`
Instruction SQL JDBC	`com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper`	`sqlStatement`
JMS	`com.ibm.tivoli.itcam.toolkit.ai.enable.jmsrequestmapper`	`jms`
Service Web JAX-RPC	`com.ibm.tivoli.itcam.toolkit.ai.enable.webservicerequestmapper`	`webServices`
Service Web Axis	`com.ibm.tivoli.itcam.toolkit.ai.enable.webservicerequestmapper`	`webServices`
MQI	`com.ibm.tivoli.itcam.toolkit.ai.enable.mqrequestmapper`	`mqi`
EJB	`com.ibm.tivoli.itcam.toolkit.ai.enable.ejbrequestmapper`	`ejb`
Fabrique de connexions JDBC	`com.ibm.tivoli.itcam.toolkit.ai.enable.sqlconnectfactoryrequestmapper`	`connectionFactory`
SCA	`com.ibm.tivoli.itcam.toolkit.ai.enable.scarequestmapper`	`sca`
Service Web JAX-WS	`com.ibm.tivoli.itcam.toolkit.ai.enable.webservicerequestmapper`	`webServices`

Tableau 233. Propriétés d'activation et noms de type de l'associateur de demande (suite)

Type de demande	Propriété d'activation	Nom de type d'associateur de demande
WebSphere Portal Server Portal (extension de la classe `org.apache.jetspeed.portlet.Portlet`)	`com.ibm.tivoli.itcam.toolkit.ai.enable.portalrequestmapper`	`portalPortal`
Portail WebSphere Portal Server version 6.1, 7 et 8 (implémentation de l'interface `javax.portlet.Portlet`)	`com.ibm.tivoli.itcam.toolkit.ai.enable.portal6requestmapper`	`Portal6Portal`

Important : Il n'existe aucune manière significative de configurer l'associateur de demande personnalisé pour les types de requête qui ne sont pas répertoriés dans le Tableau 233, à la page 939.

Tableau 234. Données d'entrée et de sortie de l'associateur de demande

Type de demande	Noms des symboles de données d'entrée	Clés de contexte des données de sortie
Servlet	Pour plus d'informations, voir Tableau 235, à la page 944.	**remappedURI** définit un identificateur URI renommé. **remappedURL** définit une adresse URL renommée. **appName** définit un nom d'application renommée. **userid** définit l'ID utilisateur associé à la demande.
JNDI	• **$jndiContext** objet contextuel • **$lookup** chaîne de recherche • **$context** "JNDIlookup"	**renamedLookup** définit une chaîne de recherche renommée.
Demande personnalisée	• **$this** objet ‘this' associé à la méthode de la demande personnalisée • **$0** arguments communiqués à la méthode de la demande personnalisée, spécifiés sous la forme d'un tableau d'objets • **$className** nom de la classe de la demande personnalisée • **$methodName** nom de la méthode de la demande personnalisée • **$context** nom de la demande d'origine issu de la définition edgeRequest	**customRequestName** définit le nom de la demande personnalisée renommée

Tableau 234. Données d'entrée et de sortie de l'associateur de demande (suite)

Type de demande	Noms des symboles de données d'entrée	Clés de contexte des données de sortie
EJB	• **$ejb** objet de l'implémentation EJB • **$appName** nom de l'application • **$ejbType** type de l'EJB • **$className** nom de classe de l'objet d'implémentation EJB • **$methodName** nom de la méthode métier EJB • **$context** "EJBBusinessMethod"	**appName** définit le nom de l'application renommée **ejbType** définit le type EJB renommé **className** définit le nom de la classe renommée **methodName** définit le nom de la méthode renommée
JCA	• **$interaction** objet Interaction • **$interactionSpec** objet InteractionSpec • **$record** objet Record • **$context** "J2Cexecute"	**lookupName** est le nom de la recherche renommée **productName** est le nom du produit renommé **productVersion** est la version du produit renommé
Source de données JDBC	• **$this** objet source de données ou objet pilote • **$dataSource** objet $this, transtypé en objet source de données • **$driver** objet $this, transtypé en objet pilote • **$dataSourceName** nom de la source de données, tel que java.lang.String • **$context** indique le type de demande "JDBCgetConnection" ou "JDBCgetConnection FromDriver"	**dataSourceName** est le nom de la source de données renommée, si l'objet $this est une source de données **url** est l'adresse URL du pilote renommé, si l'objet $this est un pilote
Instruction SQL JDBC	• **$this** instruction SQL ou connexion SQL • **$sqlText** contient le texte SQL sous la forme java.lang.String, si l'objet $this est une instruction SQL • **$sqlStatement** objet $this, transtypé en instruction SQL • **$sqlConnection** objet $this, transtypé en connexion SQL • **$dataSourceName** nom de la source de données • **$context** indique le type de demande : "JDBCexecute", JDBCexecuteQuery", "JDBCexecuteUpdate", "JDBCcreateStatement", "JDBCprepareStatement"	**dataSourceName** est le nom de la source de données renommée **sqlText** est le texte SQL renommé

Tableau 234. Données d'entrée et de sortie de l'associateur de demande (suite)

Type de demande	Noms des symboles de données d'entrée	Clés de contexte des données de sortie
JMS	• **$this** est l'objet ‘this' de la méthode instrumentée. Peut être QueueBrowser, MessageConsumer, MessageProducer ou MessageListener • **$0** objet de file d'attente pour une demande d'envoi, ou objet de rubrique pour une demande de publication • **$queueBrowser** objet $this, transtypé en objet de type QueueBrowser • **$messageConsumer** objet $this, transtypé en objet de type MessageConsumer • **$messageProducer** objet $this, transtypé en objet de type MessageProducer • **$messageListener** objet $this, transtypé en objet de type MessageListener • **$queue** objet $0, transtypé en file d'attente • **$topic** objet $0, transtypé en rubrique • **$context** indique le type de demande : "JMSreceive", "JMSsend", "JMSbrowse", "JMSpublish", "JMSonmessage"	**queueName** est le nom de la file d'attente renommée **providerURL** est l'URL du fournisseur renommé **topicName** est le nom de la rubrique renommée
Service Web JAX-RPC	• **$messageContext** encapsuleur IMessageContextWrapper • **$appName** nom de l'application • **$requestName** nom de la demande par défaut • **$url** adresse URL • **$context** indique le type de demande : "WebServicesJaxRpc ProviderRequest", "WebServicesJaxRpc ClientRequest"	**appName** est le nom de l'application renommée **requestName** est le nom de la demande renommée **url** est l'adresse URL renommée
Service Web Axis	• **$messageContext** encapsuleur IMessageContextWrapper • **$appName** nom de l'application • **$requestName** nom de la demande par défaut • **$url** adresse URL • **$context** indique le type de demande : "WebServicesAxisClient Request", "WebServicesAxis ProviderRequest"	**appName** est le nom de l'application renommée **requestName** est le nom de la demande renommée **url** est l'adresse URL renommée

Tableau 234. Données d'entrée et de sortie de l'associateur de demande (suite)

Type de demande	Noms des symboles de données d'entrée	Clés de contexte des données de sortie
MQI	• **$queue** objet MQQueue, s'il est connu • **$qmgr** objet MQQueueManager, s'il est connu • **$message** objet MQMessage ou MQMsg2, s'il est connu • **$session** objet MQSESSION, s'il est connu • **$getMsgOptions** objet MQGetMessageOptions, s'il est connu • **$qmgrName** nom du gestionnaire de files d'attente • **$queueName** nom de la file d'attente • **$context** indique le type de demande MQ : "MQCONN", "MQCONNX", "MQDISC", "MQBACK", "MQBEGIN", "MQCLOSE", "MQCMIT", "MQINQ", "MQOPEN", "MQSET", "MQGET", "MQPUT", "MQPUT1", "MQGETBROWSE"	**qmgrName** est le nom du gestionnaire de files d'attente renommé **qname** est le nom de la file d'attente renommée
EJB	• **$appName** nom de l'application • **$ejbType** type de l'EJB • **$className** nom de classe de l'objet d'implémentation EJB • **$methodName** nom de la méthode métier EJB • **$context** "EJBBusinessMethod"	**appName** définit le nom de l'application renommée **ejbType** définit le type EJB renommé **className** définit le nom de la classe renommée **methodName** définit le nom de la méthode renommée
Fabrique de connexions JDBC	• **$connectionFactory** fabrique de connexions • **$dataSourceName** nom de la source de données • **$context** "JDBCgetConnection"	**dataSourceName** est le nom de la source de données renommée
SCA	• **$uri** identificateur URI • **$operationName** nom d'opération • **$context** indique le type de demande : "SCA_Generic", "SCA_Ref", "SCA_Target"	**uri** est l'identificateur URI renommé **operationName** est le nom de l'opération renommée

Tableau 234. Données d'entrée et de sortie de l'associateur de demande (suite)

Type de demande	Noms des symboles de données d'entrée	Clés de contexte des données de sortie
Service Web JAX-WS	• **$messageContext** encapsuleur IMessageContextWrapper • **$appName** nom de l'application • **$requestName** nom de la demande par défaut • **$url** adresse URL • **$context** indique le type de demande : "WebServicesJAXWS ClientRequest", "WebServicesJAXWS ProviderRequest", "WebServicesJAXWS AsyncRequest"	**appName** est le nom de l'application renommée **requestName** est le nom de la demande renommée **url** est l'adresse URL renommée
WebSphere Portal Server Portal (extension de la classe `org.apache.jetspeed.portlet.Portlet`)	• **$portletAdapter** PortletAdapter • **$portletRequest** PortletRequest • **$portletResponse** PortletResponse • **$portletName** nom du portlet • **$pageTitle** titre de la page • **$url** adresse URL de la demande • **$userid** ID utilisateur de la demande • **$context** "Portal.Portlet"	**portletName** est le nom du portlet renommé **title** est le titre de la page renommée **url** est l'adresse URL renommée **userid** est l'ID utilisateur renommé
Portail WebSphere Portal Server version 6.1, 7 et 8 (implémentation de l'interface `javax.portlet.Portlet`)	• **$portlet** Portlet • **$renderRequest** RenderRequest • **$renderResponse** RenderResponse • **$portletName** Nom du portlet • **$pageTitle** Titre de la page • **$url** Adresse URL de la demande • **$userid** ID utilisateur de la demande • **$context** "Portal.Portlet"	**portletName** Nom du portlet renommé **title** Titre de la page renommée **url** URL renommée **userid** ID utilisateur renommé

Pour les demandes de servlet, il existe un grand nombre de symboles de données d'entrée.

Tableau 235. Noms des symboles de données d'entrée disponibles pour les demandes de servlet

Nom du symbole	Type de valeur	Contenu du symbole
$context	String	"ServletMethod"
$servlet	javax.servlet.http.HttpServlet	Objet HttpServlet associé à la demande de servlet
$httpServletRequest	javax.servlet.http.HttpServletRequest	Objet HttpServletRequest associé à la demande de servlet
$httpServletResponse	javax.servlet.http.HttpServletResponse	Objet HttpServletResponse associé à la demande de servlet
$appName	java.lang.String	Nom d'application associé au servlet

Tableau 235. Noms des symboles de données d'entrée disponibles pour les demandes de servlet (suite)		
Nom du symbole	**Type de valeur**	**Contenu du symbole**
$URL	java.lang.StringBuffer	Adresse URL que le client a utilisée pour faire la demande
$RemoteUser	java.lang.String	Nom de connexion de l'utilisateur qui effectue cette demande, s'il est authentifié
$URI	java.lang.String	Partie de l'URL de la demande allant du nom de protocole jusqu'à la chaîne de requête
$ServletPath	java.lang.String	Partie de l'URL de la demande qui appelle le servlet.
$SessionID	javax.servlet.http.HttpSession	Session en cours associée à la demande
$QueryString	java.lang.String	Chaîne de demande qui se trouve dans l'adresse URL de la demande, après le chemin.
$SessionAttribute	java.lang.String	Ce symbole paramétré retourne une valeur d'attribut de session. Il dispose d'un paramètre, le nom d'attribut (doit être une chaîne). Par exemple, `$SessionAttribute("attr1")` renvoie la valeur de l'attribut attr1.
$cookie	javax.servlet.http.Cookie	Ce symbole paramétré retourne un cookie nommé. Il dispose d'un paramètre, le nom du cookie (doit être une chaîne). Par exemple, `$cookie("cookie1")` renvoie la valeur de l'attribut cookie1.

Exemples de définition d'associateur de demande
Les exemples suivants illustrent l'utilisation de l'associateur de demande.

Changement du nom d'application de servlet
Dans cet exemple, le nom d'application figurant dans une demande de servlet est remplacé par l'URI et la chaîne de requête.

Le fichier *base_cd*`/runtime/changeAppname.xml` contient la définition d'associateur de demande suivante :

```
<gpe>
   <runtimeConfiguration>
         <requestMapperDefinition type="servlet">
               <selection>
                     <matchCriteria>true</matchCriteria>
                     <mapTo>
                           <key>appName</key>
                           <value>$URI + “.” + $QueryString</value>
                     </mapTo>
               </selection>
         </requestMapperDefinition>
```

```
   </runtimeConfiguration>
</gpe>
```

Changement de nom d'une source de données
Dans cet exemple, le nom de la source de données figurant dans une demande SQL est remplacé par un autre nom plus facile à comprendre.

Le fichier *base_cd*/runtime/renameDataSource.xml contient la définition suivante de l'associateur de demande :

```
<gpe>
 <runtimeConfiguration>
   <requestMapperDefinition type=”sqlStatement”>
      <selection>
         <matchCriteria>$dataSourceName != null</matchCriteria>
         <selection>
           <matchCriteria>$dataSourceName.equals("jdbc/TradeDataSource")
</matchCriteria>
           <mapTo>
             <key>dataSourceName</key>
             <value>"Daytrader Data Source"</value>
           </mapTo>
         </selection>
         <selection>
           <matchCriteria>$dataSourceName.equals("jdbc/LongDataSource")
</matchCriteria>
           <mapTo>
             <key>dataSourceName</key>
             <value>"Long term trader Data Source"</value>
           </mapTo>
         </selection>
      </selection>
   </requestMapperDefinition>
 </runtimeConfiguration>
<gpe>
```

La première balise <selection> garantit que $dataSourceName n'a pas la valeur null. Puis, la deuxième balise <selection> peut sans risque évaluer $dataSourceName.equals().

Si la première balise <selection> est absente et qu'une valeur null est transmise pour $dataSourceName, l'associateur de demande génère une exception. Dans ce cas, il manquera des données de surveillance dans le résultat de la demande.

Pour activer cet associateur de demande, le fichier *base_cd*/runtime/toolkit_global_custom.properties contient les lignes suivantes :

```
com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper=true
am.camtoolkit.gpe.customxml.renameDataSource=renameDataSource.xml
```

Suppression des informations sensibles d'une demande SQL
Dans cet exemple, une application inclut des numéros de sécurité sociale dans des demandes SQL. L'associateur de demande supprime les numéros de la version de la demande que l'utilisateur peut afficher.

Dans les demandes SQL, le numéro de sécurité sociale est répertorié avec le nom de colonne SS, SS = *numéro*. L'associateur de demande recherche la chaîne SS = et supprime les neuf symboles après cette chaîne.

Le fichier *base_cd*/runtime/removeSSN.xml contient la définition suivante de l'associateur de demande :

```
<gpe>
    <runtimeConfiguration>
         <requestMapperDefinition type="sqlStatement">
             <symbolDefinitions>
                 <symbol>
                     <name>$offsetOfSS</name>
                     <eval>$sqlText.indexOf("SS = ")</eval>
                 </symbol>
                 <symbol>
```

```
                    <name>$sqlTextContainsSS</name>
<eval>$sqlText != null AND $offsetOfSS > 0 AND $sqlText.length() GE
$offsetOfSS+16</eval>
                </symbol>
                <conditionalSymbol>
                    <name>$sqlTextPriorToSSKeyword</name>
                    <type>java.lang.String</type>
                    <defaultValue>""</defaultValue>
                    <if condition="$sqlTextContainsSS">
                      <return>$sqlText.substring(0, $offsetOfSS+5)</return>
                    </if>
                </conditionalSymbol>
                <conditionalSymbol>
                    <name>$sqlTextAfterSS</name>
                    <type>java.lang.String</type>
                    <defaultValue>""</defaultValue>
                    <if condition="$sqlTextContainsSS">
                      <return>$sqlText.substring($offsetOfSS+16)</return>
                    </if>
                </conditionalSymbol>
            </symbolDefinitions>
            <selection>
                 <matchCriteria>$sqlText != null AND $sqlText.length() >
0</matchCriteria>
                 <selection>
                      <matchCriteria>$sqlTextContainsSS</matchCriteria>
                      <mapTo>
                           <key>sqlText</key>
                           <value>$sqlTextPriorToSSKeyword + "?" +
$sqlTextAfterSS</value>
                      </mapTo>
                 </selection>
            </selection>
        </requestMapperDefinition>
    </runtimeConfiguration>
</gpe>
```

Pour activer cet associateur de demande, le fichier *base_cd*/runtime/toolkit_global_custom.properties contient les lignes suivantes :

```
com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper=true
am.camtoolkit.gpe.customxml.renameDataSource=removeSSN.xml
```

Configuration de l'Agent WebSphere Applications pour surveiller WebSphere Extreme Scale

Après avoir installé l'Agent WebSphere Applications, vous pouvez effectuer une configuration supplémentaire pour surveiller WebSphere Extreme Scale (WXS) dans un environnement autonome ou WebSphere Application Server.

Pourquoi et quand exécuter cette tâche

Les étapes de configuration varient selon le mode d'installation de WebSphere Extreme Scale et l'activation ou non de la sécurité. Avant d'exécuter le processus de configuration, effectuez les opérations ci-dessous.

Procédure

1. Confirmez le mode d'installation de WebSphere Extreme Scale.

   Mode autonome
   WebSphere Extreme Scale est installé dans un environnement sans WebSphere Application Server.

   Mode WAS imbriqué
   WebSphere Extreme Scale est installé dans un environnement WebSphere Application Server.
2. Confirmez si la sécurité est activée pour WebSphere Extreme Scale. Si un client Java sécurisé est utilisé en mode WebSphere Application Server imbriqué, vous devez suivre la procédure de connexion de sécurité.
3. Cliquez sur les liens ci-dessous pour obtenir les instructions voulues.

- Pour configurer WebSphere Extreme Scale dans un environnement autonome, cliquez sur «Configuration de la surveillance WebSphere Extreme Scale dans un environnement autonome», à la page 948.
- Pour configurer WebSphere Extreme Scale dans un environnement imbriqué sans sécurité, cliquez sur «Configuration de la surveillance WebSphere Extreme Scale dans l'environnement WebSphere sans activation de la sécurité», à la page 949.
- Pour configurer WebSphere Extreme Scale dans un environnement imbriqué où la sécurité est activée, cliquez sur «Configuration de la surveillance WebSphere Extreme Scale dans l'environnement WebSphere où la sécurité est activée», à la page 950.

Configuration de la surveillance WebSphere Extreme Scale dans un environnement autonome
Cette rubrique indique comment configurer l'Agent WebSphere Applications lorsque WebSphere Extreme Scale est installé dans un environnement sans WebSphere Application Server.

Procédure

1. Arrêtez Agent WebSphere Applications.
   a) Accédez au répertoire *rép_install* où vous avez installé l'Agent WebSphere Applications.
   b) Exécutez la commande `bin/was-agent.sh stop`.
2. Exécutez le script de configuration.

   ```
   rép_install/code_plateforme/yn/bin/wxs-agent-config.sh config
   ```

   Où
   - *rép_install* correspond au répertoire d'installation de l'Agent WebSphere Applications.
   - *code_plateforme* est le code de la plateforme sur laquelle vous avez installé l'agent, par exemple lx8266 représente Linux x86_64 R2.6 (64 bits), et aix536 représente AIX R5.3 (64 bits).

   Exemple de commande :

   ```
   /opt/ibm/apm/agent/lx8266/yn/bin/wxs-agent-config.sh config
   ```

   ```
   /opt/ibm/apm/agent/aix536/yn/bin/wxs-agent-config.sh config
   ```
3. Lorsque vous êtes invité à indiquer le chemin d'installation de l'agent, spécifiez le répertoire de base de l'Agent WebSphere Applications.

   Remarque : Le script recherche le fichier de configuration dont le nom est indiqué dans le chemin d'installation fourni. Par défaut, il s'agit de *rép_install*`/config/${hostname}_yn.xml`. Si le système vous indique que le fichier n'existe pas, cela peut être dû au fait que vous n'avez pas démarré l'Agent WebSphere Applications avant d'effectuer cette configuration. Démarrez l'Agent WebSphere Applications et arrêtez-le au moins une fois.
4. A l'invite `WebSphere Extreme Scale Catalog Server connector type`, entrez 1 pour continuer.
5. A l'invite `Input a node name to identify this agent node on UI`, entrez le nom du noeud.

   Le nom du noeud permet d'identifier la zone WebSphere Extreme Scale surveillée et il s'affiche dans le nom d'instance qui apparaît dans l'interface utilisateur Tableau de bord d'Application Performance.
6. A l'invite `WebSphere Extreme Scale Catalog Server security enabled?`, entrez 1 si la sécurité est activée. Entrez ensuite le nom d'utilisateur et le mot de passe. Si la sécurité n'est pas activée, entrez 2.
7. Indiquez le nom d'hôte et le numéro de port du serveur de catalogue. S'il existe plusieurs serveurs de catalogue, ajoutez-les les uns après les autres. Vous pouvez également ajouter plusieurs zones de la même façon.
   - Le nom d'hôte est le nom du système où se trouve le serveur de catalogue. Vérifiez qu'il est possible d'y accéder. Si ce n'est pas le cas, utilisez l'adresse IP comme nom d'hôte.

- Le numéro de port est le numéro **JMXServicePort** du serveur de catalogue WebSphere Extreme Scale. La valeur par défaut est 1099. Vous trouverez plus de détails sur le numéro de port dans WebSphere Extreme Scale Knowledge Center.

8. Pour démarrer l'agent, exécutez la commande ci-après.

```
rép_install/bin/was-agent.sh start
```

Remarque :

- La configuration de l'agent est stockée dans *rép_install*/config/${hostname}_yn.xml. Si vous souhaitez modifier une configuration, exécutez à nouveau ce script ou modifiez directement le fichier .xml.
- La configuration précédente est sauvegardée dans *rép_install*/config/${hostname}_yn.xml.bak. Vous pourrez la restaurer si nécessaire.
- Vous pouvez appuyer sur les touches Ctrl-C pour quitter le script lorsque vous exécutez *rép_install*/*code_plateforme*/yn/bin/wxs-agent-config.sh config. Votre configuration existante n'est pas modifiée.

Configuration de la surveillance WebSphere Extreme Scale dans l'environnement WebSphere imbriqué

Cette rubrique indique comment configurer l'Agent WebSphere Applications lorsque WebSphere Extreme Scale est installé dans un environnement WebSphere Application Server.

Pourquoi et quand exécuter cette tâche

Si la sécurité n'est pas activée pour le serveur WebSphere Extreme Scale, vous pouvez exécuter directement le processus de configuration. Sinon, vous devez au préalable terminer l'étape «Configuration de la surveillance WebSphere Extreme Scale dans l'environnement WebSphere où la sécurité est activée», à la page 950.

Configuration de la surveillance WebSphere Extreme Scale dans l'environnement WebSphere sans activation de la sécurité

Si vous installez WebSphere Extreme Scale dans un environnement WebSphere Application Server dans lequel la sécurité n'est pas activée, vous pouvez configurer directement l'Agent WebSphere Applications.

Procédure

1. Arrêtez Agent WebSphere Applications.
   a) Accédez au répertoire *rép_install* où vous avez installé l'Agent WebSphere Applications.
   b) Exécutez la commande bin/was-agent.sh stop.
2. Exécutez le script de configuration.

```
rép_install/code_plateforme/yn/bin/wxs-agent-config.sh config
```

   Où

   - *rép_install* correspond au répertoire d'installation de l'Agent WebSphere Applications.
   - *code_plateforme* est le code de la plateforme sur laquelle vous avez installé l'agent, par exemple lx8266 représente Linux x86_64 R2.6 (64 bits), et aix536 représente AIX R5.3 (64 bits).

   Exemple de commande :

```
/opt/ibm/apm/agent/lx8266/yn/bin/wxs-agent-config.sh
```

```
/opt/ibm/apm/agent/aix536/yn/bin/wxs-agent-config.sh
```

3. Lorsque vous êtes invité à indiquer le chemin d'installation de l'agent, spécifiez le répertoire de base de l'Agent WebSphere Applications.

Remarque : Le script recherche le fichier de configuration dont le nom est indiqué dans le chemin d'installation fourni. Par défaut, il s'agit de *rép_install*/config/${hostname}_yn.xml. Si le système vous indique que le fichier n'existe pas, cela peut être dû au fait que vous n'avez pas démarré l'Agent WebSphere Applications avant d'effectuer cette configuration. Démarrez l'Agent WebSphere Applications et arrêtez-le au moins une fois.

4. A l'invite `WebSphere Extreme Scale Catalog Server connector type`, entrez 2 pour continuer.
5. A l'invite `Input a node name to identify this agent node on UI`, entrez le nom du noeud.

   Le nom du noeud permet d'identifier la zone WebSphere Extreme Scale surveillée et il s'affiche dans le nom d'instance qui apparaît dans l'interface utilisateur Tableau de bord d'Application Performance.
6. A l'invite `WebSphere Extreme Scale Catalog Server security enabled?`, entrez 2 pour continuer.
7. Indiquez le nom d'hôte et le numéro de port du serveur de catalogue. S'il existe plusieurs serveurs de catalogue, ajoutez-les les uns après les autres. Vous pouvez également ajouter plusieurs zones de la même façon.
   - Le nom d'hôte est le nom du système où se trouve le serveur de catalogue. Vérifiez qu'il est possible d'y accéder. Si ce n'est pas le cas, utilisez l'adresse IP comme nom d'hôte.
   - Le numéro de port indique le numéro **JMXServicePort** du serveur de catalogue WebSphere Extreme Scale. Il est hérité de la valeur **BOOTSTRAP_ADDRESS** pour chaque WebSphere Application Server. Vous trouverez plus de détails sur le numéro de port dans WebSphere Extreme Scale Knowledge Center.
8. Pour démarrer l'agent, exécutez la commande ci-après.

   ```
   rép_install/bin/was-agent.sh start
   ```

   Remarque :
   - La configuration de l'agent est stockée dans *rép_install*/config/${hostname}_yn.xml. Si vous souhaitez modifier une configuration, exécutez à nouveau ce script ou modifiez directement le fichier .xml.
   - La configuration précédente est sauvegardée dans *rép_install*/config/${hostname}_yn.xml.bak. Vous pourrez la restaurer si nécessaire.
   - Vous pouvez appuyer sur les touches Ctrl-C pour quitter le script lorsque vous exécutez *rép_install*/*code_plateforme*/yn/bin/wxs-agent-config.sh config. Votre configuration existante n'est pas modifiée.

Configuration de la surveillance WebSphere Extreme Scale dans l'environnement WebSphere où la sécurité est activée

Si vous installez WebSphere Extreme Scale dans un environnement WebSphere Application Server où la sécurité est activée, vous devez terminer les étapes d'installation initiales avant de configurer l'Agent WebSphere Applications.

Pourquoi et quand exécuter cette tâche

Si vous souhaitez surveiller les serveurs WebSphere Extreme Scale dans des environnements WebSphere Application Server dans lesquels la sécurité est activée, vous devez configurer les paramètres de sécurité manuellement.

La procédure s'applique aux cas suivants :

- Les serveurs WebSphere Extreme Scale doivent être déployés sur les serveurs d'applications WebSphere Application Server (ou l'agent de noeud ou des processus DMGR).
- L'Agent WebSphere Applications doit être déployé sur un noeud où s'exécute un service de catalogue de zone WebSphere Extreme Scale. Configurez l'agent pour la surveillance de WebSphere Extreme

Scale sous ce noeud et définissez-le de manière à ce qu'il se connecte à cette instance de service de catalogue.

- Une instance d'agent doit être utilisée pour surveiller une seule zone WebSphere Extreme Scale.

Procédure

1. Si la version du kit Java Development Kit (JDK) de WebSphere Application Server est antérieure à 1.7, vous devez reconfigurer l'Agent WebSphere Applications pour qu'il utilise le même environnement JRE que WebSphere Application Server.
   a) Ouvrez le fichier *rép_install*/config/.yn.environment.
   b) Ajoutez la ligne suivante à la première ligne.

   ```
   #JAVAHOME=/opt/IBM/WebSphere/AppServer/java/8.0/jre
   ```

2. Configurez le fichier de propriétés de sécurité de l'Agent WebSphere Applications.

   Pour obtenir des instructions, voir «Configuration de l'agent pour qu'il utilise les fichiers JAR et les propriétés de sécurité de WebSphere Application Server», à la page 951.
3. Facultatif : Si un client Java sécurisé est utilisé, assurez-vous que l'authentification est correctement configurée. Modifiez le fichier de propriétés du client et le fichier de propriétés SSL. Pour obtenir des instructions, voir «Configuration des données d'identification de connexion», à la page 952.

   Remarque : Si la clé n'est pas sécurisée par des paramètres SSL, entrez un mot de passe et un nom d'utilisateur uniquement, et vous pourrez ignorer cette étape.
4. Exécutez le script de configuration pour lancer la console de configuration. Voir «Exécution de la configuration», à la page 954 .

Configuration de l'agent pour qu'il utilise les fichiers JAR et les propriétés de sécurité de WebSphere Application Server

Configurez l'Agent WebSphere Applications pour qu'il utilise les fichiers JAR et les propriétés de sécurité de WebSphere Application Server.

Pourquoi et quand exécuter cette tâche

Pour effectuer cette configuration, modifiez le fichier kynwb.properties.

Procédure

1. Ouvrez le fichier *rép_install*/*code_plateforme*/yn/config/kynwb.properties. S'il n'existe pas, créez-le.
   - *rép_install* correspond au répertoire d'installation de l'Agent WebSphere Applications.
   - *code_plateforme* est le code de la plateforme sur laquelle vous avez installé l'agent, par exemple lx8266 représente Linux x86_64 R2.6 (64 bits), et aix536 représente AIX R5.3 (64 bits).
2. Le chemin d'accès aux classes apparaît au début du fichier. Ajoutez les lignes suivantes avant les lignes existantes.
   - Pour WebSphere Application Server 9.0 :

     ```
     rép_base_serveur_app/plugins/com.ibm.ws.runtime.jar:\
     rép_base_serveur_app/lib/bootstrap.jar:\
     rép_base_serveur_app/runtimes/com.ibm.ws.admin.client_9.0.jar:\
     rép_base_serveur_app/lib/wsogclient.jar:\
     ```

   - Pour WebSphere Application Server 8.5 :

     ```
     rép_base_serveur_app/plugins/com.ibm.ws.runtime.jar:\
     rép_base_serveur_app/lib/bootstrap.jar:\
     rép_base_serveur_app/runtimes/com.ibm.ws.admin.client_8.5.0.jar:\
     rép_base_serveur_app/lib/wsogclient.jar:\
     ```

   Exemple de chemin d'accès aux classes modifié :

```
/opt/IBM/WebSphere/plugins/com.ibm.ws.runtime.jar:\
/opt/IBM/WebSphere/lib/bootstrap.jar:\
/opt/IBM/WebSphere/runtimes/com.ibm.ws.admin.client_8.5.0.jar:\
/opt/IBM/WebSphere/lib/wsogclient.jar:\
lib/kynwb.jar:\
lib/kynwxssec_api.jar:\
lib/itcam.cg.mbean.jar:\
wasdc/7.3/installer/lib/itcamfwas.jar:\
```

3. A la fin du fichier *rép_install*/*code_plateforme*/yn/config/kynwb.properties, ajoutez les lignes indiquant les fichiers de propriétés de sécurité devant être utilisés par l'agent. Il s'agit généralement des fichiers utilisés par l'utilitaire wsadmin :

   ```
   -Dcom.ibm.CORBA.ConfigURL=file:/profil_serveur_app/properties/sas.client.props
   -Dcom.ibm.SSL.ConfigURL=file:/profil_serveur_app/properties/ssl.client.props
   ```

   Si les paramètres de sécurité requis par l'agent sont différents de ceux utilisés par l'utilitaire wsadmin, créez des copies distinctes des fichiers et attribuez-leur les chemins d'accès, par exemple :

   ```
   -Dcom.ibm.CORBA.ConfigURL=file:/opt/IBM/ITM/config/sas.client.props
   -Dcom.ibm.SSL.ConfigURL=file:/opt/IBM/ITM/config/ssl.client.props
   ```

   Remarque : Lorsque vous installez un groupe de correctifs ou un correctif temporaire pour l'Agent WebSphere Applications, les modifications apportées aux fichiers yn.ini et kynwb.properties sont écrasées. Après avoir effectué ces installations, vous devez appliquer à nouveau les modifications à ces deux fichiers.

Configuration des données d'identification de connexion
Si un client Java sécurisé est utilisé, il doit lire un fichier de propriétés qui contient une liste des paramètres CSIv2. Ces paramètres déterminent la manière dont le client s'authentifie auprès d'un serveur. Vous devez vous assurer que l'authentification est correctement configurée.

Pourquoi et quand exécuter cette tâche

En général, le fichier contenant ces paramètres est spécifié dans la propriété JVM com.ibm.CORBA.ConfigURL. D'autres paramètres SSL se trouvent dans le fichier indiqué dans la propriété JVM com.ibm.SSL.ConfigURL.

Si l'Agent WebSphere Applications est configuré pour surveiller les serveurs eXtreme Scale imbriqués dans WebSphere Application Server, il agit en tant que client Java sécurisé. Pour cette raison, -Dcom.ibm.CORBA.ConfigURL et -Dcom.ibm.SSL.ConfigURL doivent être spécifiés dans le fichier kynwb.properties.

Dans la plupart des cas, ces propriétés pointent vers les fichiers sas.client.props et ssl.client.props du répertoire *profil_serveur_app*/properties. Ces fichiers sont utilisés par des outils tels que wsadmin ou xscmd. Par conséquent, si vous pouvez utiliser l'un de ces outils pour vous connecter à un serveur de catalogue Extreme Scale sans avoir à saisir de données d'identification, vous n'avez pas besoin de personnaliser les paramètres.

Si la connexion échoue ou exige la saisie d'un nom d'utilisateur ou d'un mot de passe, vous devez effectuer une configuration supplémentaire.

Modification du fichier de propriétés du client
Modifiez le fichier sas.client.props utilisé par l'Agent WebSphere Applications.

Pourquoi et quand exécuter cette tâche
Le chemin complet du fichier sas.client.props est indiqué dans kynwb.properties, dans la propriété -Dcom.ibm.CORBA.ConfigURL. Fournissez les informations de connexion et de sécurité pour l'instance WebSphere Application Server qui exécute l'instance Catalog Services pour laquelle l'agent est configuré.

Procédure

1. Ouvrez le fichier *profil_serveur_app*/properties/sas.client.props.
2. Remplacez la valeur de la propriété com.ibm.CORBA.loginSource par properties :

```
com.ibm.CORBA.loginSource=properties
```

3. Attribuez à la propriété com.ibm.CORBA.securityServerHost le nom d'hôte d'un serveur d'applications dans la zone WebSphere Extreme Scale. Il peut s'agir du serveur local ou d'un autre serveur. Le serveur doit toujours être disponible au démarrage de l'agent. Exemple :

```
com.ibm.CORBA.securityServerHost=server.company.com
```

4. Attribuez à la propriété com.ibm.CORBA.securityServerPort le port RMI du profil de serveur d'applications, par exemple :

```
com.ibm.CORBA.securityServerPort=2819
```

5. Affectez à la propriété com.ibm.CORBA.loginUserid le nom de connexion permettant de communiquer avec le serveur d'applications, et à la propriété com.ibm.CORBA.loginPassword, le mot de passe. Par exemple :

```
com.ibm.CORBA.loginUserid=admin
com.ibm.CORBA.loginPassword=password
```

6. Affectez aux propriétés suivantes la valeur true ou false, correspondant aux paramètres des **communications entrantes CSIv2** dans la console d'administration WebSphere :

```
com.ibm.CSI.performTLClientAuthenticationRequired
com.ibm.CSI.performTLClientAuthenticationSupported
com.ibm.CSI.performTransportAssocSSLTLSRequired
com.ibm.CSI.performTransportAssocSSLTLSSupported
```

   Les propriétés com.ibm.CSI.performTLClientAuthentication* sont liées aux paramètres **Client certificate authentication**. Les propriétés com.ibm.CSI.performTransportAssocSSLTLS* sont liées aux paramètres **Transport**.
7. Facultatif : si l'alias SSL par défaut (DefaultSSLSettings) n'est pas utilisé, définissez le nom de l'alias de configuration SSL dans la propriété com.ibm.ssl.alias.
8. Sauvegardez le fichier, puis chiffrez le mot de passe dans le fichier sas.client.props. Pour chiffrer le mot de passe, exécutez la commande suivante :
   - Sur les systèmes Linux et UNIX, exécutez *profil_serveur_app*/bin/PropFilePasswordEncoder.sh sas.client.props com.ibm.CORBA.loginPassword

   Important : Si l'authentification du certificat client est requise et que l'authentification de base est activée, il se peut que vous deviez également définir la propriété com.ibm.CORBA.validateBasicAuth=false.

Modification du fichier de propriétés SSL du client
Modifiez le fichier de propriétés SSL par le biais duquel l'Agent WebSphere Applications accède aux certificats du serveur.

Pourquoi et quand exécuter cette tâche

Modifiez le fichier ssl.client.props devant être utilisé par l'agent. Le chemin d'accès complet à ce fichier est indiqué dans le fichier kynwb.properties, dans la propriété -Dcom.ibm.SSL.ConfigURL. Fournissez les informations relatives au magasin de clés de confiance SSL et au magasin de clés pour l'instance WebSphere Application Server qui exécute l'instance Catalog Services pour laquelle l'agent est configuré.

Vous pouvez créer et gérer des certificats par le biais de la console d'administration WebSphere (**Sécurité** > **Certificat SSL et gestion des clés** > **Magasins de clés et certificats**) ou à l'aide de l'outil iKeyman.

Procédure

1. Ouvrez le fichier *profil_serveur_app*/properties/ssl.client.props.
2. Attribuez à la propriété com.ibm.ssl.alias la même valeur que celle indiquée pour cette même propriété dans le fichier sas.client.props.

   Conseil : Le fichier ssl.client.props peut contenir plusieurs configurations SSL. Chaque configuration commence par la propriété com.ibm.ssl.alias.
3. Affectez à la propriété com.ibm.ssl.enableSignerExchangePrompt la valeur false.
4. Définissez les propriétés de magasin de clés suivantes pour permettre à l'application client d'accéder à la clé de chiffrement :

   com.ibm.ssl.keyStoreName
   Nom identifiant ce magasin de clés

   com.ibm.ssl.keyStore
   Chemin complet et nom du magasin de clés

   com.ibm.ssl.keyStorePassword
   Mot de passe du magasin de clés

   com.ibm.ssl.keyStoreType
   Type du magasin de clés. Utilisez le type PKCS12 par défaut en raison de son interopérabilité avec les autres applications.

   Important : Si l'authentification par certificat client n'est pas requise, le magasin de clés peut contenir une clé autosignée. Dans le cas contraire, celui-ci doit contenir une clé signée par un certificat stocké dans le magasin de clés de confiance du serveur.
5. Définissez les propriétés de magasin de clés de confiance suivantes pour permettre à l'application client d'accéder aux certificats de signataire :

   com.ibm.ssl.trustStoreName
   Nom identifiant ce magasin de clés de confiance

   com.ibm.ssl.trustStore
   Chemin complet et nom du magasin de clés de confiance

   com.ibm.ssl.trustStorePassword
   Mot de passe du magasin de clés de confiance

   com.ibm.ssl.trustStoreType
   Type du magasin de clés de confiance. Utilisez le type PKCS12 par défaut en raison de son interopérabilité avec les autres applications.

   Important : Si le client doit utiliser une connexion SSL, le certificat de signataire du serveur doit se trouver dans son magasin de clés de confiance.

Exécution de la configuration
Après avoir vérifié l'environnement et la sécurité, vous pouvez exécuter le processus de configuration.

Procédure

1. Arrêtez Agent WebSphere Applications.
   a) Accédez au répertoire *rép_install* où vous avez installé l'Agent WebSphere Applications.
   b) Exécutez la commande bin/was-agent.sh stop.
2. Exécutez le script de configuration.

   ```
   rép_install/code_plateforme/yn/bin/wxs-agent-config.sh config
   ```

   Où

   - *rép_install* correspond au répertoire d'installation de l'Agent WebSphere Applications.
   - *code_plateforme* est le code de la plateforme sur laquelle vous avez installé l'agent, par exemple lx8266 représente Linux x86_64 R2.6 (64 bits), et aix536 représente AIX R5.3 (64 bits).

Exemple de commande :

```
/opt/ibm/apm/agent/lx8266/yn/bin/wxs-agent-config.sh config
```

```
/opt/ibm/apm/agent/aix536/yn/bin/wxs-agent-config.sh config
```

3. Lorsque vous êtes invité à indiquer le chemin d'installation de l'agent, spécifiez le répertoire de base de l'Agent WebSphere Applications.

   Remarque : Le script recherche le fichier de configuration dont le nom est indiqué dans le chemin d'installation fourni. Par défaut, il s'agit de *rép_install*/config/${hostname}_yn.xml. Si le système vous indique que le fichier n'existe pas, cela peut être dû au fait que vous n'avez pas démarré l'Agent WebSphere Applications avant d'effectuer cette configuration. Démarrez l'Agent WebSphere Applications et arrêtez-le au moins une fois.
4. A l'invite `WebSphere Extreme Scale Catalog Server connector type`, entrez 2 pour continuer.
5. A l'invite `Input a node name to identify this agent node on UI`, entrez le nom du noeud.

   Le nom du noeud permet d'identifier la zone WebSphere Extreme Scale surveillée et il s'affiche dans le nom d'instance qui apparaît dans l'interface utilisateur Tableau de bord d'Application Performance.
6. A l'invite `WebSphere Extreme Scale Catalog Server security enabled?`, entrez 1 pour continuer. Entrez ensuite le nom d'utilisateur et le mot de passe.
7. Indiquez le nom d'hôte et le numéro de port du serveur de catalogue. S'il existe plusieurs serveurs de catalogue, ajoutez-les les uns après les autres. Vous pouvez également ajouter plusieurs zones de la même façon.
   - Le nom d'hôte est le nom du système où se trouve le serveur de catalogue. Vérifiez qu'il est possible d'y accéder. Si ce n'est pas le cas, utilisez l'adresse IP comme nom d'hôte.
   - Le numéro de port indique le numéro **JMXServicePort** du serveur de catalogue WebSphere Extreme Scale. Il est hérité de la valeur **BOOTSTRAP_ADDRESS** pour chaque WebSphere Application Server. Vous trouverez plus de détails sur le numéro de port dans WebSphere Extreme Scale Knowledge Center.
8. Pour démarrer l'agent, exécutez la commande ci-après.

   ```
   rép_install/bin/was-agent.sh start
   ```

   Remarque :
   - La configuration de l'agent est stockée dans *rép_install*/config/${hostname}_yn.xml. Si vous souhaitez modifier une configuration, exécutez à nouveau ce script ou modifiez directement le fichier .xml.
   - La configuration précédente est sauvegardée dans *rép_install*/config/${hostname}_yn.xml.bak. Vous pourrez la restaurer si nécessaire.
   - Vous pouvez appuyer sur les touches Ctrl-C pour quitter le script lorsque vous exécutez *rép_install*/bin/wxs-agent-config.sh config. Votre configuration existante n'est pas modifiée.

Annulation de la configuration de la surveillance WebSphere Extreme Scale

Si vous ne souhaitez pas surveiller WebSphere Extreme Scale, vous pouvez annuler la configuration de l'Agent WebSphere Applications.

Procédure

1. Arrêtez Agent WebSphere Applications.
   a) Accédez au répertoire *rép_install* où vous avez installé l'Agent WebSphere Applications.
   b) Exécutez la commande bin/was-agent.sh stop.
2. Exécutez le script d'annulation de configuration.

```
rép_install/{pc}/yn/bin/wxs-agent-config.sh unconfig
```

Où

- *rép_install* correspond au répertoire d'installation de l'Agent WebSphere Applications.
- *code_plateforme* est le code de la plateforme sur laquelle vous avez installé l'agent, par exemple lx8266 représente Linux x86_64 R2.6 (64 bits), et aix536 représente AIX R5.3 (64 bits).

Exemple de commande :

```
/opt/ibm/apm/agent/lx8266/yn/bin/wxs-agent-config.sh unconfig
```

```
/opt/ibm/apm/agent/aix536/yn/bin/wxs-agent-config.sh unconfig
```

Configuration de la surveillance de WebSphere Infrastructure Manager

Configurez l'agent WebSphere Infrastructure Manager pour surveiller les performances de WebSphere Deployment Manager et de l'agent de noeud.

Pourquoi et quand exécuter cette tâche

L'agent WebSphere Infrastructure Manager est un agent multi-instance. Vous devez créer la première instance et démarrer l'agent manuellement.

Procédure

1. Pour configurer l'agent, exécutez la commande ci-après.

   ```
   rép_install/bin/wim-agent.sh config nom_instance
   ```

   Où *nom_instance* est le nom à attribuer à l'instance, et *rép_install* est le répertoire d'installation de l'agent WebSphere Infrastructure Manager. Le répertoire d'installation par défaut est `/opt/ibm/apm/agent`.
2. A l'invite `Edit 'Monitoring Agent for WebSphere Infrastructure Manager' settings`, entrez 1 pour continuer.
3. A l'invite `Java home`, spécifiez le répertoire dans lequel Java est installé.

   La valeur par défaut est `/opt/ibm/apm/agent/JRE/lx8266/jre`.
4. A l'invite `DMGR Profile Home`, spécifiez le répertoire de base du profil Deployment Manager.

   Le répertoire par défaut est `/opt/IBM/WebSphere/AppServer/profiles/Dmgr01`.
5. A l'invite `JMX user ID`, spécifiez l'ID utilisateur utilisé pour se connecter au serveur MBean.
6. A l'invite `Enter JMX password`, spécifiez le mot de passe de l'utilisateur.
7. A l'invite `Re-type JMX password`, entrez une nouvelle fois le mot de passe.
8. Pour démarrer l'agent, exécutez la commande ci-après.

   ```
   rép_install/bin/wim-agent.sh start nom_instance
   ```

Résultats

Vous avez créé une instance agent WebSphere Infrastructure Manager et démarré l'agent de surveillance pour commencer la collecte des échantillons de données pour la surveillance des données.

Configuration de la surveillance de WebSphere MQ

Pour pouvoir démarrer l'agent, vous devez d'abord lui affecter un nom d'instance et effectuer plusieurs tâches de configuration relatives à l'ID utilisateur et aux noms de système géré. De plus, vous pouvez éventuellement activer le suivi des transactions pour l'agent.

Avant de commencer

- Les instructions figurant dans cette rubrique concernent l'édition la plus récente de cet agent. Pour plus d'informations sur la vérification de la version d'un agent dans votre environnement, voir Commande de version d'agent. Pour des informations détaillées sur la liste des versions d'agent et sur les nouveautés de chacune d'elles, voir «Historique des modifications», à la page 53.
- Assurez-vous que votre environnement possède la configuration système requise pour l'agent WebSphere MQ. Pour les toutes dernières informations sur la configuration système requise, voir le rapport détaillé sur la configuration système requise pour l'agent WebSphere MQ.

Pourquoi et quand exécuter cette tâche

Les instructions concernent l'édition la plus récente de l'agent, sauf indication contraire.

Pour configurer l'environnement pour l'agent WebSphere MQ, vous devez commencer par vérifier que l'ID utilisateur de l'agent peut accéder aux objets IBM MQ (WebSphere MQ), configurer IBM MQ (WebSphere MQ) pour l'activation des données, puis configurer l'agent WebSphere MQ.

La procédure suivante, qui inclut des étapes obligatoires et facultatives, permet de configurer l'agent WebSphere MQ. Effectuez les étapes nécessaires en fonction de vos besoins.

Procédure

1. Autorisez l'ID utilisateur qui est employé pour configurer, démarrer et arrêter l'agent à accéder aux objets IBM MQ (WebSphere MQ). Voir «ID utilisateur autorisés à exécuter l'agent», à la page 957 .
2. Configurez IBM MQ (WebSphere MQ) pour activer les données que vous voulez surveiller. Voir «Configuration d'IBM MQ (WebSphere MQ) pour l'activation des données», à la page 959 .
3. Configurez l'agent en fournissant un nom d'instance d'agent, un nom de gestionnaire de files d'attente et, éventuellement, un nom d'agent. Voir «Configuration de l'agent WebSphere MQ», à la page 961 .
4. Facultatif : En fonction de vos exigences en termes de surveillance, vous pourriez avoir besoin d'un nom de système géré unique pour distinguer les agents de surveillance. Utilisez l'option `Agent Name` dans la commande `mq-agent.sh config` pour spécifier le qualificatif intermédiaire du nom de système géré. Voir «Spécification de noms de systèmes gérés uniques pour plusieurs gestionnaires de files d'attente», à la page 964 .
5. Facultatif : Pour configurer l'agent en vue de collecter les données de suivi des transactions du gestionnaire de files d'attente surveillées, utilisez la page **Configuration d'agent**. Pour obtenir des instructions, voir «Configuration du suivi des transactions pour l'agent WebSphere MQ», à la page 966.
6. Facultatif : Autorisez l'agent à collecter les données d'historique à long terme pour les files d'attente et les canaux. Pour obtenir des instructions, voir «Activation de la collecte de données pour l'historique à long terme de files d'attente et de canal», à la page 967.
7. Facultatif : Pour surveiller le gestionnaire de files d'attente à distance sur MQ Appliance, vous devez effectuez des étapes de configuration supplémentaires sur l'agent et IBM MQ (WebSphere MQ). Pour plus d'informations, voir «Surveillance à distance des gestionnaires de file d'attente sur MQ Appliance», à la page 969 ou «Surveillance à distance des gestionnaires de file d'attente haute disponibilité sur MQ Appliance», à la page 970.

ID utilisateur autorisés à exécuter l'agent

Pour qu'un ID utilisateur puisse configurer, démarrer et arrêter l'agent WebSphere MQ, il doit appartenir au groupe **mqm**, qui dispose de privilèges d'administration complets sur IBM MQ (WebSphere MQ). En

outre, pour un utilisateur non superutilisateur ou un utilisateur non-administrateur, vous devez accorder aux utilisateurs l'accès aux objets IBM MQ (WebSphere MQ) à l'aide de la commande de contrôle IBM MQ (WebSphere MQ).

Pourquoi et quand exécuter cette tâche

Sur AIX ou Linux, vous devez ajouter l'ID utilisateur au groupe **mqm** et puis accorder à l'ID utilisateur l'accès approprié aux objets IBM MQ (WebSphere MQ) avec la commande **setmqaut**.

Sur les systèmes Windows, vous devez ajouter l'identificateur utilisateur au groupe **mqm**. Si l'ID utilisateur ne fait pas partie du groupe d'utilisateurs Administrateur, vous devez également utiliser l'éditeur de registre pour accorder à l'ID utilisateur des autorisations lui permettant de démarrer ou d'arrêter l'agent.

Procédure

- Linux AIX

  Sur un système AIX ou Linux, procédez comme suit :

  a) Connectez-vous au système AIX ou Linux en utilisant l'ID racine.

  b) Ajoutez l'ID utilisateur qui est utilisé pour exécuter l'agent sur le groupe **mqm**.

  c) (WebSphere MQ version 7.5 ou ultérieure) : si l'ID utilisateur n'est pas celui d'un superutilisateur sur le système AIX ou Linux, vous devez lui accorder le niveau de droit approprié pour accéder aux objets IBM MQ (WebSphere MQ) en exécutant la commande suivante :

  ```
  setmqaut -m gestionnaire_files_attente -t qmgr -p ID_utilisateur +inq +connect +dsp +setid
  ```

  où *gestionnaire_files_attente* est le nom du gestionnaire de files d'attente de WebSphere MQ version 7.5 ou ultérieure et *ID_utilisateur* l'ID d'un utilisateur non superutilisateur ou non-administrateur pour exécuter l'agent.

- Windows

  Sur les systèmes Windows, procédez comme suit :

  a) Connectez-vous aux systèmes Windows comme administrateur système.

  b) Ajoutez l'ID utilisateur qui est utilisé pour exécuter l'agent sur le groupe **mqm**.

  c) Si l'ID utilisateur que vous utilisez pour démarrer, exécuter et arrêter l'agent n'est pas membre du groupe Administrateur, utilisez l'éditeur de registre pour définir les droits d'un ID utilisateur afin de garantir que l'agent peut être démarré et arrêté correctement :

  a. Cliquez sur **Démarrer** > **Exécuter**, puis tapez `regedit.exe` pour ouvrir l'éditeur de registre.

  b. Dans l'éditeur de registre, recherchez la clé `HKEY_LOCAL_MACHINE\SOFTWARE\Candle`.

  c. Cliquez avec le bouton droit sur la clé et cliquez sur **Autorisations**.

  d. Si l'ID utilisateur pour l'agent WebSphere MQ n'est pas dans la liste Groupe ou noms d'utilisateur, cliquez sur **Ajouter** pour ajouter cet ID utilisateur à la liste.

  e. Cliquez sur l'ID utilisateur dans la liste.

  f. Dans la liste des autorisations pour l'*ID_utilisateur*, où *ID_utilisateur* est l'ID utilisateur de l'agent WebSphere MQ, sélectionnez **Contrôle total** dans la colonne Autoriser, puis cliquez sur **OK**.

  g. Dans l'éditeur de registre, recherchez la clé `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`.

  h. Cliquez avec le bouton droit sur la clé et cliquez sur **Autorisations**.

  i. Si l'ID utilisateur pour l'agent WebSphere MQ n'est pas dans la liste Groupe ou noms d'utilisateur, cliquez sur **Ajouter** pour ajouter cet ID utilisateur à la liste.

  j. Cliquez sur l'ID utilisateur dans la liste Groupe ou noms d'utilisateur.

k. Dans la liste des autorisations pour l'*ID_utilisateur*, où *ID_utilisateur* est l'ID utilisateur de l'agent WebSphere MQ, sélectionnez **Lecture** dans la colonne Autoriser, puis cliquez sur **OK**.

l. Fermez l'éditeur de registre.

m. Accédez au répertoire *rép_install*, où *rép_install* est le répertoire d'installation de l'agent.

n. Cliquez avec le bouton droit et cliquez sur **Propriétés**.

o. Sous l'onglet Sécurité, si l'ID utilisateur pour l'agent WebSphere MQ n'est pas dans la liste Groupe ou noms d'utilisateur, cliquez sur **Editer**, puis sur **Ajouter** pour ajouter cet ID utilisateur à la liste.

p. Cliquez sur l'ID utilisateur dans la liste Groupe ou noms d'utilisateur.

q. Dans la liste des autorisations pour l'*ID-utilisateur*, sélectionnez **Contrôle total** dans la colonne Autoriser, où **ID-utilisateur** est l'ID utilisateur de l'agent WebSphere MQ.

r. Cliquez sur **OK**.

Que faire ensuite

L'étape suivante consiste à configurer IBM MQ (WebSphere MQ) pour l'activation des données. Voir «Configuration d'IBM MQ (WebSphere MQ) pour l'activation des données», à la page 959 .

Configuration d'IBM MQ (WebSphere MQ) pour l'activation des données

Avant de configurer l'agent WebSphere MQ, il est recommandé de commencer par configurer IBM MQ (WebSphere MQ) pour activer les données que vous voulez surveiller.

Pourquoi et quand exécuter cette tâche

Déterminez le type de données que vous voulez surveiller à l'aide de l'agent WebSphere MQ. Activez les données au niveau du gestionnaire de files d'attente en utilisant les commandes MQSC si les données ne sont pas générées par le gestionnaire de files d'attente par défaut.

A faire : Vous devez démarrer MQSC pour le gestionnaire de files d'attente cibles cible avant d'exécuter les commandes MQSC. Pour obtenir la liste des gestionnaires de files d'attente, exécutez la commande **dspmq** à partir du répertoire `bin` dans le répertoire d'installation d'IBM MQ (WebSphere MQ). Pour démarrer MQSC pour un gestionnaire de files d'attente, exécutez la commande suivante à partir du répertoire `bin`, où *<nom_gest_files_att>* correspond au nom du gestionnaire de files d'attente que vous voulez configurer.

```
runmqsc <nom_gest_files_att>
```

Procédure

- Pour voir l'ancienneté du message le plus ancien d'une file d'attente, effectuez les étapes expliquées dans la rubrique «Activation de la surveillance en temps réel des files d'attente», à la page 959.
- Pour surveiller les événements du gestionnaire de files d'attente qui ne sont pas générés par le gestionnaire de files d'attente par défaut, procédez comme décrit à la rubrique «Activation de la surveillance des événements pour le gestionnaire de files d'attente», à la page 960.
- Pour obtenir les données de suivi des transactions, procédez comme décrit à la rubrique «Activation de la trace de l'activité des applications MQI», à la page 960.
- Pour surveiller un gestionnaire de files d'attente éloignées, vérifiez que l'agent WebSphere MQ peut collecter les données de surveillance par l'intermédiaire d'un canal du système distant. Pour plus d'informations, voir «Paramètres de sécurité de la surveillance éloignée», à la page 961.

Activation de la surveillance en temps réel des files d'attente

Pourquoi et quand exécuter cette tâche

Pour voir l'ancienneté du message le plus ancien d'une file d'attente (en secondes), vous devez activer la surveillance en temps réel de la file d'attente.

Procédure

Pour activer la surveillance en temps réel des files d'attente de votre environnement, utilisez les commandes ci-après.

- Pour activer la surveillance en temps réel de toutes les files d'attente dont l'attribut MONQ est défini sur QMGR, exécutez la commande suivante :

  ```
  ALTER QMGR MONQ(niveau_collecte)
  ```

  , *niveau_collecte* spécifiant le niveau de collecte des données de surveillance pour les files d'attente. Vous pouvez définir ce niveau sur LOW, MEDIUM ou HIGH selon les besoins de votre environnement.
- Pour activer la surveillance en temps réel d'une file d'attente individuelle, exécutez la commande suivante :

  ```
  ALTER QLOCAL(nom_file) MONQ(niveau_collecte)
  ```

  où *nom_file* représentant le nom de la file d'attente et *niveau_collecte*, le niveau de collecte des données de surveillance pour les files d'attente. Vous pouvez définir ce niveau sur LOW, MEDIUM ou HIGH selon les besoins de votre environnement.

Résultats
Les données peuvent être affichées dans le widget de groupe Ancienneté du plus ancien message de la file d'attente après le démarrage de l'agent WebSphere MQ.

Activation de la surveillance des événements pour le gestionnaire de files d'attente

Pourquoi et quand exécuter cette tâche

La surveillance des événements fait partie des techniques de surveillance disponibles pour surveiller votre réseau IBM MQ. Après avoir activé le gestionnaire de files d'attente afin d'émettre certains types d'événement, des messages d'événement sont mis en file d'attente d'événements lorsque l'événement se produit, de sorte à pouvoir être surveillés et affichés par l'agent WebSphere MQ.

Les types d'événement suivants ne sont ni surveillés ni affichés avec la configuration du gestionnaire de files d'attente par défaut. Utilisez la commande **ALTER QMGR** pour permettre au gestionnaire de files d'attente de générer ces événements afin qu'ils puissent être affichés sur le Tableau de bord d'Application Performance.

- Evénements de canal
- Evénements de performance

Procédure

Utilisez les commandes suivantes pour permettre au gestionnaire de files d'attente de générer les événements qui vous intéressent :

- Pour générer des événements de canal, exécutez `ALTER QMGR CHLEV(ENABLED)`.
- Pour générer des événements de performance, exécutez `ALTER QMGR PERFMEV(ENABLED)`.

Résultats
Les événements surveillés peuvent être affichés dans le widget de groupe Evénements du gestionnaire de files d'attente une fois l'agent WebSphere MQ démarré.

Activation de la trace de l'activité des applications MQI

Pourquoi et quand exécuter cette tâche
Pour pouvoir afficher les données de suivi des transactions dans les tableaux de bord de middleware et de topologie, la trace de l'activité des applications MQI doit être activée au niveau du gestionnaire de files d'attente.

Procédure

- Pour activer la collecte des informations de trace de l'activité des applications MQI, exécutez la commande MQSC suivante :

```
ALTER QMGR ACTVTRC(ON)
```

Paramètres de sécurité de la surveillance éloignée

Pourquoi et quand exécuter cette tâche

Pour utiliser l'agent WebSphere MQ pour surveiller un gestionnaire de files d'attente éloignées, vous devez vous assurer que les paramètres de sécurité d'IBM MQ (WebSphere MQ) n'empêchent pas l'agent de collecter les données de surveillance par l'intermédiaire d'un canal du système distant.

La procédure ci-après fournit un exemple de paramètre de sécurité simple pour la surveillance éloignée. Pour exercer un contrôle plus précis sur l'accès octroyé aux systèmes de connexion au niveau d'un canal, vous pouvez utiliser des enregistrements d'authentification de canal. Pour plus d'informations, voir la documentation sur les mécanismes de sécurité d'IBM MQ.

Procédure

1. Désactivez l'authentification de canal à l'aide de la commande MQSC suivante :

```
ALTER QMGR CHLAUTH(DISABLED) CONNAUTH(' ')
```

2. Modifiez les paramètres de canal comme indiqué ci-après, *canal_moniteur_distant* représentant le nom du canal utilisé pour la surveillance éloignée.

   - Linux AIX

```
ALTER CHANNEL(canal_moniteur_distant) CHLTYPE(SVRCONN) MCAUSER('mqm')
```

   - Windows

```
ALTER CHANNEL(canal_moniteur_distant) CHLTYPE(SVRCONN) MCAUSER(MUSR_MQADMIN)
```

3. Actualisez les paramètres de sécurité.

```
REFRESH SECURITY
```

Configuration de l'agent WebSphere MQ

Vous devez attribuer un nom d'instance à l'agent WebSphere MQ et configurer l'agent pour qu'il puisse commencer à surveiller votre environnement IBM MQ (WebSphere MQ).

Avant de commencer

- Assurez-vous que l'ID utilisateur de l'agent possède les droits appropriés lui permettant d'accéder aux objets IBM MQ (WebSphere MQ). Si ce n'est pas fait, suivez les instructions de la rubrique «ID utilisateur autorisés à exécuter l'agent», à la page 957.
- Configurez IBM MQ (WebSphere MQ) de sorte à activer la collecte de données requise. Si ce n'est pas fait, consultez «Configuration d'IBM MQ (WebSphere MQ) pour l'activation des données», à la page 959.
- Vous devez fournir le nom du gestionnaire de files d'attente que l'agent WebSphere MQ doit surveiller. Contactez l'administrateur IBM MQ (WebSphere MQ) si vous ne connaissez pas le nom du gestionnaire de files d'attente approprié. Sinon, exécutez la commande **dspmq** à partir du répertoire `bin` dans le répertoire d'installation d'IBM MQ (WebSphere MQ) pour obtenir la liste des gestionnaires de files d'attente. Vous devez fournir la valeur QMNAME renvoyée lorsque vous configurez l'agent WebSphere MQ.

Pourquoi et quand exécuter cette tâche

L'agent WebSphere MQ est un agent d'instance multiple. Vous devez créer la première instance et démarrer l'agent manuellement.

Sur les systèmes UNIX ou Linux, vous pouvez choisir de configurer l'agent avec ou sans interactions. Sur les systèmes Windows, vous pouvez configurer l'agent sans interactions uniquement.

- Pour configurer l'agent avec interaction, exécutez le script de configuration et répondez aux invites. Voir «Configuration interactive», à la page 962 .
- Pour configurer l'agent sans interaction, éditez le fichier de réponses silencieux, puis exécutez le script de configuration. Voir «Configuration en mode silencieux», à la page 963 .

Important : Si vous avez également installé Monitoring Agent for WebSphere MQ, qui est fourni comme composant dans le produit ITCAM for Applications, sur le même système que l'agent WebSphere MQ, fourni dans Cloud APM, ne les utilisez pas pour surveiller le même gestionnaire de files d'attente sur le système.

Configuration interactive

Procédure

Pour configurer l'agent en exécutant le script et en répondant aux invites, procédez comme suit :

1. Entrez la commande suivante pour créer une instance d'agent :

   ```
   rép_install/bin/mq-agent.sh config nom_instance
   ```

   où *nom_instance* est le nom à attribuer à l'instance.
2. A l'invite `Queue Manager Name`, indiquez le nom du gestionnaire de files d'attente à surveiller.
3. A l'invite `Nom de l'agent`, indiquez le nom d'agent à utiliser comme qualificatif intermédiaire du nom de système géré. N'appuyez pas sur la touche Entrée pour ignorer la spécification de ce paramètre.

   A faire : Ce nom d'agent est différent du nom d'instance d'agent. Le nom d'instance d'agent est utilisé dans le nom du fichier de configuration d'agent afin de distinguer les fichiers de configuration entre les agents, par exemple, *nom_hôte*_mq_*nom_instance*`.cfg`. Le nom d'agent est utilisé comme identificateur court pour créer des noms de système géré uniques. Pour savoir à quel moment un nom de système géré unique est requis, voir «Spécification de noms de systèmes gérés uniques pour plusieurs gestionnaires de files d'attente», à la page 964.
4. Si vous souhaitez surveiller un gestionnaire de files d'attente éloignées, spécifiez les paramètres de configuration ci-après. Si vous souhaitez surveiller un gestionnaire de files d'attente locales, appuyez sur la touche Entrée pour continuer.

   - `Connection Name` : nom de connexion de la surveillance éloignée. Le format est *adresse_IP*`(`*numéro_port*`)`. Par exemple, `127.0.0.1(1414)`. Si vous configurez l'instance d'agent pour la première fois, vous pouvez appuyer sur la touche Entrée pour accepter la valeur par défaut (null). Le nom de connexion approprié peut être détecté automatiquement.
   - `Channel` : nom du canal utilisé pour la collecte de données à distance. Si vous configurez l'instance d'agent pour la première fois, vous pouvez appuyer sur la touche Entrée pour accepter la valeur par défaut (null). Le canal SYSTEM.DEF.SVRCONN est utilisé.

   Limitation : Les journaux d'erreurs d'un gestionnaire de files d'attente éloignées ne peuvent pas être surveillés. Si l'agent surveille un gestionnaire de files d'attente éloignées, le tableau de bord MQ Errors Details ne contient pas de données.
5. Lorsque vous êtes invité à saisir le chemin d'accès à la bibliothèque WebSphere MQ, appuyez sur Entrée pour accepter la valeur par défaut, qui est le chemin d'accès à la bibliothèque 64 bits d'IBM MQ (WebSphere MQ) automatiquement découvert par l'agent WebSphere MQ. Si aucune valeur par défaut n'est affichée, vous devez fournir le chemin d'accès à la bibliothèque 64 bits d'IBM MQ (WebSphere MQ) pour poursuivre.

Par exemple, /opt/mqm8/lib64 est le chemin d'accès à la bibliothèque 64 bits pour un système Linux.

6. Pour démarrer l'agent, entrez la commande suivante :

```
rép_install/bin/mq-agent.sh start nom_instance
```

Configuration en mode silencieux

Procédure

Pour configurer l'agent en éditant le fichier de réponses silencieux et en exécutant le script sans intervenir, procédez comme suit :

1. Ouvrez le fichier mq_silent_config.txt dans un éditeur de texte.
   - Linux AIX *rép_install*/samples/mq_silent_config.txt
   - Windows *rép_install*\tmaitm6_x64\samples\mq_silent_config.txt

   où *rép_install* correspond au répertoire d'installation de l'agent WebSphere MQ.
2. Obligatoire : Pour **QMNAME**, indiquez le nom du gestionnaire de files d'attente à surveiller.
3. Obligatoire : Pour **AGTNAME**, indiquez le nom d'agent à utiliser comme qualificatif intermédiaire du nom de système géré.

   A faire : Ce nom d'agent est différent du nom d'instance d'agent. Le nom d'instance d'agent est utilisé dans le nom du fichier de configuration d'agent afin de distinguer les fichiers de configuration entre les agents, par exemple, *nom_hôte*_mq_*nom_instance*.cfg. Le nom d'agent est utilisé comme identificateur court pour créer des noms de système géré uniques. Pour savoir à quel moment un nom de système géré unique est requis, voir «Spécification de noms de systèmes gérés uniques pour plusieurs gestionnaires de files d'attente», à la page 964.
4. Si vous souhaitez surveiller un gestionnaire de files d'attente éloignées, spécifiez les paramètres de configuration suivants :
   - **CONNAME** : nom de connexion de la surveillance éloignée. Le format est *adresse_IP* (*numéro_port*). Par exemple, 127.0.0.1(1414).
   - **CHANNEL** : nom du canal utilisé pour la collecte de données à distance. S'il n'est pas spécifié, le canal SYSTEM.DEF.SVRCONN est utilisé.

   Limitation : Les journaux d'erreurs d'un gestionnaire de files d'attente éloignées ne peuvent pas être surveillés. Si l'agent surveille un gestionnaire de files d'attente éloignées, le tableau de bord MQ Errors Details ne contient pas de données.
5. Facultatif : Pour **WMQLIBPATH**, indiquez le chemin d'accès à la bibliothèque 64 bits d'IBM MQ (WebSphere MQ). Par exemple, /opt/mqm8/lib64. Si aucune valeur n'est indiquée, le chemin d'accès peut être reconnu automatiquement au cours de la configuration de l'agent.
6. Sauvegardez et fermez le fichier mq_silent_config.txt, puis exécutez la commande suivante à partir de la ligne de commande :
   - Linux AIX *rép_install*/bin/mq-agent.sh config *nom_instance* *chemin_fichier_réponses*
   - Windows *rép_install*\BIN\mq-agent.bat config *nom_instance* "*chemin_vers_fichier_réponses*"

   où *nom_instance* est le nom de l'instance que vous configurez et *chemin_fichier_réponses* le chemin d'accès complet au fichier de réponses silencieux.

   A faire : Sur les systèmes Windows, n'omettez pas les guillemets doubles ("") qui entourent le chemin d'accès du fichier de réponses silencieux, surtout lorsque le chemin d'accès contient des caractères spéciaux.

   Par exemple, si le fichier de réponses se trouve dans le répertoire par défaut, lancez la commande suivante.

- Linux AIX

```
/opt/ibm/apm/agent/bin/mq-agent.sh config nom_instance
/opt/ibm/apm/agent/samples/mq_silent_config.txt
```

- Windows

```
C:\IBM\APM\BIN\mq-agent.bat config nom_instance
"C:\IBM\APM\tmaitm6_x64\samples\mq_silent_config.txt"
```

7. Pour démarrer l'agent, entrez la commande suivante :

- Linux AIX

```
rép_install/bin/mq-agent.sh start nom_instance
```

- Windows

```
rép_install\bin\mq-agent.bat start nom_instance
```

Résultats

Vous pouvez à présent vous connecter à la console Cloud APM et utiliser l'éditeur d'applications pour ajouter l'instance de l'agent WebSphere MQ au Tableau de bord d'Application Performance. Pour obtenir des instructions de démarrage de la console Cloud APM, voir «Démarrage de la console Cloud APM», à la page 1003. Pour plus d'informations sur l'utilisation de l'éditeur d'applications, voir «Gestion des applications», à la page 1129.

Que faire ensuite

- Si vous avez activé la collecte des informations de trace de l'activité des applications MQI au niveau du gestionnaire de files d'attente, utilisez la page **Configuration d'agent** pour configurer l'agent WebSphere MQ de sorte à collecter les données de suivi des transactions du gestionnaire de files d'attente surveillé. Voir «Configuration du suivi des transactions pour l'agent WebSphere MQ», à la page 966. Si l'agent ne figure pas sur la page **Configuration d'agent**, redémarrez le serveur Cloud APM.
- En fonction de vos exigences en termes de surveillance, vous pourriez avoir besoin d'un nom de système géré unique pour distinguer les agents de surveillance. Utilisez l'option `Agent Name` dans la commande `mq-agent.sh config` pour spécifier le qualificatif intermédiaire du nom de système géré. Voir «Spécification de noms de systèmes gérés uniques pour plusieurs gestionnaires de files d'attente», à la page 964 .
- Pour configurer l'agent WebSphere MQ pour la surveillance éloignée, vous devez effectuer certaines tâches de configuration manuelle après avoir créé une instance d'agent. Pour connaître les instructions, consultez les rubriques suivantes :
  - «Surveillance à distance des gestionnaires de file d'attente sur MQ Appliance», à la page 969
  - «Surveillance à distance des gestionnaires de file d'attente haute disponibilité sur MQ Appliance», à la page 970

Spécification de noms de systèmes gérés uniques pour plusieurs gestionnaires de files d'attente

Parfois, il est nécessaire d'utiliser des noms de système géré uniques afin de différencier des agents de surveillance qui se connectent au même serveur Cloud APM. Utilisez le paramètre **AGTNAME** dans le fichier de réponses silencieux ou l'option `Nom de l'agent` dans la commande **`mq-agent.sh config`** pour indiquer le qualificatif intermédiaire utilisé dans le nom de système géré.

Pourquoi et quand exécuter cette tâche

Au démarrage de l'agent WebSphere MQ, ce dernier enregistre le système géré suivant :

```
nomgestionnairefilesd'attentesurveillé:nomagent:MQ
```

où

- *nomgestionnairefilesd'attentesurveillé* correspond au nom du gestionnaire de files d'attente surveillé par l'agent.
- *nomagent* correspond au qualificatif intermédiaire du nom de système géré. Si la valeur *nomagent* n'est pas spécifiée, aucune valeur n'est utilisée.

La spécification de la valeur du nom de l'agent s'avère utile dans les cas suivants :

- Si votre site comporte plusieurs gestionnaires de files d'attente ayant le même nom et s'exécutant sur des noeuds différents, spécifiez le nom de l'agent pour chaque gestionnaire de files d'attente afin que l'agent WebSphere MQ puisse créer des noms de système géré uniques.
- Si le nom du système géré comporte plus de 32 caractères, 2 noms de gestionnaires de files d'attente différents peuvent être résolus sur le même nom en raison de sa troncature. Pour distinguer les noms de système géré des gestionnaires de files d'attente, indiquez un nom d'agent pour chaque gestionnaire de files d'attente.
- Si vous voulez grouper et identifier les noms de gestionnaire de files d'attente par autre chose que le nom d'hôte et le nom de gestionnaire de files d'attente, comme le nom de cluster haute disponibilité.
- Si vous voulez configurer plusieurs agents connectés au même serveur Cloud APM de sorte qu'ils surveillent les gestionnaires de files d'attente avec le même nom sur des hôtes différents.

Configuration interactive

Procédure

Pour utiliser l'option `Nom de l'agent` dans la commande **`mq-agent.sh config`**, procédez comme suit :

1. Sur la ligne de commande, exécutez la commande suivante pour lancer la configuration de l'agent WebSphere MQ.

   ```
   ./mq-agent.sh config nom_instance
   ```

   où *nom_instance* est le nom de l'instance que vous avez démarrée.
2. Suivez les options pour configurer l'instance d'agent.

   Le nom du gestionnaire de files d'attente est obligatoire. Pour les autres options, si aucune modification n'est nécessaire, utilisez la valeur par défaut.
3. Lorsque l'option `Nom de l'agent` apparaît, indiquez le qualificateur intermédiaire du nom du système géré.

   A faire : Le nom de système géré complet est *nomgestionnairefilesd'attentesurveillé*:*nomagent*:MQ. La longueur maximale pour le nom de système géré complet est de 32 caractères, ce qui signifie que la longueur maximale du qualificateur intermédiaire *nomagent* dépend de la longueur du nom du gestionnaire de files d'attente. Si la valeur spécifiée pour l'option `Nom de l'agent` dépasse la longueur maximale, la valeur de *nomagent* est tronquée à 8 caractères.

   Par exemple, pour surveiller un gestionnaire de files d'attente nommé PERSONNEL sur le noeud AIX1 et qu'un autre gestionnaire nommé PERSONNEL se trouve sur un noeud nommé LINUX2, exécutez la commande suivante pour le noeud AIX1 en premier :

   ```
   ./mq-agent.sh config PERSONNEL
   ```

   Indiquez ensuite le nom de l'agent lorsque l'option *Nom de l'agent* apparaît :

   ```
   Nom de l'agent (par défaut : ) : AIX1
   ```

Pour surveiller simultanément le gestionnaire de files d'attente PERSONNEL sur le noeud LINUX2, exécutez la commande suivante en premier :

```
./mq-agent.sh config PERSONNEL
```

Indiquez ensuite le nom de l'agent :

```
Nom de l'agent (par défaut : ) : LINUX2
```

A faire : Les noms des noeuds d'agent sont utilisés pour l'option `Nom de l'agent` dans les exemples de code à des fins explicatives uniquement. Vous pouvez spécifier d'autres chaînes pour l'option `Nom de l'agent`.

Configuration en mode silencieux

Procédure

Pour utiliser le paramètre **AGTNAME** dans le fichier de réponses silencieux, procédez comme suit :

1. Ouvrez le fichier de réponses silencieux `mq_silent_config.txt` dans un éditeur de texte.
2. Indiquez un nom d'agent pour le paramètre **AGTNAME**.

   A faire : Le nom de système géré complet est *nomgestionnairefilesd'attentesurveillé*:*nomagent*:MQ. La longueur maximale pour le nom de système géré complet est de 32 caractères, ce qui signifie que la longueur maximale du qualificateur intermédiaire *nomagent* dépend de la longueur du nom du gestionnaire de files d'attente. Si la valeur indiquée pour le paramètre **AGTNAME** dépasse la longueur maximale autorisée, la valeur de *nomagent* est tronquée à 8 caractères.
3. Sauvegardez et fermez le fichier `mq_silent_config.txt`, puis exécutez la commande suivante à partir de la ligne de commande :

   ```
   rép_install/BIN/mq-agent.sh config nom_instance chemin_fichier_réponses
   ```

   où *nom_instance* est le nom de l'instance que vous configurez et *chemin_fichier_réponses* le chemin d'accès complet au fichier de réponses silencieux.

Que faire ensuite

Connectez vous à console Cloud APM. Si l'instance d'agent portant l'ancien nom de système géré apparaît toujours comme déconnectée, éditez votre application pour la supprimer, puis ajoutez la nouvelle instance d'agent portant le nom d'agent attribué.

Configuration du suivi des transactions pour l'agent WebSphere MQ

Vous pouvez afficher les données de suivi des transactions d'IBM MQ (WebSphere MQ) dans les tableaux de bord de topologie et du middleware après avoir activé la collecte de données sur la page **Configuration d'agent** pour l'agent WebSphere MQ.

Avant de commencer

- Assurez-vous que la collecte des informations de trace de l'activité des applications MQI est activée au niveau du gestionnaire de files d'attente. Si ce n'est pas fait avant d'avoir configuré et démarré l'agent WebSphere MQ, suivez les instructions de la rubrique «Activation de la trace de l'activité des applications MQI», à la page 960, puis redémarrez l'agent.
- Assurez-vous que la version d'IBM MQ (WebSphere MQ) que vous utilisez est prise en charge par la fonction de suivi des transactions. Pour les informations les plus récentes sur les versions d'IBM MQ (WebSphere MQ) prises en charge, voir la déclaration des prérequis dans le rapport détaillé sur la configuration système requise pour l'agent WebSphere MQ.
- Assurez-vous que l'agent WebSphere MQ est configuré pour surveiller le gestionnaire de files d'attente. Pour obtenir des instructions, voir «Configuration de l'agent WebSphere MQ», à la page 961.

A faire : Vérifiez que vous avez mis à niveau l'agent WebSphere MQ dans sa version la plus récente. Vous devez mettre à niveau l'agent, de même que configurer et activer le suivi des transactions afin de visualiser les données dans certains des widgets, tels le widget Volume des messages.

Procédure

Pour configurer le suivi des transactions pour l'agent WebSphere MQ, procédez comme suit :

1. A partir de la barre de navigation, cliquez sur **Configuration système** > **Configuration d'agent**.
   La page **Configuration d'agent** s'affiche.
2. Cliquez sur l'onglet **WebSphere MQ**.
3. Cochez les cases des gestionnaires de files d'attente que vous voulez surveiller et effectuez l'une des actions suivantes de la liste **Actions** :
   - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Enabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour sur Enabled.

     Conseil : Le suivi des files d'attente alias et des files d'attente éloignées est activé par défaut. Pour réduire le volume de données faisant l'objet du suivi, vous pouvez désactiver le suivi des files d'attente alias et éloignées en cliquant sur **Set Alias Queue Tracking** > **Disabled** dans la liste **Actions**. Une fois le suivi des files d'attente alias et éloignées désactivé, ces files d'attente sont supprimées de la vue de topologie des transactions.
   - Pour activer le suivi des transactions, cliquez sur **Set Transaction Tracking** > **Disabled**. Le statut indiqué dans la colonne **Transaction Tracking** est mis à jour et défini sur Disabled.

Résultats

Vous avez configuré l'agent WebSphere MQ pour le suivi des gestionnaires de files d'attente sélectionnés. Les données de suivi des transactions peuvent être affichées dans les tableaux de bord de topologie et de middleware. Pour plus d'informations, voir «Ajout d'applications middleware au Tableau de bord d'Application Performance », à la page 100.

Activation de la collecte de données pour l'historique à long terme de files d'attente et de canal

Par défaut, l'historique à long terme de file d'attente et de canal n'est pas collecté et n'est pas affiché dans les tableaux de bord ou widgets de groupe prédéfinis. Toutefois, vous pouvez activer l'agent pour la collecte des données d'historique à long terme, et utiliser ensuite l'onglet **Détails d'attribut** pour interroger les données collectées.

Avant de commencer

Vérifiez que l'agent WebSphere MQ est installé et configuré. Pour plus d'informations, voir «Configuration de l'agent WebSphere MQ», à la page 961.

Pourquoi et quand exécuter cette tâche

Les données d'historique à long terme de canal ou de file d'attente peuvent être utiles pour détecter les problèmes liés à des canaux ou files d'attente individuels.

Si vous êtes un utilisateur de Tivoli Data Warehouse, l'agent peut également envoyer les données d'historique à long terme à Tivoli Data Warehouse pour un traitement supplémentaire.

Procédure

Exécutez les étapes suivantes pour permettre à l'agent WebSphere MQ de collecter les données d'historique à long terme de file d'attente ou de canal :

1. Ouvrez le ficher d'environnement suivant avec un éditeur de texte. Si le fichier `mq.environment` n'existe pas, créez-le vous-même.
   - Linux AIX *rép_install*`/config/mq.environment`

- Windows *rép_install*\Config\KMQENV_*instance*

  où :

  - *rép_install* est le répertoire d'installation de l'agent. Par défaut, il s'agit de /opt/ibm/apm sur les systèmes Linux et AIX, et de C:\IBM\APM sur les systèmes Windows.
  - *instance* est le nom de l'instance d'agent.

2. Activez la collecte de données en définissant **LH_COLLECTION** à la valeur ENABLED.

   ```
   LH_COLLECTION=ENABLED
   ```

3. Facultatif : Si vous êtes un utilisateur de Tivoli Data Warehouse et souhaitez que l'agent envoie les données collectées à Tivoli Data Warehouse, définissez **LH_PVTHISTORY** à la valeur ENABLED.

   ```
   LH_PVTHISTORY=ENABLED
   ```

   A faire : Activez cette option uniquement si les données collectées doivent être envoyées à Tivoli Data Warehouse.

4. Sauvegardez votre modification et redémarrez l'agent.

Résultats

L'agent WebSphere MQ commence à collecter les données d'historique à long terme de file d'attente et de canal. Si vous avez spécifié LH_PVTHISTORY=ENABLED, les données d'historique à long terme collectées peuvent également être envoyées à Tivoli Data Warehouse.

Que faire ensuite

Utilisez l'onglet **Détails d'attribut** pour afficher les données collectées dans le tableau de bord de l'instance d'agent configurée. Sélectionnez **Channel_Long-Term_History** ou **Queue_Long-Term_History** dans la liste **Jeu de données**. Pour plus d'informations sur l'onglet **Détails d'attribut**, voir «Création d'une page de graphiques ou de tableaux personnalisés», à la page 1123.

Activation de la surveillance des statistiques de file d'attente pour le gestionnaire de files d'attente IBM MQ

Par défaut, les statistiques de file d'attente ne sont pas collectées et ne s'affichent dans aucun tableau de bord ou widget de groupe. Vous pouvez cependant permettre à l'agent de collecter des statistiques pour le gestionnaire de files d'attente et d'afficher ensuite les données collectées.

Avant de commencer

Vérifiez que l'agent WebSphere MQ est installé et configuré. Pour plus d'informations, voir «Configuration de l'agent WebSphere MQ», à la page 961.

Procédure

Pour permettre à l'agent WebSphere MQ de collecter les données statistiques, procédez comme suit :

1. Configurez le gestionnaire de files d'attente pour qu'il collecte les informations sur les statistiques de file d'attente. Exécutez la commande MQSC suivante :

   ```
   ALTER QMGR STATQ(ON)
   ```

2. Définissez l'intervalle au cours duquel les données comptables sont collectées. Exécutez la commande suivante :

   ```
   ALTER QMGR STATINT(n)
   ```

   Où **n** est le nombre de secondes correspondant à la période au cours de laquelle les données comptables sont collectées.

3. Activez la collecte des informations statistiques pour une file d'attente spécifique. Exécutez la commande MQSC suivante :

```
ALTER QLOCAL(nom_file_attente) STATQ(QMGR)
```

Où **nom_file_attente** est le nom de la file d'attente pour laquelle vous souhaitez collecter les informations statistiques.

Que faire ensuite

Utilisez l'une des méthodes suivantes pour afficher les données sur la surveillance des statistiques de file d'attente MQ :

- Affichez les données de surveillance dans l'onglet **Détails d'attribut** du jeu de données **MQ_Queue_Statistics**. Pour plus d'informations sur l'onglet **Détails d'attribut**, voir «Création d'une page de graphiques ou de tableaux personnalisés», à la page 1123.
- Définissez les seuils basés sur les indicateurs de **MQ_Queue_Statistics**, tels que **Expired Message Count**. Pour plus d'informations sur les seuils, voir «Seuils et groupes de ressources», à la page 1004.

Surveillance à distance des gestionnaires de file d'attente sur MQ Appliance

Vous pouvez utiliser l'agent WebSphere MQ pour surveiller le gestionnaire de files d'attente éloignées dans l'environnement MQ Appliance.

Avant de commencer

- Installez l'agent WebSphere MQ sur une plateforme prise en charge.
- Installez le client IBM MQ. Sa version doit être la même que celle du gestionnaire de files d'attente MQ distant.

Procédure

1. Configuration d'une connexion au gestionnaire de files d'attente distant. Sur ce dernier, définissez un canal de connexion au serveur et un programme d'écoute utilisé pour la communication avec l'agent de surveillance. Exécutez la commande suivante :

```
M2000# mqcli
M2000(mqcli)#runmqsc gest_file_att_éloign
> DEFINE LISTENER(prog_écoute) TRPTYPE(TCP) PORT(num_port)
> DEFINE CHANNEL(nom_canal)CHLTYPE(SVRCONN) TRPTYPE(TCP)
CONNAME('IP_hôte(num_port)') QMNAME(gest_file_att_éloign)
> END
```

   où :

   - *gest_file_att_éloign* est le nom du gestionnaire de files d'attente éloignées.
   - *prog_écoute* est le nom du programme d'écoute sur le gestionnaire de files d'attente éloignées.
   - *num_port* est le numéro de port à utiliser pour le programme d'écoute.
   - *nom_canal* est le nom que vous attribuez au canal serveur et au canal client.
   - *IP_hôte* est l'adresse IP du système distant.
2. Configurez le programme d'écoute de sorte qu'il démarre automatiquement, puis démarrez le programme d'écoute sur le gestionnaire de files d'attente éloignées en exécutant les commandes suivantes sur le système distant :

```
M2000# mqcli
M2000(mqcli)#runmqsc gest_file_att_éloign
> ALTER LISTENER(prog_écoute) TRPTYPE(tcp) CONTROL(gest_file_att_éloign)
> START LISTENER(prog_écoute)
> END
```

3. Vérifiez que les paramètres d'authentification de canal sont correctement configurés pour l'ID utilisateur ayant servi à démarrer l'instance de l'agent MQ. Pour plus d'informations, voir Setting up a queue manager to accept client connections dans IBM MQ Appliance Knowledge Center.

4. Créez une instance de l'agent WebSphere MQ pour la surveillance à distance en suivant les instructions présentées dans «Configuration de l'agent WebSphere MQ», à la page 961 et fournissez les informations de connexion au gestionnaire de files d'attente distant dans les invites qui s'affichent après **Remote Monitoring Settings**.

```
Remote Monitoring Settings (For a local queue manager, just press Enter in
this section) :
Connection name for remote monitoring, for example: 192.168.1.1(1415)
Connection Name (default is: null):
Channel name for remote monitoring, SYSTEM.DEF.SVRCONN is as default.
Channels (default is: null):
```

5. Démarrez l'instance de l'agent WebSphere MQ.

Surveillance à distance des gestionnaires de file d'attente haute disponibilité sur MQ Appliance

Pour surveiller le gestionnaire de file d'attente haute disponibilité à distance sur MQ Appliance, vous avez deux options. La première option consiste à utiliser une instance d'agent unique pour vous connecter à un système doté du gestionnaire de file d'attente actif. La seconde option consiste à utiliser une instance d'agent distincte pour chaque dispositif sur lequel le gestionnaire de file d'attente pourrait s'exécuter.

Pourquoi et quand exécuter cette tâche

Seule la seconde option est décrite ici. Pour utiliser les différentes instances d'agent, vous avez besoin de deux installations de l'agent WebSphere MQ sur les systèmes Linux ou UNIX. Sur les systèmes Windows, vous n'avez besoin que d'une installation de l'agent et vous devez créer des instances d'agent distinctes.

Procédure

- Linux AIX

  Procédez comme suit pour utiliser l'agent WebSphere MQ installé sur les systèmes Linux ou UNIX pour la surveillance éloignée :

  a) Installez l'agent WebSphere MQ dans différents répertoires sur le système.

  b) Créez une instance de chaque agent WebSphere MQ installé. Pour obtenir des instructions, voir «Configuration de l'agent WebSphere MQ», à la page 961.

  c) Modifiez le fichier de configuration de chaque instance d'agent de sorte à activer la surveillance éloignée en remplaçant son contenu par les lignes suivantes :

```
SET GROUP NAME (GROUP1) -
DEFAULT(YES) -
RETAINHIST(120) -
COMMAND (YES) -
MSGACCESS(DESC) -
EVENTS(REMOVE) -
ACCOUNTINGINFO(REMOVE) -
STATISTICSINFO(REMOVE)

SET MANAGER NAME(nom_gest_file_att) REMOTE(YES)
SET AGENT NAME(IDagent)
SET QUEUE NAME(*) MGRNAME(nom_gest_file_att) QDEFTYPE(PREDEFINED)
SET CHANNEL NAME(*) MGRNAME(nom_gest_file_att)
PERFORM STARTMON SAMPINT(300) HISTORY(NO)
```

  où :

  – *nom_gest_file_att* est le nom du gestionnaire de files d'attente haute disponibilité.

  – *IDagent* est l'ID qui identifie le système du gestionnaire de file d'attente. Il s'agit généralement du nom d'hôte ou de l'adresse IP du système distant sur lequel le gestionnaire de file d'attente haute disponibilité s'exécute.

  Le nom et le chemin d'accès du fichier de configuration sont les suivants : *rép_install*/config/*nom_hôte*_mq_*nom_gest_file_att*.cfg.

d) Créez une paire de canaux client et serveur entre le gestionnaire de file d'attente principal et l'agent WebSphere MQ et entre le gestionnaire de file d'attente secondaire et l'agent WebSphere MQ sur le système distant où le gestionnaire de file d'attente principal est installé.

A faire : Vous devez exécuter toutes les commandes suivantes avant de passer à l'étape suivante.

a. Exécutez les commandes suivantes pour le gestionnaire de file d'attente principal :

```
M2000# mqcli
M2000(mqcli)#runmqsc gest_file_att_principal
>DEFINE LISTENER(prog_écoute_principal) TRPTYPE(TCP) PORT(num_port_principal)
>DEFINE CHANNEL(nom_canal_principal) CHLTYPE(SVRCONN) TRPTYPE(TCP)
>DEFINE CHANNEL(nom_canal_principal) CHLTYPE(CLNTCONN) TRPTYPE(TCP)
CONNAME('IP_hôte(num_port_principal)') QMNAME(gest_file_att_principal)
```

où :

- *gest_file_att_principal* est le nom du gestionnaire de files d'attente principal.
- *prog_écoute_principal* est le nom du programme d'écoute pour le gestionnaire de files d'attente principal.
- *num_port_principal* est le numéro du port utilisé par le programme d'écoute.
- *nom_canal_principal* est le nom que vous attribuez au canal serveur et au canal client.
- *IP_hôte* est l'adresse IP du système sur lequel le gestionnaire de file d'attente principal est installé.

b. Exécutez les commandes suivantes pour le gestionnaire de file d'attente secondaire sur le gestionnaire de file d'attente principal. Cette opération permet d'ajouter les informations de connexion pour le gestionnaire de file d'attente secondaire au fichier de table de définition de canal du client du gestionnaire de file d'attente principal. Le même agent peut ensuite se connecter au gestionnaire de file d'attente secondaire automatiquement lorsque le gestionnaire de file d'attente principal procède à une reprise en ligne.

```
>DEFINE LISTENER(prog_écoute_secondaire) TRPTYPE(TCP) PORT(num_port_secondaire)
>DEFINE CHANNEL(nom_canal_secondaire) CHLTYPE(SVRCONN) TRPTYPE(TCP)
>DEFINE CHANNEL(nom_canal_secondaire) CHLTYPE(CLNTCONN) TRPTYPE(TCP)
CONNAME('IP_hôte(num_port_secondaire)') QMNAME(gest_file_att_secondaire)
```

où :

- *gest_file_att_secondaire* est le nom du gestionnaire de file d'attente secondaire sur le système distant. Il est identique au nom du gestionnaire de files d'attente principal.
- *prog_écoute_secondaire* est le nom du programme d'écoute pour le gestionnaire de files d'attente secondaire.
- *num_port_secondaire* est le numéro du port utilisé par le programme d'écoute.
- *nom_canal_secondaire* est le nom que vous attribuez au canal serveur et au canal client.
- *IP_hôte* est l'adresse IP du système sur lequel le gestionnaire de file d'attente secondaire est installé.

c. Enfin, exécutez la commande suivante :

```
> END
>EXIT
```

e) Créez le fichier de table de définition de canal du client (AMQCLCHL.TAB) pour l'instance de l'agent WebSphere MQ sur le premier dispositif MQ.

a. Utilisez la commande **runmqsc** ou **runmqsc -n** pour créer le fichier AMQCLCHL.TAB du gestionnaire de files d'attente sur le premier dispositif MQ :

```
runmqsc -n
>DEFINE CHANNEL(nom_canal_principal) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+
>CONNAME('IP_hôte_dispositif1(num_port_principal)') QMNAME(nom_gest_file_att)
```

où *IP_hôte_dispositif1* est l'adresse IP du premier dispositif MQ ; les valeurs de *nom_canal_principal* et *num_port_principal* sont identiques à celles que vous avez définies à l'étape 4.

Conseil : Par défaut, le fichier AMQCLCHL.TAB est créé dans le répertoire `var/mqm/qmgrs/nom_gest_file_att/@ipcc`.

b. Déplacez le fichier AMQCLCHL.TAB principal dans le répertoire *rép_install_agent*`/arch/mq/bin` sur le système où l'agent WebSphere MQ est installé pour le gestionnaire de files d'attente principal.

f) Créez le fichier de table de définition de canal du client (AMQCLCHL.TAB) pour l'instance de l'agent WebSphere MQ sur le deuxième dispositif MQ.

a. Utilisez la commande **runmqsc** ou **runmqsc -n** pour créer le fichier AMQCLCHL.TAB du gestionnaire de files d'attente sur le deuxième dispositif MQ :

```
runmqsc -n
>DEFINE CHANNEL(nom_canal_secondaire) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+
>CONNAME('IP_hôte_dispositif2(num_port_secondaire)') QMNAME(nom_gest_file_att)
```

où *IP_hôte_dispositif2* est l'adresse IP du deuxième dispositif MQ ; les valeurs de *nom_canal_secondaire* et *num_port_secondaire* sont identiques à celles que vous avez définies à l'étape 4.

b. Déplacez le fichier AMQCLCHL.TAB secondaire dans le répertoire *rép_install_agent*`/arch/mq/bin` sur le système où l'agent WebSphere MQ est installé pour le gestionnaire de files d'attente secondaire.

g) Vérifiez que les paramètres d'authentification de canal sont correctement configurés pour l'ID utilisateur utilisé pour configurer la connexion entre l'instance d'agent et le gestionnaire de file d'attente.

h) Démarrez tous les programmes d'écoute pour le gestionnaire de file d'attente surveillé à distance et démarrez toutes les instances de l'agent WebSphere MQ.

- Windows

Procédez comme suit pour utiliser l'agent WebSphere MQ installé sur les systèmes Windows pour la surveillance éloignée :

a) Installez l'agent WebSphere MQ sur le système Windows.

b) Créez deux instances de l'agent WebSphere MQ pour chaque gestionnaire de file d'attente haute disponibilité.

c) Modifiez le fichier de configuration de chaque instance d'agent de sorte à activer la surveillance éloignée en remplaçant son contenu par les lignes suivantes :

```
SET GROUP NAME (GROUP1) -
DEFAULT(YES) -
RETAINHIST(120) -
COMMAND (YES) -
MSGACCESS(DESC) -
EVENTS(REMOVE) -
ACCOUNTINGINFO(REMOVE) -
STATISTICSINFO(REMOVE)

SET MANAGER NAME(nom_gest_file_att) REMOTE(YES)
SET AGENT NAME(IDagent)
SET QUEUE NAME(*) MGRNAME(nom_gest_file_att) QDEFTYPE(PREDEFINED)
SET CHANNEL NAME(*) MGRNAME(nom_gest_file_att)
PERFORM STARTMON SAMPINT(300) HISTORY(NO)
```

où :

– *nom_gest_file_att* est le nom du gestionnaire de files d'attente haute disponibilité.

– *IDagent* est l'ID qui identifie le système du gestionnaire de file d'attente. Il s'agit généralement du nom d'hôte ou de l'adresse IP du système distant sur lequel le gestionnaire de file d'attente haute disponibilité s'exécute.

Conseil : Le nom et le chemin d'accès du fichier de configuration sont les suivants : *rép_install* \TMAITM6_x64\mq_<*nom_instance*>.cfg.

d) Créez une paire de canaux client et serveur entre le gestionnaire de file d'attente principal et l'agent WebSphere MQ et entre le gestionnaire de file d'attente secondaire et l'agent WebSphere MQ sur le système distant où le gestionnaire de file d'attente principal est installé.

A faire : Vous devez exécuter toutes les commandes suivantes avant de passer à l'étape suivante.

a. Exécutez les commandes suivantes pour le gestionnaire de file d'attente principal :

```
M2000# mqcli
M2000(mqcli)#runmqsc gest_file_att_principal
>DEFINE LISTENER(prog_écoute_principal) TRPTYPE(TCP) PORT(num_port_principal)
>DEFINE CHANNEL(nom_canal_principal) CHLTYPE(SVRCONN) TRPTYPE(TCP)
>DEFINE CHANNEL(nom_canal_principal) CHLTYPE(CLNTCONN) TRPTYPE(TCP)
CONNAME('IP_hôte(num_port_principal)') QMNAME(gest_file_att_principal)
```

où :

- *gest_file_att_principal* est le nom du gestionnaire de files d'attente principal.
- *prog_écoute_principal* est le nom du programme d'écoute pour le gestionnaire de files d'attente principal.
- *num_port_principal* est le numéro du port utilisé par le programme d'écoute.
- *nom_canal_principal* est le nom que vous attribuez au canal serveur et au canal client.
- *IP_hôte* est l'adresse IP du système sur lequel le gestionnaire de file d'attente principal est installé.

b. Exécutez les commandes suivantes pour le gestionnaire de file d'attente secondaire sur le gestionnaire de file d'attente principal. Cette opération permet d'ajouter les informations de connexion pour le gestionnaire de file d'attente secondaire au fichier de table de définition de canal du client du gestionnaire de file d'attente principal. Le même agent peut ensuite se connecter au gestionnaire de file d'attente secondaire automatiquement lorsque le gestionnaire de file d'attente principal procède à une reprise en ligne.

```
>DEFINE LISTENER(prog_écoute_secondaire) TRPTYPE(TCP) PORT(num_port_secondaire)
>DEFINE CHANNEL(nom_canal_secondaire) CHLTYPE(SVRCONN) TRPTYPE(TCP)
>DEFINE CHANNEL(nom_canal_secondaire) CHLTYPE(CLNTCONN) TRPTYPE(TCP)
CONNAME('IP_hôte(num_port_secondaire)') QMNAME(gest_file_att_secondaire)
```

où :

- *gest_file_att_secondaire* est le nom du gestionnaire de file d'attente secondaire sur le système distant. Il est identique au nom du gestionnaire de files d'attente principal.
- *prog_écoute_secondaire* est le nom du programme d'écoute pour le gestionnaire de files d'attente secondaire.
- *num_port_secondaire* est le numéro du port utilisé par le programme d'écoute.
- *nom_canal_secondaire* est le nom que vous attribuez au canal serveur et au canal client.
- *IP_hôte* est l'adresse IP du système sur lequel le gestionnaire de file d'attente secondaire est installé.

c. Enfin, exécutez la commande suivante :

```
> END
>EXIT
```

e) Créez le fichier de table de définition de canal du client (AMQCLCHL.TAB) pour chaque instance de l'agent WebSphere MQ.

a. Utilisez la commande **runmqsc** ou **runmqsc -n** pour créer le fichier AMQCLCHL.TAB du gestionnaire de files d'attente sur le premier dispositif MQ :

```
runmqsc -n
>DEFINE CHANNEL(nom_canal_principal) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+
>CONNAME('IP_hôte_dispositif1(num_port_principal)') QMNAME(nom_gest_file_att)
```

où *IP_hôte_dispositif1* est l'adresse IP du premier dispositif MQ ; les valeurs de *nom_canal_principal* et *num_port_principal* sont identiques à celles que vous avez définies à l'étape 4.

b. Créez le fichier AMQCLCHL.TAB du gestionnaire de files d'attente sur le deuxième dispositif MQ :

```
runmqsc -n
>DEFINE CHANNEL(nom_canal_secondaire) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+
>CONNAME('IP_hôte_dispositif2(num_port_secondaire)') QMNAME(nom_gest_file_att)
```

où *IP_hôte_dispositif2* est l'adresse IP du deuxième dispositif MQ ; les valeurs de *nom_canal_secondaire* et *num_port_secondaire* sont identiques à celles que vous avez définies à l'étape 4.

f) Attribuez aux deux fichiers AMQCLCHL.TAB des noms différents, par exemple, NODE1.TAB et NODE2.TAB. Transférez-les vers le répertoire *rép_install*\TMAITM6_x64, où *rép_install* est le répertoire d'installation de l'agent WebSphere MQ.

g) Modifiez le fichier kmqcma_*nom_instance*.ini de sorte à définir la valeur de **MQCHLTAB** sur le fichier de table de définition de canal du client pour chaque instance d'agent.
Par exemple, définissez MQCHLTAB=NODE1.TAB dans le fichier kmqcma_instance1.ini et MQCHLTAB=NODE2.TAB dans le fichier kmqcma_instance2.ini.

h) Ouvrez Windows Register Editor, localisez la clé **MQCHLTAB** et redéfinissez sa valeur AMQCLCHL.TAB sur le nom du fichier de table de définition de canal du client approprié pour chaque instance d'agent.

- **HKEY_LOCAL_MACHINE\SOFTWARE\Candle\KMQ\Ver730*instance1*\Environment**

  MQCHLTAB=*NODE1.TAB*

- **HKEY_LOCAL_MACHINE\SOFTWARE\Candle\KMQ\Ver730*instance2*\Environment**

  MQCHLTAB=*NODE2.TAB*

i) Vérifiez que les paramètres d'authentification de canal sont correctement configurés pour l'ID utilisateur utilisé pour configurer la connexion entre l'instance d'agent et le gestionnaire de file d'attente.

j) Démarrez tous les programmes d'écoute pour le gestionnaire de file d'attente surveillé à distance et démarrez toutes les instances de l'agent WebSphere MQ.

Chapitre 8. Intégration à d'autres produits et composants

Vous pouvez intégrer d'autres produits et composants à IBM Cloud Application Performance Management afin d'obtenir une solution robuste.

Intégration à Cloud Event Management

Cloud Event Management permet de gérer les incidents en temps réel dans vos services, vos applications et votre infrastructure. Lorsque vous configurez l'intégration entre Cloud Event Management et IBM Cloud Application Performance Management, tous les événements générés dans Cloud APM sont envoyés à Cloud Event Management.

Pourquoi et quand exécuter cette tâche

Configurez une URL de webhook dans Cloud Event Management. Configurez ensuite Cloud APM de sorte à utiliser l'URL de webhook pour envoyer des événements à Cloud Event Management. Pour plus d'informations sur Cloud Event Management, voir le Knowledge Center d'IBM Cloud Event Management.

Procédure

1. Cliquez sur **Intégrations** sur la page Cloud Event Management **Administration**.
2. Cliquez sur **Configurer une intégration**.
3. Accédez à la vignette **IBM Cloud Application Performance Management** et cliquez sur **Configurer**.
4. Attribuez un nom à l'intégration et cliquez sur **Copier** pour ajouter l'URL de webhook générée au presse-papiers. Veillez à sauvegarder le webhook généré pour qu'il soit disponible ultérieurement dans le processus de configuration. Vous pouvez par exemple le sauvegarder dans un fichier.
5. Pour commencer à recevoir des informations d'alerte de Cloud APM, assurez-vous de définir l'option d'**activation de la gestion des événements depuis cette source** sur `activé` dans Cloud Event Management.
6. Cliquez sur **Sauvegarder**.
7. Connectez-vous à votre abonnement Cloud APM.
8. Accédez à **Configuration système** > **Configuration avancée** > **Gestionnaire d'événements**. Pour plus d'informations, voir Configuration avancée.
9. Collez l'URL de webhook dans la zone **Webhook de gestion des événements Cloud**.
10. Cliquez sur **Sauvegarder**.

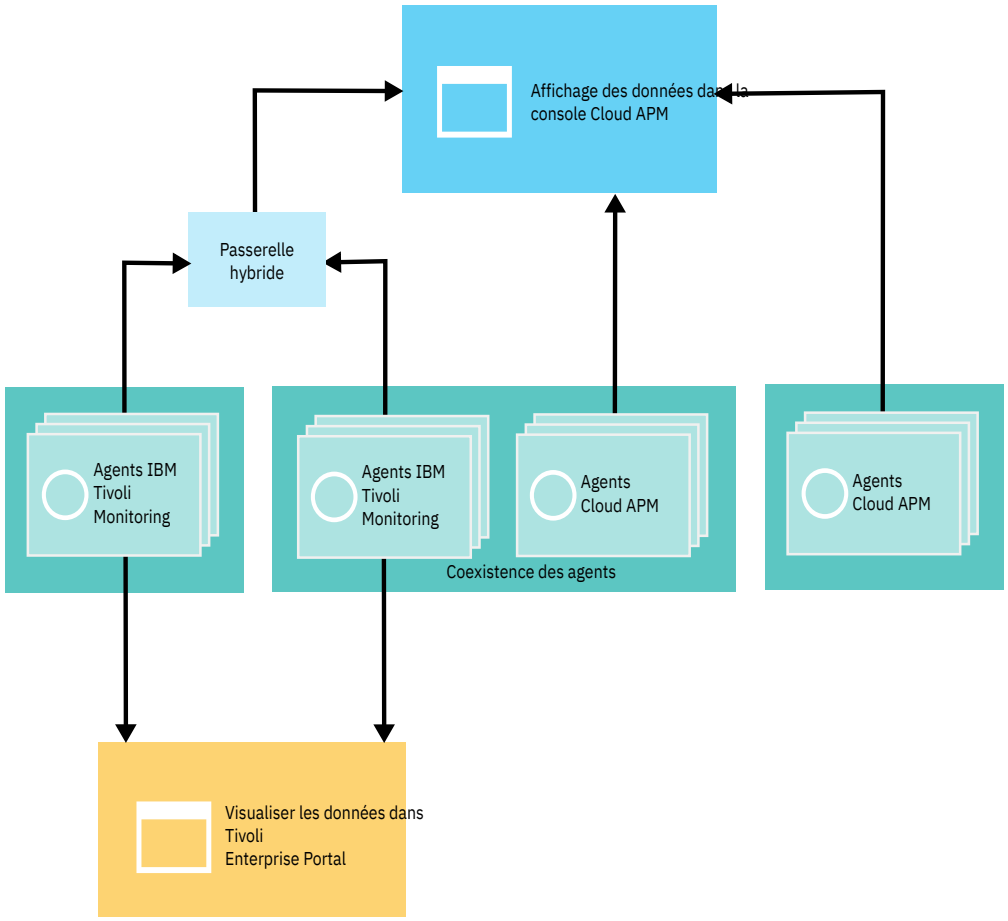
Intégration à IBM Tivoli Monitoring V6.3

Dans un environnement qui inclut les produits IBM Tivoli Monitoring et IBM Cloud Application Performance Management, vous pouvez utiliser ces produits ensemble de plusieurs façons.

Les options suivantes sont disponibles pour l'intégration à IBM Tivoli Monitoring :

- Vous pouvez installer la Passerelle hybride d'IBM Cloud Application Performance Management pour offrir une vue consolidée des systèmes gérés à partir d'un ou plusieurs domainesTivoli Monitoring et de votre domaine Cloud APM dans les pages du Tableau de bord d'Application Performance. Pour plus d'informations sur l'intégration des agents, voir «Passerelle hybride», à la page 979.
- Vous pouvez installer des agents Tivoli Monitoring et Cloud APM sur le même système. Lorsque des agents coexistent sur le même ordinateur, mais ne sont pas dans le même répertoire, les données des agents Cloud APM sont disponibles dans la console Cloud APM et les données des agents Tivoli

Monitoring sont disponibles dans Tivoli Enterprise Portal. Si des agents coexistants surveillent les mêmes ressources, certaines limitations s'appliquent. Pour plus d'informations sur la coexistence des agents, voir «Coexistence de l'agent Cloud APM et de l'agent Tivoli Monitoring», à la page 976.



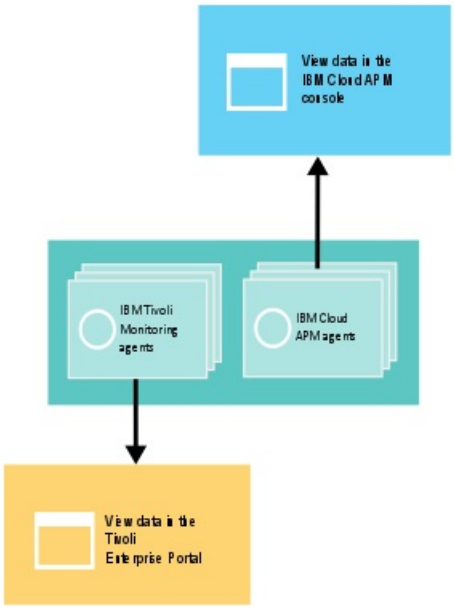
Coexistence de l'agent Cloud APM et de l'agent Tivoli Monitoring

La coexistence des agents est prise en charge. Vous pouvez installer les agents IBM Cloud Application Performance Management sur le même ordinateur que les agents IBM Tivoli Monitoring. Cependant, les deux types d'agent ne peuvent pas être installés dans le même répertoire.

Les agents Cloud APM sont mentionnés sous le nom d'agents de la version 8. Les agents Tivoli Monitoring sont mentionnés sous le nom d'agents de la version 6 ou 7.

Lorsque des agents coexistent sur le même ordinateur, les données issues des agents version 8 sont disponibles dans la console Cloud APM et les données issues des agents version 6 ou 7 sont disponibles dans Tivoli Enterprise Portal.

Lorsque des agents version 6 ou 7 qui coexistent sur le même ordinateur que des agents version 8 et qui surveillent différentes ressources, sont intégrés à la Passerelle hybride d'IBM Cloud Application Performance Management, les données issues des deux versions d'agents sont disponibles dans la console Cloud APM. Pour plus d'informations, voir «Passerelle hybride», à la page 979.



Le tableau suivant dresse la liste des agents Tivoli Monitoring avec des liens de documentation :

Tableau 236. Liens de documentation pour les agents Tivoli Monitoring

Agents Tivoli Monitoring	**Liens de l'ensemble de rubriques IBM Knowledge Center**
IBM Monitoring Agent for Citrix Virtual Desktop Infrastructure	IBM Tivoli Monitoring for Virtual Environments
IBM Tivoli Monitoring for Virtual Environments Agent for Cisco UCS	IBM Tivoli Monitoring for Virtual Environments
IBM Tivoli Monitoring for Virtual Environments Agent for Linux Kernel-based Virtual Machines	IBM Tivoli Monitoring for Virtual Environments
IBM Tivoli Monitoring for Virtual Environments Agent for VMware VI	IBM Tivoli Monitoring for Virtual Environments
IBM Tivoli Monitoring: HMC Base Agent	IBM Tivoli Monitoring
IBM Tivoli Monitoring: Linux OS Agent	IBM Tivoli Monitoring
IBM Tivoli Monitoring: UNIX OS Agent	IBM Tivoli Monitoring
IBM Tivoli Monitoring : Agent Windows OS	IBM Tivoli Monitoring
ITCAM Agent for DB2	ITCAM for Applications
Agent ITCAM pour les serveurs HTTP	ITCAM for Applications
ITCAM Agent for J2EE	ITCAM for Applications
ITCAM for Microsoft Applications : agent Microsoft Active Directory	ITCAM for Microsoft Applications
ITCAM for Microsoft Applications: Microsoft Cluster Server Agent	ITCAM for Microsoft Applications
ITCAM for Microsoft Applications: Microsoft Exchange Server Agent	ITCAM for Microsoft Applications
ITCAM for Microsoft Applications: Microsoft Hyper-V Server Agent	ITCAM for Microsoft Applications

Tableau 236. Liens de documentation pour les agents Tivoli Monitoring (suite)	
Agents Tivoli Monitoring	**Liens de l'ensemble de rubriques IBM Knowledge Center**
ITCAM for Microsoft Applications: Microsoft Internet Information Services Agent	ITCAM for Microsoft Applications
ITCAM for Microsoft Applications: Skype for Business Server Agent	ITCAM for Microsoft Applications
ITCAM for Microsoft Applications: Microsoft .NET Framework Agent	ITCAM for Microsoft Applications
ITCAM for Microsoft Applications: Microsoft SharePoint Server Agent	ITCAM for Microsoft Applications
Monitoring Agent for Microsoft SQL Server	ITCAM for Microsoft Applications
ITCAM Agent for SAP Applications	ITCAM for Applications
ITCAM Agent for WebSphere Applications	IBM Tivoli Composite Application Manager for Application Diagnostics pour les versions 7.1 et précédentes et dans ITCAM for Applications pour les versions 7.2 et ultérieures.
ITCAM Agent for WebSphere DataPower Appliance	ITCAM for Applications
Monitoring Agent for WebSphere Message Broker	ITCAM for Applications
Monitoring Agent for WebSphere MQ	Knowledge Center d'ITCAM for Applications
ITCAM Extended Agent for Oracle Database	ITCAM for Applications
ITCAM Monitoring Agent for SAP HANA Database	Informations de référence sur ITCAM Monitoring Agent for SAP HANA Database
ITCAM Web Response Time Agent	IBM Tivoli Composite Application Manager pour des transactions

Si des agents coexistants surveillent les mêmes ressources, le scénario suivant n'est pas pris en charge :

- Les agents version 6 ou 7 sont intégrés à la Passerelle hybride pour afficher des données issues des deux agents dans la console Cloud APM. Par exemple, si les agents version 6 ou 7 sont connectés à la même instance de serveur Cloud APM via la Passerelle hybride, n'utilisez pas l'agent IBM Integration Bus version 8 ni Monitoring Agent for WebSphere Message Broker version 6 ou 7 pour surveiller le même courtier sur votre système.

Si un agent Tivoli Monitoring, intégré à la Passerelle hybride pour afficher les données dans la console Cloud APM, surveille une ressource et que vous voulez que votre agent Cloud APM surveille cette ressource, procédez comme suit :

1. Supprimez l'agent Tivoli Monitoring de toutes les applications qui l'incluent.
2. Supprimez l'agent Tivoli Monitoring du groupe de systèmes gérés Tivoli Monitoring dont l'utilisation a été configurée dans Cloud APM.
3. Attendez au moins 24 heures, puis installez l'agent Cloud APM et ajoutez-le à une application.

Lorsque des agents multi-instances qui coexistent sur le même ordinateur sont intégrés à la Passerelle hybride et surveillent les mêmes ressources, attribuez des noms différents à chaque instance pour afficher les données issues des deux agents dans la console Cloud APM.

Pour les agents dotés d'un collecteur de données, deux agents du même type sont pris en charge. Les données de diagnostic approfondi, de ressource et de suivi des transactions s'affichent dans la console Cloud APM. Les données de ressource s'affichent dans Tivoli Enterprise Portal. Les agents suivants partagent un collecteur de données :

Monitoring Agent for HTTP Server

L'agent HTTP Server est un agent Cloud APM et l'Agent ITCAM pour les serveurs HTTP est un agent IBM Tivoli Monitoring. Si vous disposez des deux agents dans votre environnement, vous pouvez configurer les deux collecteurs de données sur le même serveur HTTP pour les deux agents. Pour plus d'informations sur l'agent HTTP Server, voir «Configuration de la surveillance de HTTP Server», à la page 275.

agent Microsoft .NET

Pour plus d'informations sur la coexistence de l'agent Microsoft .NET, voir «Activation du suivi des transactions dans l'environnement de coexistence d'agent», à la page 540.

Agent WebSphere Applications

Pour plus d'informations sur la coexistence de l'Agent WebSphere Applications, voir «Configuration de l'Agent WebSphere Applications», à la page 884 et «Configuration du collecteur de données pour l'environnement de coexistence d'agent», à la page 886.

Passerelle hybride

Pour afficher les données de surveillance et les événements de vos agents IBM Tivoli Monitoring et OMEGAMON dans la console Cloud APM, vous devez créer un groupe de systèmes gérés et installer la Passerelle hybride d'IBM Cloud Application Performance Management dans votre domaine Tivoli Monitoring, et configurer des communications dans la console Cloud APM **Gestionnaire de passerelle hybride**. Consultez les informations de référence pour vous aider à planifier l'installation et la configuration d'une ou plusieurs Passerelles hybrides dans vos environnements Tivoli Monitoring et Cloud APM.

Où installer la Passerelle hybride

Vous pouvez installer la Passerelle hybride dans un ou plusieurs domaines Tivoli Monitoring : un Tivoli Enterprise Monitoring Server concentrateur par domaine. Pour plus d'informations sur l'emplacement d'installation de la Passerelle hybride, voir les informations de la rubrique Préparation de l'installation de la passerelle hybride. Pour connaître la configuration système requise pour la Passerelle hybride qui comprend Tivoli Enterprise Portal Server, voir le site Hybrid Gateway Software Product Compatibility report (onglet **Prerequisites**).

Agents Tivoli Monitoring et OMEGAMON pris en charge

Pour qu'un agent Tivoli Monitoring soit disponible pour la Passerelle hybride, il doit également être pris en charge dans Cloud APM, à l'exception des agents iOS et OMEGAMON. Pour une liste des agents et versions Tivoli Monitoring disponibles, voir Hybrid Gateway supported agents (APM Developer Center).

Pour obtenir la liste des agents OMEGAMON que vous pouvez afficher dans la console Cloud APM, consultez la rubrique d'initiation correspondant à votre édition dans l'ensemble de rubriques relatives à IBM OMEGAMON for Application Performance Management dans IBM Knowledge Center.

Agents Tivoli Monitoring et OMEGAMON dans la console Cloud APM

Après avoir sélectionné l'application prédéfinie "Mes composants" ou une application définie dans le Tableau de bord d'Application Performance qui inclut Tivoli Monitoring ou des systèmes gérés OMEGAMON (ou les deux), un tableau de bord de statut récapitulatif de tous les systèmes gérés s'affiche, ainsi qu'un tableau de bord détaillé d'une instance de système géré unique. Vous pouvez également créer des pages de tableau de bord dans l'onglet **Vues personnalisées**.

Vous pouvez afficher les événements de situation pour ces agents dans l'onglet **Evénements**. En revanche, vous ne pouvez pas créer de nouveaux seuils pour les agents Tivoli Monitoring et OMEGAMON dans le gestionnaire de seuils. A la place, créez les nouvelles situations dans Tivoli Monitoring.

Tous les événements Tivoli Monitoring et OMEGAMON possibles ne sont pas disponibles dans le tableau de bord Evénements. Seuls les événements des noeuds d'agent pouvant être ajoutés à une application sont affichés. Par exemple, pour l'agent Tivoli Monitoring for WebSphere Application Server, les événements associés à une instance de serveur particulière sont affichés mais les événements de l'agent dans son ensemble ne le sont pas.

Affichez jusqu'à 1500 systèmes gérés à partir de chaque domaine Tivoli Monitoring
Le nombre maximal de systèmes gérés, sous-noeuds compris, pouvant s'afficher dans un domaine Tivoli Monitoring est de 1500. Par défaut, la limite est de 200 systèmes. Vous pouvez planifier de prendre en charge une plus grande quantité de systèmes. Pour obtenir des instructions, voir «Planification d'un grand nombre de systèmes gérés», à la page 988.

La limite pour tous les domaines Tivoli Monitoring doit être comprise dans la plage maximale prise en charge par Cloud APM. Pour plus d'informations, voir «Présentation de l'architecture», à la page 45.

Surveillance des ressources uniquement
La surveillance des ressources est disponible pour vos agents Tivoli Monitoring. Pour plus d'informations sur la surveillance des ressources, voir «Offres et modules complémentaires», à la page 47 et «Fonctions», à la page 55. Si vous possédez l'abonnement IBM Cloud Application Performance Management, Advanced, le suivi des transactions et les tableaux de bord de diagnostic ne sont pas disponibles pour les systèmes gérés à partir de votre environnement Tivoli Monitoring.

Tivoli Authorization Policy Server affecte la disponibilité des systèmes gérés par Tivoli Monitoring
Pour les environnements Tivoli Monitoring qui incluent Tivoli Authorization Policy Server, les systèmes gérés disponibles par le biais de la Passerelle hybride sont affectés par les règles d'autorisation. Pour plus d'informations, voir Utilisation des règles d'autorisation par rôle dans Tivoli Monitoring Knowledge Center.

Pour une démonstration vidéo, voir Integrating with Tivoli Monitoring - Passerelle hybride.

Préparation de l'installation de la passerelle hybride

Pour installer la Passerelle hybride d'IBM Cloud Application Performance Management, vous devez d'abord vous assurer que votre environnement est configuré correctement. Examinez les informations pour vous aider à planifier votre installation de la Passerelle hybride.

Où installer la Passerelle hybride

La Passerelle hybride doit être installée sur un système x86-64 Red Hat Enterprise Linux version 6.2 (ou version ultérieure) disposant d'une connexion réseau avec IBM Tivoli Monitoring et IBM Cloud Application Performance Management.

La Passerelle hybride peut être installée sur le même système que Tivoli Enterprise Portal Server ou sur un système distinct de Tivoli Enterprise Portal Server si les systèmes fonctionnent sous Red Hat Enterprise Linux. Toutefois, la Passerelle hybride ne peut pas être installée sur le même système que votre serveur Cloud APM.

Un domaine Tivoli Monitoring comporte un Tivoli Enterprise Monitoring Server concentrateur. Lorsque votre environnement Tivoli Monitoring est constitué de plusieurs domaines, vous pouvez installer la Passerelle hybride dans plusieurs domaines.

Pour la configuration système requise pour la Passerelle hybride, cliquez sur l'onglet **Matériel** dans le Rapport de compatibilité des produits logiciels de la Passerelle hybride.

Configuration du Tivoli Enterprise Portal Server pour la Passerelle hybride

Pour les environnements Tivoli Monitoring où le serveur de portail a une charge lourde, il est recommandé que vous installiez un serveur de portail dédié distinct pour traiter les demandes provenant de la Passerelle hybride. Si vous configurez un serveur de portail distinct :

- Vous pouvez utiliser le même hôte pour le serveur de portail et pour la Passerelle hybride si serveur de portail exécute Red Hat Enterprise Linux.
- Assurez-vous que le serveur de portail distinct dispose du support d'application pour les agents dont les données sont affichées dans la console Cloud APM.
- Assurez-vous que les clients Tivoli Enterprise Portal ne sont pas connectés à un serveur de portail distinct pour effectuer des tâches d'administration telles que la création d'espaces de travail personnalisés, la création de situations et la création de groupes de systèmes gérés.

La version de Tivoli Enterprise Portal Server doit être V6.3 Fix Pack 6 ou supérieure. Si votre serveur de portail est à une version antérieure, les agents Tivoli Monitoring intégrés peuvent ne pas être disponibles pour être ajoutés à une application dans la console Cloud APM.

Le fournisseur de données du tableau de bord IBM Tivoli Monitoring doit être activé sur Tivoli Enterprise Portal Server. Pour plus de détails, voir Verifying the dashboard data provider is enabled dans l'ensemble de rubriques IBM Tivoli Monitoring dans IBM Knowledge Center.

Les ports TCP qui doivent être ouverts sur la Passerelle hybride
Les ports TCP suivants doivent être ouverts sur la Passerelle hybride. Pour chaque port, un côté envoie la demande et l'autre côté fournit une réponse. Le côté qui initie la connexion est indiqué.

- La Passerelle hybride initie une connexion unidirectionnelle avec le serveur Cloud APM sur le port 443 et envoie des demandes HTTPS.

  Si la Passerelle hybride utilise un proxy direct passe-système pour se connecter au serveur Cloud APM, configurez la Passerelle hybride afin que le port du proxy soit utilisé à la place du port 443 pour initier les connexions unidirectionnelles avec le serveur Cloud APM. Pour obtenir des instructions, voir «Utilisation d'un proxy direct pour communiquer avec le serveur Cloud APM», à la page 983.
- Si vous utilisez HTTP pour communiquer avec le serveur de portail, ouvrez le port 15200. Si vous utilisez HTTPS, ouvrez le port 15201. La Passerelle hybride initie une connexion unidirectionnelle avec le serveur de portail sur le port 15200 ou 15201. Pour utiliser un port personnalisé, mettez à jour la valeur du paramètre **Port Portal Server**. Pour plus d'informations, voir «Gestionnaire de Passerelle hybride», à la page 990.

  Si la Passerelle hybride utilise un proxy direct passe-système pour se connecter au serveur de portail, configurez la Passerelle hybride afin que le port du proxy soit utilisé à la place pour les connexions unidirectionnelles qu'il initie avec le serveur de portail. Définissez la valeur du paramètre **Port proxy passe-système**. Pour plus d'informations, voir «Gestionnaire de Passerelle hybride», à la page 990.
- Pour que la Passerelle hybride écoute les événements EIF entrants de Tivoli Enterprise Monitoring Server, ouvrez le port 9998. Le serveur de surveillance initie une connexion unidirectionnelle avec la Passerelle hybride sur le port 9998. La utilitaire d'installation affiche un avertissement si ce port n'est pas ouvert.

Privilèges requis pour exécuter le script d'installation de la Passerelle hybride
Vous devez exécuter le script d'installation de la Passerelle hybride avec les privilèges de superutilisateur. Pour obtenir la liste complète des systèmes d'exploitation pris en charge, visitez le System requirements (APM Developer Center)

Installation de la passerelle hybride
Téléchargez et installez la Passerelle hybride d'IBM Cloud Application Performance Management pour afficher les systèmes gérés à partir de votre domaine IBM Tivoli Monitoring dans la console Cloud APM.

Avant de commencer
Passez en revue et effectuez les tâches de préparation requises dans Préparation de l'installation de la passerelle hybride.

Procédure

Procédez comme suit pour installer la Passerelle hybride dans votre domaine Tivoli Monitoring :

1. Téléchargez le package Passerelle hybride.

   Le fichier `APM_Hybrid_Gateway_Install.tar` contient la Passerelle hybride et le script d'installation.

   a) Connectez-vous à votre compte et accédez à Produits et services sur IBM Marketplace.

   b) Sous **IBM Cloud APM**, cliquez sur **Plus d'actions**.

   c) Cliquez sur **Afficher les packages supplémentaires**.

   d) Sélectionnez **Passerelle hybride**. Si nécessaire, faites défiler vers le bas pour trouver l'entrée.

e) Cliquez sur **Télécharger**.

2. Si nécessaire, transférez le fichier vers le système où s'exécutera la Passerelle hybride.
3. Entrez la commande suivante pour extraire les fichiers :

   ```
   tar -xf APM_Hybrid_Gateway_Install.tar
   ```

   Le fichier d'archive contient un script utilisé pour déployer la Passerelle hybride. Le script d'installation est extrait dans le répertoire et les fichiers de la Passerelle hybride sont extraits dans des sous-répertoires.
4. Accédez au répertoire de la Passerelle hybride et exécutez le script d'installation avec des privilèges de superutilisateur :

   ```
   cd APM_Hybrid_Gateway_Install_version
   ./install.sh
   ```

   où *version* est la version actuelle, par exemple 8.1.4.0.

   L'analyse des prérequis de votre environnement commence et prend un moment. Si des exigences ne sont pas satisfaites, un message vous dirige vers un fichier journal contenant la raison de l'échec. Si un prérequis est manquant (par exemple, espace disque insuffisant), l'installation s'arrête. Vous devez corriger l'incident, et relancer l'installation. Vous pouvez également désactiver le prérequis comme indiqué dans Contournement de l'analyse des prérequis.
5. Une fois que le système a été soumis à l'analyse des prérequis, répondez à l'invite pour accepter le contrat de licence en sélectionnant 1 pour oui.

   Un message vous invite à vous connecter à la console Cloud APM et à configurer la Passerelle hybride avant de continuer. Le nom du profil par défaut, dérivé du nom d'hôte, est affiché également.
6. Appuyez sur Entrée pour accepter le nom par défaut ou entrez un nom de profil.

   Si vous avez déjà créé un profil pour ce domaine Tivoli Monitoring, utilisez le même nom que celui que vous avez fourni dans le Gestionnaire de la Passerelle hybride. Si vous n'avez pas encore créé un profil, vous pouvez accepter le nom par défaut ou fournir un nouveau nom, mais veillez à en conserver la trace car vous devrez le réutiliser pour créer le profil ultérieurement. (Voir «Configuration de la Passerelle hybride à l'aide de la console Cloud APM», à la page 985.)

   Une fois que vous avez appuyé sur la touche Entrée, l'installation de la Passerelle hybride continue.

Résultats

La Passerelle hybride est installée dans le répertoire `/opt/ibm/hybridgateway` et démarre automatiquement. Le fichier journal d'installation se trouve dans `/opt/ibm/hybridgateway/logs/install-hybridgateway-`*`horodatage`*`.log`. Les fichiers journaux de la Passerelle hybride se trouvent dans le répertoire `/opt/ibm/wlp/usr/servers/hybridgateway/logs`. Jusqu'à ce que la connexion à Tivoli Enterprise Portal Server soit configurée, les échecs de connexion sont consignés.

Que faire ensuite

- Vous pouvez configurer la Passerelle hybride de sorte à utiliser un proxy direct pour communiquer avec le serveur Cloud APM. Pour obtenir des instructions, voir «Utilisation d'un proxy direct pour communiquer avec le serveur Cloud APM», à la page 983.
- Vous pouvez vérifier le statut de la Passerelle hybride avec la commande suivante : *`rép_install`*`/hybridgateway/bin/hybridgateway.sh status`. Pour plus d'options, voir «Gestion de la passerelle hybride», à la page 989.
- Si vous n'avez pas encore créé le groupe de systèmes gérés pour la Passerelle hybride, suivez les instructions fournies dans «Création du groupe de systèmes gérés», à la page 983.
- Si vous n'avez pas encore créé un profil de Passerelle hybride pour le domaine Tivoli Monitoring, suivez les instructions dans «Configuration de la Passerelle hybride à l'aide de la console Cloud APM», à la page 985.

- Si votre environnement Tivoli Monitoring comporte un ou plusieurs domaines concentrateur, vous pouvez installer la Passerelle hybride dans d'autres domaines. Répétez les étapes de cette procédure pour installer la Passerelle hybride dans un autre domaine Tivoli Monitoring.

Utilisation d'un proxy direct pour communiquer avec le serveur Cloud APM
Vous pouvez configurer la Passerelle hybride d'IBM Cloud Application Performance Management de sorte à utiliser un proxy direct pour communiquer avec le serveur Cloud APM.

Procédure

1. Sur l'hôte où vous avez installé la Passerelle hybride, éditez le fichier `/opt/ibm/wlp/usr/servers/hybridgateway/bootstrap.properties` :
   - Si la Passerelle hybride utilise le protocole HTTP pour communiquer avec le serveur Cloud APM, ajoutez les lignes suivantes :

     ```
     http.proxyHost=hôte_proxy
     http.proxyPort=hôte_proxy
     ```

   - Si la Passerelle hybride utilise le protocole HTTPS pour communiquer avec le serveur Cloud APM, ajoutez les lignes suivantes :

     ```
     https.proxyHost=hôte_proxy
     https.proxyPort=port_proxy
     ```

   où *hôte_proxy* est le nom d'hôte ou l'adresse IP du proxy, accessible à partir de l'hôte de la Passerelle hybride et *port_proxy* est le port du proxy.
2. Redémarrez l'Passerelle hybride.

Création du groupe de systèmes gérés
Utilisez l'éditeur de groupe d'objet sur le client Tivoli Enterprise Portal pour créer un groupe de systèmes gérés à afficher dans la console Cloud APM.

Avant de commencer

- Les types d'agent IBM Tivoli Monitoring et OMEGAMON que vous pouvez inclure dans le groupe de systèmes gérés doivent faire partie des agents pris en charge. Par exemple, pour Tivoli Monitoring, les agents pris en charge incluent Monitoring Agent for Oracle Database ou Monitoring Agent for Linux OS.

  Pour obtenir la liste actuelle des agents Tivoli Monitoring pris en charge, visitez le Hybrid Gateway supported agents (APM Developer Center). Pour obtenir la liste des agents OMEGAMON que vous pouvez afficher dans la console Cloud APM, consultez la rubrique d'initiation dans l'ensemble de rubriques relatives à IBM OMEGAMON for Application Performance Management dans IBM Knowledge Center.
- Les agents Tivoli Monitoring et OMEGAMON doivent être connectés à la même infrastructure IBM Tivoli Monitoring. Si votre environnement comporte plusieurs domaines Tivoli Monitoring, créez un groupe de systèmes gérés pour chaque Tivoli Enterprise Monitoring Server concentrateur pour lequel une Passerelle hybride est installée.
- Par défaut, vous pouvez ajouter jusqu'à 200 systèmes gérés au groupe de systèmes gérés pour les afficher à partir du domaine Tivoli Monitoring dans le Tableau de bord d'Application Performance. Vous pouvez augmenter la limite jusqu'à 1500 systèmes en effectuant plusieurs étapes de planification. Pour plus d'informations, voir «Planification d'un grand nombre de systèmes gérés», à la page 988. S'il existe plusieurs Passerelles hybrides pour un environnement Tivoli Monitoring comportant plusieurs concentrateurs, le groupe de systèmes gérés pour chaque domaine doit respecter la limite maximale autorisée par Cloud APM. Pour plus d'informations, voir Architecture overview.
- La méthode par défaut de traitement des sous-noeuds a évolué dans l'édition de Cloud APM de mars 2017. Dans les éditions précédentes, si vos agents tels que l'Agent WebSphere Applications comportaient des sous-noeuds, vous deviez affecter le noeud de gestion au groupe de systèmes gérés et tous les sous-noeuds étaient inclus automatiquement. Bien qu'un seul noeud de gestion fût affecté

au groupe de systèmes gérés, les sous-noeuds étaient inclus dans le comptage visant à déterminer le nombre maximal de systèmes gérés.

Dans l'édition Cloud APM de mars 2017 et ultérieure, les sous-noeuds pour lesquels vous souhaitez afficher les données de mesure dans la console Cloud APM doivent être affectés spécifiquement au groupe de systèmes gérés.L'agent de gestion est à présent découvert automatiquement si l'un de ses sous-noeuds est clairement affecté au groupe de systèmes gérés. Pour les applications de surveillance basées sur des sous-noeuds, Cloud APM aura peut-être besoin de demander à l'agent de gestion les informations nécessaires à l'identification précise des ressources de surveillance qui apparaissent dans le navigateur du tableau de bord Cloud APM. C'est pour cette raison qu'avec la version actuelle du mode de reconnaissance, l'agent de gestion est inclus automatiquement et qu'au moins un sous-noeud associé est affecté au groupe de systèmes gérés configuré pour être utilisé par la Passerelle hybride. Le mode de reconnaissance actuel prend en charge le contrôle précis des ressources de sous-noeud pouvant être visualisées dans la console Cloud APM et correspond mieux à la façon dont les applications Cloud APM sont construites, en particulier pour les applications qui impliquent de grands ensembles d'instances de ressource de sous-noeud. Utilisez toujours le mode de reconnaissance par défaut actuel lorsque vous intégrez les agents OMEGAMON à Cloud APM.

Vous pouvez spécifier la version du mode de reconnaissance utilisée par la Passerelle hybride en affectant la valeur appropriée à une propriété externe appelée `MSN_DISCOVERY_MODE`, traitée par la Passerelle hybride au cours de l'initialisation.Pour contrôler le mode de reconnaissance utilisé par la Passerelle hybride, ajoutez la propriété `MSN_DISCOVERY_MODE` (ou modifiez sa valeur actuelle) au fichier de propriétés suivant sur le système où la Passerelle hybride est installée, puis redémarrez la Passerelle hybride.

```
rép_install_PH/wlp/usr/servers/hybridgateway/bootstrap.properties
```

Les valeurs admises pour la propriété `MSN_DISCOVERY_MODE` sont les suivantes :

- `MSN_DISCOVERY_MODE=1` force la Passerelle hybride à utiliser le mode de reconnaissance d'agent initial, où tous les sous-noeuds sont découverts automatiquement pour n'importe quel agent de gestion affecté au groupe de systèmes gérés Tivoli Monitoring.
- `MSN_DISCOVERY_MODE=2` force la Passerelle hybride à utiliser le nouveau mode de reconnaissance d'agent par défaut où seuls les sous-noeuds clairement affectés au groupe de systèmes gérés sont interrogés par la Passerelle hybride. Le ou les agents de gestion associés sont reconnus automatiquement.

- Si vous préférez créer le groupe de systèmes gérés à l'aide des commandes **`tacmd createsystemlist`** et **`tacmd editsystemlist`** IBM Tivoli Monitoring, voir *IBM Tivoli Monitoring Command Reference* (https://www.ibm.com/support/knowledgecenter/SSTFXA_6.3.0/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm) pour obtenir des informations sur la manière d'exécuter les commandes.

Procédure

Pour créer un groupe de systèmes gérés sur le client Tivoli Enterprise Portal, suivez la procédure ci-dessous.

1. Démarrez le client Tivoli Enterprise Portal avec un ID utilisateur et un mot de passe ayant un accès complet à tous les types de systèmes gérés (**Allowed Applications** est défini sur **All Applications** pour l'ID utilisateur.)
2. Cliquez sur **Editeur de groupe d'objets**.
3. Développez l'objet **Système géré** et sélectionnez **Tous les systèmes gérés** pour combiner plusieurs types d'agent (comme Windows et Oracle) dans le groupe de systèmes gérés. Si vous préférez que le groupe de systèmes gérés ne contienne qu'un seul type d'agent de surveillance, tel que système d'exploitation Linux ou applications WebSphere, sélectionnez le type d'agent.
4. Cliquez sur **Créer un groupe** et entrez un nom pour le groupe de systèmes gérés.

   Le nom peut comporter des lettres et des chiffres, sans espace, ponctuation ni caractère spécial autre que le trait de soulignement (_).

Une fois que vous avez cliqué sur **OK**, le nouveau groupe de systèmes gérés s'affiche dans le dossier du système géré.

5. Sélectionnez les systèmes gérés dans la liste **Available Managed Systems** et cliquez sur la pour les déplacer vers la liste **Assigned**.

   Vous pouvez sélectionner plusieurs systèmes gérés en maintenant la touche Ctrl enfoncée tout en cliquant sur chaque système géré pour les sélectionner. Après avoir sélectionné un système géré, vous pouvez utiliser Maj+clic pour sélectionner tous les systèmes gérés entre cette sélection et la première sélection.
6. Après avoir ajouté des systèmes gérés au groupe, cliquez sur **OK** pour sauvegarder vos modifications et fermer l'éditeur de groupe d'objet.

Que faire ensuite

- Après avoir créé le groupe de systèmes gérés et installé la Passerelle hybride, vous devez configurer cette dernière dans la console Cloud APM.
- Pour la configuration, spécifiez le nom du groupe de systèmes gérés que vous avez créé, l'ID utilisateur Tivoli Enterprise Portal autorisé à accéder à tous les types d'agent et le nom d'hôte et port de Tivoli Enterprise Portal Server.
- Pour obtenir les instructions d'installation, voir «Installation de la passerelle hybride», à la page 981.
- Pour obtenir des instructions de configuration, voir «Configuration de la Passerelle hybride à l'aide de la console Cloud APM», à la page 985.

Configuration de la Passerelle hybride à l'aide de la console Cloud APM

Utilisez la page **Gestionnaire de la passerelle hybride** dans la console Cloud APM afin de configurer la Passerelle hybride d'IBM Cloud Application Performance Management pour la connexion à Tivoli Enterprise Portal Server et la spécification du groupe de systèmes gérés.Vous pouvez créer un profil de Passerelle hybride pour chaque Tivoli Enterprise Monitoring Server concentrateur de votre environnement.

Procédure

Procédez comme suit pour configurer la Passerelle hybride dans la console Cloud APM.

1. Le cas échéant, connectez-vous à la console Cloud APM.

   (Voir «Démarrage de la console Cloud APM», à la page 1003.)
2. Cliquez sur **Configuration système** > **Gestionnaire de la Passerelle hybride**.

   La page s'affiche avec un tableau des Passerelles hybrides configurées pour vos domaines Tivoli Monitoring. Si un profil avec un nom vide est affiché, il s'applique à la Passerelle hybride qui a été installée avant l'édition d'août 2017. Pour plus d'informations, voir «Nom de profil», à la page 990.
3. Cliquez sur **Ajouter** pour ouvrir la fenêtre **Add Hybrid Gateway**, entrez un nouveau nom dans la zone **Nom de profil** et cliquez sur **Ajouter**.

   Si vous avez déjà installé la Passerelle hybride dans le domaine Tivoli Monitoring, veillez à utiliser le même nom que celui que vous avez indiqué ou accepté au cours de l'installation de la Passerelle hybride. Le nom du profil indiqué au cours de l'installation et le nom que vous entrez ici doivent être une correspondance exacte.

   La fenêtre **Edit Hybrid Gateway** s'ouvre.
4. Dans la zone **Nom de groupe de systèmes gérés**, entrez le nom du groupe de systèmes gérés de la Passerelle hybride.

   Il s'agit du nom utilisé dans «Création du groupe de systèmes gérés», à la page 983.
5. Indiquez l'adresse, le port et le protocole de communications Web de Tivoli Enterprise Portal Server :

Option	Description
Nom d'hôte Portal Server	Entrez l'adresse IP, le nom d'hôte qualifié complet ou nom de domaine de l'hôte Portal Server.

Option	Description
Port Portal Server	Entrez le numéro de port utilisé par Portal Server pour les communications Web. Le port par défaut est 15200 pour HTTP ou 15201 pour HTTPS. La valeur 0 définit le port 15200 par défaut pour HTTP ou 15201 pour HTTPS.
Protocole Portal Server	Sélectionnez le protocole Internet **HTTP** ou le protocole Internet **HTTPS** sécurisé pour vous connecter à Portal Server.

6. Renseignez les zones **Nom d'utilisateur Portal Server** et **Mot de passe Portal Server** avec le nom d'utilisateur de connexion et le mot de passe correspondant pour démarrer le client Tivoli Enterprise Portal.

   L'ID utilisateur doit avoir accès à tous les types d'agent de surveillance (**Allowed Applications** est défini sur **All Applications**), comme l'ID `sysadmin`. Pour plus d'informations, voir Administrer les utilisateurs dans Tivoli Monitoring IBM Knowledge Center.
7. Si l'accès à Portal Server s'effectue via un serveur proxy, indiquez l'adresse, le port et le protocole Web :

Option	Description
Nom d'hôte proxy passe-système	Entrez l'adresse IP ou le nom qualifié complet du système hôte proxy.
Port proxy passe-système	Entrez le numéro de port du système hôte proxy.
Protocole proxy passe-système	Sélectionnez le protocole utilisé pour les communications via le proxy : HTTP ou HTTPS

Résultats

Une fois que vous cliquez sur **Sauvegarder**, une connexion est établie au service de la Passerelle hybride et les systèmes gérés de votre domaine Tivoli Monitoring sont reconnus. Le groupe de systèmes gérés est interrogé toutes les 5 minutes pour les données de surveillance des ressources.

Que faire ensuite

- Vous devez configurer Tivoli Monitoring pour interagir avec Cloud APM. Pour obtenir des instructions, voir «Configuration de Tivoli Monitoring pour une intégration à Cloud APM», à la page 987.
- Vous pouvez répéter ces étapes pour ajouter un profil pour chaque domaine Tivoli Monitoring à partir duquel vous souhaitez surveiller des systèmes gérés Cloud APM.
- Vous pouvez gérer les profils existants à l'aide des outils **Gestionnaire de la passerelle hybride** :

  Sélectionnez une Passerelle hybride et cliquez sur **Editer** pour ouvrir la fenêtre **Edit Hybrid Gateway**.

  Sélectionnez une Passerelle hybride dont vous ne voulez plus et cliquez sur **Supprimer**. Une fois que vous avez confirmé que vous souhaitiez supprimer la Passerelle hybride, le profil est définitivement supprimé.

  Cliquez sur un en-tête de colonne pour trier le tableau en fonction de cette colonne ; utilisez la combinaison Ctrl + Clic sur une autre colonne pour ajouter un tri secondaire.

  Cliquez à l'intérieur de la zone de texte de filtre et entrez le début de la valeur qui va servir au filtrage. Au fur et à mesure de la saisie, les lignes qui ne répondent pas aux critères sont filtrées. Pour effacer le filtre, cliquez sur × dans la zone de filtre ou appuyez sur la touche Retour arrière.

Configuration de Tivoli Monitoring pour une intégration à Cloud APM

Pour intégrer votre domaine IBM Tivoli Monitoring à Cloud APM, vous devez exécuter des tâches comme la configuration de Tivoli Enterprise Portal Server et du concentrateur Tivoli Enterprise Monitoring Server.

Procédure

Pour chaque domaine Tivoli Monitoring sur lequel une Passerelle hybride est installée, suivez la procédure ci-dessous :

1. Configurez Tivoli Enterprise Portal Server pour activer le fournisseur de données du tableau de bord.

   Le fournisseur de données doit intégrer Cloud APM à la Passerelle hybride. Pour connaître les instructions, consultez les rubriques suivantes :

   - Windows Windows : Installation du serveur de portail (étape 16c).
   - Linux AIX Configuration du serveur de portail sous Linux ou AIX : procédure de ligne de commande (étape 14).

   Si vous utilisez la fonction de secours automatique, vous devez spécifier une substitution de domaine. La Passerelle hybride utilise le nom de domaine pour collecter les données provenant des deux serveurs de surveillance concentrateurs, quel que soit le concentrateur auquel le serveur de portail est connecté.
2. Si vous souhaitez afficher les événements de situation des agents Tivoli Monitoring dans la console Cloud APM, configurez le serveur de surveillance concentrateur pour l'un des scénarios suivants :

   - Pour envoyer des événements à la Passerelle hybride uniquement.
   - Pour envoyer des événements à la Passerelle hybride et à des récepteurs EIF supplémentaires, tels que des serveurs Netcool/OMNIbus.

   Exécutez l'une des étapes suivantes en fonction de votre scénario applicable.

   a) Pour configurer le Tivoli Enterprise Monitoring Server concentrateur pour qu'il envoie les événements à la Passerelle hybride uniquement, suivez les étapes décrites dans la rubrique Configuring the hub monitoring server to forward events.

   Indiquez le numéro de port 9998 pour le paramètre **`ServerPort`**.
   Cloud APM ne transmet pas les événements Tivoli Monitoring à Netcool/OMNIbus. Si vous souhaitez afficher les événements Tivoli Monitoring dans Cloud APM et dans Netcool/OMNIbus, vous devez configurer Tivoli Monitoring pour envoyer les événements aux deux systèmes.

   b) Pour configurer le Tivoli Enterprise Monitoring Server concentrateur pour qu'il envoie les événements à la Passerelle hybride et à un autre récepteur EIF, tel qu'un serveur Netcool/OMNIbus, configurez le récepteur EIF par défaut en suivant les étapes décrites dans la rubrique Configuration du serveur de surveillance concentrateur pour le transfert d'événements.

   La rubrique fournit également des informations sur la création de destinations EIF supplémentaires à l'aide de la commande **`tacmd createEventDest`**. Indiquez le port 9998 en tant que numéro de port EIF pour la destination de la Passerelle hybride.

   c) Configurez toutes les situations qui existent pour les agents du groupe de systèmes gérés de la Passerelle hybride pour vous assurer que les événements de situation sont envoyés à la destination EIF pour la Passerelle hybride. Pour obtenir des instructions, voir la rubrique Spécification des situations qui transmettent des événements Netcool/OMNIbus.

Que faire ensuite

Consultez Tableau de bord d'Application Performance pour confirmer que les systèmes gérés issus du domaine Tivoli Monitoring sont transmis via la Passerelle hybride :

1. Cliquez sur **Performance** > **Tableau de bord d'Application Performance** pour ouvrir le tableau de bord **Toutes mes applications**.
2. Dans la zone récapitulative de "Mes composants", cliquez sur **Composants** pour ouvrir le tableau de bord récapitulatif de statut de tous les systèmes gérés de composant (à l'exception de l'Agent

WebSphere Applications). Si vous ne possédez pas d'application "Mes composants", ajoutez une application, comme décrit dans «Gestion des applications», à la page 1129.

3. Recherchez les systèmes gérés issus du domaine Tivoli Monitoring, indiqués par une icône de domaine **ITM** (IBM Tivoli Monitoring) dans le titre du widget de groupe Récapitulatif du statut. Si des systèmes gérés sont manquants, accédez au forum Cloud Application Performance Management et effectuez une recherche sur "Passerelle hybride".

Vous pouvez créer des applications avec des systèmes gérés provenant des domaines Tivoli Monitoring et inclure des systèmes gérés à partir de votre domaine Cloud APM. Pour plus d'informations, voir «Gestion des applications», à la page 1129.

Planification d'un grand nombre de systèmes gérés

Le nombre maximal de systèmes gérés que vous pouvez voir à partir de votre domaine IBM Tivoli Monitoring est de 1500. Si vous incluez un agent qui a des sous-noeuds dans le groupe de systèmes gérés que vous avez créé pour le profil de Passerelle hybride, tous les sous-noeuds, ainsi que l'agent, sont pris en compte dans la limite. Par défaut, cette limite est de 200 systèmes gérés, mais vous pouvez effectuer un certain nombre d'étapes de planification pour l'étendre.La limite pour tous les domaines Tivoli Monitoring doit être comprise dans la plage maximale prise en charge par Cloud APM. Pour plus d'informations, voir «Présentation de l'architecture», à la page 45.

- Définissez la valeur de la variable d'environnement Tivoli Enterprise Portal Server **KFW_REPORT_NODE_LIMIT** sur un nombre supérieur ou égal au nombre de systèmes gérés pour la Passerelle hybride. La valeur par défaut est 200. Pour plus d'informations, voir Paramètres de configuration de Tivoli Enterprise Portal Server.
  Si le nombre de systèmes gérés dépasse cette valeur, le journal des messages de Tivoli Enterprise Portal Server `KfwServices` affiche un message similaire au suivant :
  `56C6246F.0000-10:ctreportmanager.cpp,2864,"CTReport::Manager::executeDefinitionDual") Query is targeting 1497 nodes which exceeds the current limit of 200 nodes.`
- Si vous visualisez un grand nombre de systèmes, les performances peuvent se dégrader en fonction du type d'agents, du temps d'attente des réseaux entre la Passerelle hybride et les systèmes gérés, et de la taille de l'environnement surveillé par chaque agent (quantité de données collectées et affichées). Pour éviter cet effet, sélectionnez uniquement les agents qui fournissent les données nécessaires et assurent une connectivité réseau rapide entre les systèmes surveillés et l'hôte de Passerelle hybride.
- A mesure que le temps d'attente des réseaux augmente, la durée de collecte des données d'un nombre spécifique d'agents augmente. La Passerelle hybride essaye de regrouper des données de chaque agent toutes les 5 minutes. Si la durée de collecte des données de tous les agents dépasse 5 minutes, la Passerelle hybride manque des échantillons de données, et par conséquent, les métriques ne sont pas disponibles sur les pages du Tableau de bord d'Application Performance.
- Pour compenser les vitesses réseau très lentes, vous pouvez essayer d'augmenter le nombre d'unités d'exécution utilisées par la Passerelle hybride pour recueillir des échantillons de données. Le paramètre **MAX_COLLECTOR_THREADS** du fichier `bootstrap.properties` de la Passerelle hybride contrôle le nombre d'unités d'exécution. La valeur par défaut est 50.

Désinstallation de la passerelle hybride

Si vous ne voulez plus afficher les systèmes gérés IBM Tivoli Monitoring dans la console Cloud APM, désinstallez la Passerelle hybride d'IBM Cloud Application Performance Management.

Procédure

1. Dans le répertoire *rép_install*`/hybridgateway/bin` de la Passerelle hybride (comme `/opt/ibm/hybridgateway/bin`), exécutez la commande suivante :

   ```
   ./hybridgateway.sh uninstall
   ```

   La Passerelle hybride est supprimée et un message confirme qu'elle a été désinstallée avec succès. S'il existe des applications dans la console Cloud APM qui incluent des agents hybrides, ces derniers continuent à apparaître jusqu'à ce que l'infrastructure de surveillance traite leur suppression.

2. Dans la console Cloud APM, cliquez sur **Configuration du système** > **Gestionnaire de la Passerelle hybride**.
3. Sélectionnez le profil de la Passerelle hybride dont vous ne voulez plus et cliquez sur **Supprimer**.

   Une fois que vous avez confirmé que vous souhaitiez supprimer la Passerelle hybride, le profil est définitivement supprimé.

Que faire ensuite

- Pour supprimer des systèmes gérés d'agent hybride d'une application dans la console Cloud APM, suivez les instructions décrites dans «Gestion des applications», à la page 1129 pour modifier une application.
- Si au lieu d'avoir confirmation du succès de la suppression du logiciel, vous obtenez un message d'erreur similaire à celui présenté dans cet exemple, consultez le fichier journal pour en connaître les causes possibles :

```
error: Failed dependencies:
ibm-java-x86_64-jre is needed by (installed) smai-kafka-00.08.00.00-1.el6.x86_64
La désinstallation a échoué. Le programme de désinstallation n'est pas parvenu à
supprimer certains composants. Consultez le
 fichier journal
("/tmp/hybridgateway/logs/uninstall-hybridgateway-20150228080551.log") pour plus d'informations.
```

  L'erreur indiquée dans l'exemple s'est produite car ibm-java-x86_64-jre est requis par le package installé en externe sur le système. Le programme d'installation ne supprime pas le JRE car cela rendrait l'autre package inopérant. La solution consiste à désinstaller les produits dépendant d'ibm-java-x86-64-jre avant de désinstaller la Passerelle hybride.

Gestion de la passerelle hybride

Utilisez les commandes disponibles pour la Passerelle hybride d'IBM Cloud Application Performance Management afin de démarrer ou d'arrêter la Passerelle hybride, de vérifier son statut, de la désinstaller et d'en collecter les fichiers journaux si vous y êtes invité par le support IBM.

Pourquoi et quand exécuter cette tâche

Ces étapes considèrent que le répertoire d'installation de la Passerelle hybride est `/opt/ibm/`. Sur le système où la Passerelle hybride est installée, suivez l'une des étapes suivantes à partir de l'invite de commande :

Procédure

- Pour démarrer le service de la Passerelle hybride, entrez **/opt/ibm/hybridgateway/bin/hybridgateway.sh start**.
- Pour arrêter le service de la Passerelle hybride, entrez **/opt/ibm/hybridgateway/bin/hybridgateway.sh stop**.
- Pour vérifier le statut du service de la Passerelle hybride, entrez **/opt/ibm/hybridgateway/bin/hybridgateway.sh status**.
- Pour désinstaller la Passerelle hybride, entrez **/opt/ibm/hybridgateway/bin/hybridgateway.sh uninstall**.

  Voir aussi «Désinstallation de la passerelle hybride», à la page 988.
- Pour consulter les fichiers journaux de la Passerelle hybride, accédez à `/opt/ibm/wlp/usr/servers/hybridgateway/logs`.
- Pour collecter les fichiers journaux de la Passerelle hybride pour le support IBM, entrez **/opt/ibm/hybridgateway/collectLogs.sh**.

  Les fichiers journaux sont collectés et un message affiche l'emplacement des fichiers journaux compressés et vous demande de les retourner au support IBM.

Gestionnaire de Passerelle hybride
Configurez la Passerelle hybride d'IBM Cloud Application Performance Management de sorte qu'elle affiche les données de surveillance de votre domaine IBM Tivoli Monitoring dans la console Cloud APM. Vous pouvez créer un profil de Passerelle hybride pour chaque Tivoli Enterprise Monitoring Server concentrateur de votre environnement.

Une fois que vous avez cliqué sur **Configuration du système** > **Gestionnaire de Passerelle hybride**, la page qui s'affiche comporte une liste des Passerelles hybrides définies.

La page comporte un tableau de toutes les passerelles hybrides configurées pour vos domaines Tivoli Monitoring et contient les outils permettant de gérer les profils de Passerelle hybride :

- **Ajouter** permet d'ouvrir la fenêtre **Ajouter une passerelle hybride** pour affecter un nom au nouveau profil. Une fois que vous avez entré un nom et cliqué sur **Ajouter**, la fenêtre **Editer la passerelle hybride** s'ouvre.
- Sélectionnez une passerelle hybride et cliquez sur **Editer** pour ouvrir la fenêtre **Editer la passerelle hybride**.
- Sélectionnez une passerelle hybride dont vous ne voulez plus et cliquez sur **Supprimer**. Une fois que vous avez confirmé que vous souhaitiez supprimer la passerelle hybride, le profil est définitivement supprimé.
- Cliquez sur un en-tête de colonne pour trier le tableau en fonction de cette colonne ; utilisez la combinaison Ctrl + Clic sur une autre colonne pour ajouter un tri secondaire.
- Cliquez à l'intérieur de la zone de texte de filtre et entrez le début de la valeur qui va servir au filtrage. Au fur et à mesure de la saisie, les lignes qui ne répondent pas aux critères sont filtrées. Pour effacer le filtre, cliquez sur dans la zone de filtre ou appuyez sur la touche Retour arrière.

Les zones obligatoires que vous devez renseigner pour configurer la Passerelle hybride sont marquées d'un astérisque (*) dans la fenêtre **Editer la passerelle hybride**.

Nom de profil
Nom attribué à un profil de Passerelle hybride pouvant comporter jusqu'à 128 lettres, chiffres et caractères de soulignement (_).

Le nom de profil est demandé au cours de l'installation de la Passerelle hybride. Si vous avez déjà installé la Passerelle hybride dans le domaine Tivoli Monitoring, utilisez le nom que vous avez indiqué ou accepté au cours de l'installation de la Passerelle hybride.

Les versions plus anciennes de la Passerelle hybride n'utilisent pas un profil nommé pour accéder à leurs données de configuration. Si vous avez installé la Passerelle hybride avant l'édition Cloud APM l'édition d'août 2017, vous disposez d'un nom de profil spécial sans nom (vide). Une seule version plus ancienne de la Passerelle hybride est autorisée à se connecter au serveur Cloud APM. Si vous avez configuré l'ancienne version de la Passerelle hybride, le profil sans nom affiche les valeurs configurées. Dans le cas contraire, le profil sans nom affiche les valeurs par défaut. Vous pouvez conserver le profil sans nom ou le supprimer puis l'ajouter à nouveau ultérieurement le cas échéant. Il peut être utilisé uniquement pour l'édition de mars 2017 (ou antérieure) de la Passerelle hybride.

Nom de groupe de système géré
Nom du groupe de système géré Tivoli Enterprise Portal Server que vous avez créé pour afficher les agents de surveillance pris en charge dans la console Cloud APM. Tous les types d'agent de surveillance non pris en charge par votre offre Cloud APM n'apparaissent pas dans la console quelle que soit leur inclusion dans le groupe de systèmes gérés.
Pour connaître les instructions et les limitations relatives à la création du groupe de système géré pour l'activation hybride, voir .

Nom d'hôte du serveur de portail
Adresse IP ou nom de domaine complet de l'hôte Tivoli Enterprise Portal Server.

Port Portal Server
Numéro de port utilisé par Tivoli Enterprise Portal Server pour les communications. Le port par défaut est `15200` pour HTTP ou `15201` pour HTTPS. La valeur 0 définit le port `15200` par défaut pour HTTP ou `15201` pour HTTPS.

Protocole Portal Server
Détermine si le protocole HTTP Internet ou le protocole HTTPS sécurisé doit être utilisé pour se connecter à Tivoli Enterprise Portal Server. Valeur par défaut : `http`.

Nom d'utilisateur Portal Server
Nom d'utilisateur pour démarrer le client Tivoli Enterprise Portal. Cet ID utilisateur doit avoir accès à tous les types d'agent de surveillance (**Allowed Applications** est défini sur **All Applications**). Pour plus d'informations, voir Administrer les utilisateurs dans Tivoli Monitoring Knowledge Center.)

Mot de passe utilisateur Portal Server
Mot de passe associé au nom d'utilisateur de la connexion à Tivoli Enterprise Portal.

Nom d'hôte proxy passe-système
Utilisé si Tivoli Enterprise Portal Server communique via un serveur proxy passe-système. Entrez l'adresse IP ou le nom qualifié complet du système hôte proxy.

Port proxy passe-système
Utilisé si Tivoli Enterprise Portal Server communique via un serveur proxy passe-système. Entrez le numéro de port pour la communication avec le proxy.

Protocole proxy passe-système
Utilisé si Tivoli Enterprise Portal Server communique via un serveur proxy passe-système. Entrez le protocole utilisé pour les communications via le proxy. Valeur par défaut : `http`.

Les agents Tivoli Monitoring que vous affichez dans la console Cloud APM se trouvent dans votre environnement IBM Tivoli Monitoring. Vous pouvez les afficher dans les pages Tableau de bord d'Application Performance, mais vous ne pouvez pas créer de seuils pour ces agents dans le **Gestionnaire de seuils**.

Intégration à OMEGAMON

Vous pouvez afficher les données et les événements de vos composants d'application OMEGAMON dans la console Cloud APM en achetant z Systems Extension Pack et en utilisant la Passerelle hybride pour connecter ou plusieurs agents OMEGAMON déployés à Cloud APM.

Avant de commencer

- Pour utiliser z Systems Extension Pack, vous devez disposer de l'offre IBM Cloud Application Performance Management, Advanced ou de l'offre IBM Cloud Application Performance Management, Base.
- Un ou plusieurs agents sous licence OMEGAMON doivent s'exécuter sur les partitions logiques z Systems en cours de surveillance.
- Les agents OMEGAMON sont connectés à l'infrastructure IBM Tivoli Monitoring.

Pour obtenir la liste des agents OMEGAMON que vous pouvez afficher dans la console Cloud APM, consultez la rubrique d'initiation correspondant à votre édition dans l'ensemble de rubriques relatives à IBM OMEGAMON for Application Performance Management dans IBM Knowledge Center.

Procédure

Pour intégrer OMEGAMON à Cloud APM, procédez comme suit :

1. Une fois que z Systems Extension Pack est ajouté à votre produit Cloud APM, effectuez les tâches de Passerelle hybride suivantes :
   a) Installez l'Passerelle hybride.
   b) Créez le groupe de systèmes gérés que vous voulez afficher dans la console Cloud APM.

c) Configurez la Passerelle hybride dans la console Cloud APM de sorte à pouvoir connecter la Passerelle hybride à Tivoli Enterprise Portal Server et spécifiez un groupe de systèmes gérés.

Pour plus d'informations, voir les rubriques associées à la section «Passerelle hybride», à la page 979.

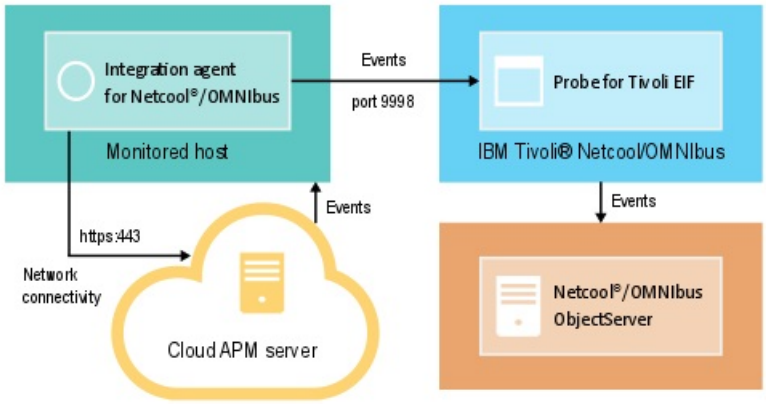
2. Pour afficher le statut de vos applications dans le tableau de bord, connectez-vous à la console Cloud APM à partir de votre navigateur. Pour plus d'informations, voir «Démarrage de la console Cloud APM», à la page 1003.

Intégration à Netcool/OMNIbus

Vous pouvez réacheminer les événements de IBM Cloud Application Performance Management vers votre gestionnaire d'événements IBM Tivoli Netcool/OMNIbus sur site.

Procédure

1. Pour visualiser l'Agent d'intégration pour Netcool/OMNIbus et la manière dont il s'intègre à Cloud APM avec Probe for Tivoli EIF pour acheminer les événements à Netcool/OMNIbus, voir la configuration



suivante :

L'Agent d'intégration pour Netcool/OMNIbus se connecte automatiquement au serveur Cloud APM. Cette connectivité permet aux événements de circuler du serveur sur le réseau sans connexion réseau entrante.

2. Configurez l'intégration pour Netcool/OMNIbus.

Installation et configuration de l'agent d'intégration pour Netcool/OMNIbus

Pour installer l'Agent d'intégration pour Netcool/OMNIbus, vous devez télécharger un fichier archive à partir du site Web IBM Marketplace, extraire les fichiers d'installation d'agent, puis redémarrer le script d'installation. Après l'installation, l'agent démarre automatiquement mais il doit être configuré.

Pourquoi et quand exécuter cette tâche

Une seule instance de l'Agent d'intégration pour Netcool/OMNIbus à la fois peut réacheminer les événements à partir d'une instance unique d'un abonnement au service Cloud APM vers le gestionnaire d'événements Netcool/OMNIbus.

Procédure

1. Téléchargez le fichier d'archive de Cloud APM Integration qui inclut l'Agent d'intégration pour Netcool/OMNIbus :
   a) Connectez-vous à votre compte et accédez à Produits et services sur IBM Marketplace.
   b) Sous **IBM Performance Management**, cliquez sur **Plus d'actions**.
   c) Cliquez sur **Afficher les packages supplémentaires**.

d) Sélectionnez **IBM Performance Management OMNIbus Integration on Cloud**. Si nécessaire, faites défiler vers le bas pour trouver cet élément.

e) Cliquez sur **Télécharger**.

2. Enregistrez le fichier dans le répertoire de transfert de votre choix. Installez l'agent sur n'importe quel système ayant une connectivité réseau à la sonde Tivoli Netcool/OMNIbus Probe for Tivoli Event Integration Facility (EIF). Si nécessaire, transférez le fichier archive d'installation sur les systèmes à surveiller. Le fichier archive contient l'agent et le script d'installation.
3. Procédez à l'extraction du fichier d'installation :

   Linux

   a. Ouvrez une session shell de terminal sur le système Red Hat Enterprise Linux.

   b. Accédez au répertoire dans lequel se trouve le fichier archive.

   c. Procédez à l'extraction des fichiers d'installation à l'aide de la commande suivante :

   ```
   tar -xf ./apm_integration_agents_xlinux_8.1.4.0.tar
   ```

   Windows

   Extrayez le fichier `apm_integration_agents_win_8.1.4.0.zip`.

   Le script d'installation est extrait dans un répertoire nommé en fonction du fichier archive et de la version. Par exemple, `IPM_Agent_Install_8.1.3.2`. Les fichiers binaires de l'agent et les fichiers liés à la configuration sont extraits dans des sous-répertoires de ce répertoire.
4. Exécutez le script d'installation avec des privilèges d'administrateur à partir du répertoire nommé en fonction du fichier archive et de la version.

   Si vous installez l'Agent d'intégration pour Netcool/OMNIbus sur le même système que votre sonde Probe for Tivoli EIF et que cette dernière utilise 9998 comme port par défaut, l'Agent d'intégration pour Netcool/OMNIbus est automatiquement configuré pour se connecter à cette sonde.

   Important : Si vous installez l'Agent d'intégration pour Netcool/OMNIbus sur un autre système que celui sur lequel se trouve votre sonde Probe for Tivoli EIF ou si vous utilisez un numéro de port autre que celui par défaut pour la sonde Probe for Tivoli EIF, vous devez configurer l'Agent d'intégration pour Netcool/OMNIbus une fois l'installation terminée.

   Pour installer l'agent, procédez comme suit :

   Linux `installAPMAgents.sh`

   Windows `installAPMAgents.bat`

   Vous êtes invité à installer l'Agent d'intégration pour Netcool/OMNIbus.

   L'analyse des prérequis de votre environnement commence et prend un moment. Si des exigences ne sont pas satisfaites, un message vous dirige vers un fichier journal contenant la raison de l'échec. Si un prérequis est manquant (par exemple, bibliothèque manquante ou espace disque insuffisant), l'installation s'arrête. Vous devez corriger l'incident, et relancer l'installation.

   L'agent est configuré avec les paramètres par défaut suivants :

   ```
   Tivoli EIF Probe Host : localhost
   Tivoli EIF Probe Port : 9998
   ```

   Après l'installation, l'Agent d'intégration pour Netcool/OMNIbus démarre automatiquement.

   L'agent de surveillance est installé dans le répertoire que vous spécifiez (*rép_install*). Les répertoires par défaut suivants sont utilisés :

   Linux `/opt/ibm/apm/agent`

   Windows `C:\IBM\APM\`
5. Si vous installez l'Agent d'intégration pour Netcool/OMNIbus sur un autre système que celui sur lequel se trouve votre sonde Probe for Tivoli EIF, ou si cette dernière utilise un numéro de port différent du

port par défaut de 9998, l'Agent d'intégration pour Netcool/OMNIbus doit être configuré pour se connecter à votre sonde Probe for Tivoli EIF.

Remarque : Si vous avez installé l'Agent d'intégration pour Netcool/OMNIbus sur le même système que votre sonde Probe for Tivoli EIF et que cette dernière utilise 9998 comme port par défaut, vous n'avez pas besoin d'effectuer cette étape.

Linux Pour configurer l'agent, procédez comme suit :

a. Exécutez la commande suivante :

```
rép_install/bin/omnibus-agent.sh config
```

b. Lorsque vous y êtes invité, indiquez votre nom d'hôte et numéro de port de sonde Probe for Tivoli EIF.

Une fois la configuration terminée, l'Agent d'intégration pour Netcool/OMNIbus démarre automatiquement.

Linux Vous pouvez également suivre la procédure décrite ci-après pour réviser et modifier vos paramètres de configuration.

a. Ouvrez le fichier de réponses *rép_install*/samples/omnibus_silent_config.txt dans un éditeur de texte.
b. Editez le fichier pour définir ou modifier vos paramètres de configuration. Prenez soin de supprimer la mise en commentaire des lignes de configuration.
c. Sauvegardez et fermez le fichier de réponses.
d. Reconfigurez l'agent. Exécutez la commande suivante en spécifiant le chemin d'accès qualifié complet au fichier de configuration que vous avez édité :

```
rép_install/bin/omnibus-agent.sh config rép_install/samples/omnibus_silent_config.txt
```

e. Redémarrez l'agent de manière à implémenter vos modifications :

```
rép_install/bin/omnibus-agent.sh stop
rép_install/bin/omnibus-agent.sh start
```

Windows Pour configurer l'agent, procédez comme suit :

a. Ouvrez le fichier de réponses *rép_install*\samples\omnibus_silent_config.txt dans un éditeur de texte.
b. Editez le fichier pour indiquer votre nom d'hôte et numéro de port de sonde Probe for Tivoli EIF. Prenez soin de supprimer la mise en commentaire des lignes de configuration.
c. Sauvegardez et fermez le fichier de réponses.
d. Reconfigurez l'agent en spécifiant le chemin d'accès complet au fichier de configuration en mode silencieux que vous avez édité :

```
rép_install\BIN\omnibus-agent.bat config rép_install\samples\omnibus_silent_config.txt
```

e. Redémarrez l'agent de manière à implémenter vos modifications :

```
rép_install\BIN\omnibus-agent.bat stop
rép_install\BIN\omnibus-agent.bat start
```

Que faire ensuite

Suivez les instructions de la rubrique Configuration de l'intégration pour Netcool/OMNIbus.

Si vous souhaitez arrêter d'utiliser Agent d'intégration pour Netcool/OMNIbus ou que vous voulez déplacer l'agent vers un autre système, désinstallez l'agent à l'aide de la commande suivante :

Linux *rép_install*/bin/omnibus-agent.sh uninstall

Windows *rép_install*\BIN\omnibus-agent.bat uninstall

Configuration de l'intégration pour Netcool/OMNIbus

Après avoir installé l'Agent d'intégration pour Netcool/OMNIbus , vous devez copier les règles d'événement vers Probe for Tivoli EIF et les modifier. Vous devez également mettre à jour Netcool/OMNIbus ObjectServer et le schéma de base de données.

Avant de commencer

Avant d'effectuer les étapes d'intégration, arrêtez l'Agent d'intégration pour Netcool/OMNIbus à l'aide des commandes suivantes :

Linux *rép_install*/bin/omnibus-agent.sh stop

Windows *rép_install*\BIN\omnibus-agent.bat stop

rép_install représente le répertoire /opt/IBM/apm/agent ou C:\IBM\APM par défaut, ou le répertoire que vous avez spécifié lors de l'installation de l'Agent d'intégration pour Netcool/OMNIbus.

Pourquoi et quand exécuter cette tâche

Après l'installation de l'Agent d'intégration pour Netcool/OMNIbus, les fichiers de configuration suivants se trouvent dans les répertoires *rép_install*/localconfig/i0/omnibus et *rép_install*\localconfig\i0\omnibus :

- itm_apm_db_update.sql
- itm_event.rules
- itm_apm_event.rules

où *rép_install* représente le répertoire /opt/IBM/apm/agent ou C:\IBM\APM par défaut, ou le répertoire que vous avez spécifié lors de l'installation de l'Agent d'intégration pour Netcool/OMNIbus.

Important : Procédez comme suit même si vos serveurs d'objets Probe for Tivoli EIF et Netcool/OMNIbus sont déjà intégrés à IBM Tivoli Monitoring, à Probe for Tivoli EIF, à IBM SmartCloud Monitoring - Application Insight, à IBM SmartCloud Application Performance Management ou à une version précédente de Cloud APM.

Procédure

Dans cette procédure, lorsque vous suivez les liens vers la documentation d'IBM Tivoli Monitoring, exécutez uniquement les étapes fournies sur la page liée.

1. Copiez les fichiers Agent d'intégration pour Netcool/OMNIbus itm_event.rules et itm_apm_event.rules dans le répertoire d'installation de Probe for Tivoli EIF.

   Les répertoires par défaut sont les suivants :

   Linux *rép_install*/tivoli/netcool/omnibus/probes/linux2x86

   Windows *rép_install*\Tivoli\Netcool\omnibus\probes\win32

   Où *rép_install* représente le répertoire par défaut.
2. Ouvrez le fichier Probe for Tivoli EIF tivoli_eif.rules dans un éditeur de texte et effectuez l'une des étapes suivantes :
   - Si vous êtes un client IBM Tivoli Monitoring existant et que vous avez déjà terminé l'intégration d'OMNIbus, ajoutez cette ligne à votre fichier itm_event.rules : include "itm_apm_event.rules".
   - Si vous n'avez pas encore configuré l'intégration d'OMNIbus, déplacez le commentaire de la ligne qui fait référence au fichier itm_event.rules.

   Pour connaître les étapes détaillées, voir Mises à jour des fichiers de règles de la sonde EIF dans la documentation d'IBM Tivoli Monitoring.

3. Si vous utilisez une solution OMNIbus multiniveau, exécutez toutes les tâches décrites dans la section Mise à jour de l'ObjectServer Netcool/OMNIbus avec des attributs, des tables et des déclencheurs IBM Tivoli Monitoring de la documentation IBM Tivoli Monitoring.
4. Mettez à jour le schéma de base de données Netcool/OMNIbus ObjectServer en chargeant le fichier `itm_apm_db_update.sql` dans la base de données :

   Linux

   ```
   $OMNIHOME/bin/nco_sql -user nom_utilisateur -password mot_de_passe
   -server nom_serveur < itm_apm_db_update.sql
   ```

   Exemple :

   ```
   $OMNIHOME/bin/nco_sql -user smadmin -password passw0rd -server NCOMS <
   /tmp/apm/itm_apm_db_update.sql
   ```

   Windows

   ```
   itm_apm_db_update.sql | %OMNIHOME%\..\bin\isql -U nom_utilisateur
   -P mot_de_passe -S nom_serveur
   ```

   Exemple :

   ```
   \temp\apm\itm_apm_db_update.sql | %OMNIHOME%\..\bin\isql -U smadmin
   -P passw0rd -S NCOMS
   ```

   Les messages d'erreur suivants peuvent s'afficher lors de l'exécution des scripts (ces messages sont inoffensifs) :

   - `Object exists` et `Attempt to insert duplicate row`, si les scripts ont été exécutés précédemment (par exemple, pour l'intégration à une version antérieure de Cloud APM ou à Tivoli Monitoring).
   - `ERROR=Object not found on line 4 of statement "-- A workspace table for the ITM event clear automation..."` sur ou près d'`itm_event_clear`.
   - `ERROR=Object not found on line 1 of statement "delete from alerts.itm_problem_events;..."` sur ou près d'`itm_problem_events`.
   - `ERROR=Object not found on line 1 of statement "drop table alerts.itm_problem_events;..."` sur ou près d'`itm_problem_events`.
5. Répétez l'étape 5 de sorte que le fichier soit chargé sur le serveur d'objets deux fois afin de garantir que toutes les dépendances soient correctement chargées.
6. Démarrez (ou redémarrez) Probe for Tivoli EIF.
7. Redémarrez l'Agent d'intégration pour Netcool/OMNIbus en utilisant les commandes suivantes :

   Linux *rép_install*`/bin/omnibus-agent.sh start`

   Windows *rép_install*`\BIN\omnibus-agent.bat start`

Intégration à Operations Analytics - Log Analysis

Si votre environnement inclut IBM Operations Analytics - Log Analysis, vous pouvez l'intégrer pour permettre les recherches dans les journaux d'application de la console Cloud APM.

Pourquoi et quand exécuter cette tâche

L'intégration à votre application Log Analysis installée implique de configurer le serveur Cloud APM avec l'adresse URL. Pour plus d'informations sur Log Analysis, voir IBM Operations Analytics - Developers Community.

Vous devez fournir l'URL de niveau supérieur pour votre installation de Log Analysis, par exemple :

```
https://loganalysis.example.com:9987/Unity
```

L'URL de Log Analysis doit être accessible à partir des hôtes sur lesquels les utilisateurs utilisent la console Cloud APM. Il n'est pas nécessaire de la rendre accessible à partir de l'Internet public.

Procédure

1. Dans la console Cloud APM, cliquez sur **Configuration du système** > **Configuration avancée**.
2. Sélectionnez la catégorie **Intégration de l'interface utilisateur**.
3. Dans la zone **URL d'analyse de journal**, entrez l'URL utilisée pour lancer votre application Log Analysis.

Résultats
L'application Log Analysis est intégrée et la fonction de recherche dans les journaux d'application à partir du Tableau de bord d'Application Performance est activée.

Remarque :

La connexion unique n'est pas prise en charge de la console Cloud APM vers l'application Log Analysis.

Que faire ensuite
Sélectionnez **Performance** > **Tableau de bord d'Application Performance** . Vous pouvez éventuellement sélectionner une application, puis utilisez la zone de recherche pour rechercher des fichiers journaux. Par défaut, les entrées sont recherchées sur la dernière heure, mais vous pouvez modifier cette plage de temps. Si vous sélectionnez une application, seuls les journaux sur les serveurs associés à cette application sont recherchés. Pour plus d'informations, voir «Recherche dans les fichiers journaux», à la page 1111.

Intégration à Operations Analytics - Predictive Insights

Lorsque vous intégrez IBM Cloud Application Performance Management à Operations Analytics - Predictive Insights, Operations Analytics - Predictive Insights analyse les données de mesure collectées par Cloud APM et génère des alarmes lorsqu'il identifie des anomalies dans les données.

Les anomalies sont affichées sous forme d'événements dans le tableau de bord de Cloud APM, comme décrit dans «Recherche d'anomalies à l'aide d'Operations Analytics - Predictive Insights», à la page 1143. Vous pouvez ensuite effectuer une exploration en aval dans l'interface utilisateur d'Operations Analytics - Predictive Insights pour afficher plus de détails sur une anomalie.

Lorsque vous ajoutezOperations Analytics - Predictive Insights à un abonnement Cloud APM, il est automatiquement configuré pour collecter et analyser les mesures de performances. Aucune autre configuration n'est requise. Pour ajouter Operations Analytics - Predictive Insights à un abonnement Cloud APM, accédez à IBM Support et ouvrez une demande de service.

Vous pouvez intégrer les agents Cloud APM suivants à Operations Analytics - Predictive Insights:

- Monitoring Agent for Db2
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for JBoss
- Monitoring Agent for Linux OS
- Monitoring Agent for Oracle Database
- Agent de surveillance des temps de réponse
- Monitoring Agent for UNIX OS
- Monitoring Agent for VMware VI
- Monitoring Agent for WebSphere Applications

- Monitoring Agent for WebSphere MQ
- Monitoring Agent for Windows OS
- Monitoring Agent for Tomcat

Intégration à Alert Notification

Pour bénéficier d'une flexibilité plus grande que celle offerte par Cloud APM avec le transfert d'e-mail de base, vous pouvez effectuer une intégration au produit Alert Notification pour développer les capacités de Cloud APM en matière de notification des utilisateurs en cas de problèmes.

L'intégration à Alert Notification vous offre un contrôle granulaire sur les personnes qui reçoivent des notifications et sur la manière dont ces dernières leur parviennent. Par exemple, chaque utilisateur peut décider s'il souhaite recevoir des e-mails, des SMS ou des messages vocaux. Les notifications peuvent également être acheminées vers Slack. Des utilisateurs différents peuvent recevoir des types de notification différents en fonction du jour, du jour de la semaine, etc. Chaque utilisateur peut décider quels types d'alerte vous souhaitez recevoir. Par exemple, un administrateur de base de données peut souhaiter recevoir uniquement des alertes de base de données ayant un niveau de gravité avertissement ou supérieur.

Avant de commencer

Alert Notification est intégré automatiquement à votre abonnement IBM Cloud Application Performance Management, ainsi qu'à votre abonnement d'essai.

Pourquoi et quand exécuter cette tâche

Les événements sont configurés automatiquement pour être envoyés à Alert Notification. Ensuite, vous pouvez créer des règles de notification pour votre abonnement afin de déterminer les alertes pour lesquelles vous souhaitez recevoir des notifications.

Vous pouvez ajouter l'application surveillée aux groupes de ressources. Pour chaque groupe de ressources sauvegardé, vous pouvez configurer une ou plusieurs adresses électroniques. Lorsque les performances d'un système géré dans un groupe dépasse un seuil, une notification par courrier électronique est envoyée aux adresses configurées pour le groupe.

Alert Notification envoie une notification par courrier électronique pour tous les événements ouverts sur les systèmes gérés affectés au groupe.

Procédure

Exécutez les étapes «1», à la page 998 et «2», à la page 998 pour le groupe de ressources pour lequel vous souhaitez acheminer des alertes en fonction du groupe de ressources.

1. Si vous souhaitez acheminer les notifications en fonction des groupes de ressources, suivez les sous-étapes ci-dessous :
   a) Dans la console Cloud APM, cliquez sur **Configuration du système** > **Gestionnaire de groupes de ressources**.
   b) Sélectionnez un groupe de ressources, puis cliquez sur **Editer** pour ouvrir l'**Editeur de groupe de ressources**.

      Important : Vous devez sauvegarder un groupe de ressources nouveau ou modifié avant d'ouvrir Alert Notification. Une fois la sauvegarde effectuée, l'éditeur de groupe de ressources se ferme et vous devez le rouvrir pour pouvoir continuer à l'utiliser.

      Si vous n'effectuez pas la sauvegarde, après avoir configuré des notifications par courrier électronique à l'étape «2», à la page 998 et être revenu à l'éditeur de groupe de ressources, vous risquez de recevoir un message d'erreur vous informant que la mise à jour synchrone n'est pas autorisée.
2. Pour configurer la notification par courrier électronique, procédez comme suit :

a) Dans l'éditeur de groupe de ressources d'APM Console, cliquez sur l'URL **Configurer la notification par courrier électronique** pour ouvrir l'application IBM Alert Notification dans un nouvel onglet ou une nouvelle fenêtre.

Cette action crée automatiquement une règle basée sur le groupe de ressources que vous avez sélectionné à l'étape «1», à la page 998.

Avertissement : Si votre navigateur n'autorise pas les fenêtres en incrustation, la fenêtre Alert Notification ne peut pas s'ouvrir. Vous devez configurer le navigateur de manière à autoriser la fenêtre Alert Notification à s'ouvrir pour pouvoir configurer la notification par courrier électronique d'un groupe de ressources.

b) Dans Alert Notification, configurez des utilisateurs et des groupes et associez leurs adresses électroniques à des groupes de ressources pour que ceux-ci reçoivent des notifications d'événements par courrier électronique.

Vous pouvez configurer vos propres règles et notifications Alert Notification pour le type d'alertes que vous souhaitez recevoir. Par exemple, un administrateur Linux peut souhaiter recevoir des e-mails, des messages SMS ou des messages vocaux pour l'ensemble des systèmes Linux. Ensuite, il peut décider de désactiver les alertes de forte gravité qui sont critiques. Une règle leur permet de filtrer tous les événements qui sont générés par l'agent de système d'exploitation Linux. Pour des informations sur l'utilisation de l'éditeur de notifications dans l'application Alert Notification, voir Création de règles de notification.

Que faire ensuite
Pour plus d'informations sur Alert Notification, voir la Documentation d'IBM Alert Notification.

Intégration à Control Desk

Vous pouvez configurer vos événements à partir de Cloud APM pour que des tickets soient ouverts automatiquement dans IBM Control Desk.

Pourquoi et quand exécuter cette tâche
Vous pouvez intégrer IBM Cloud Application Performance Management à l'aide de la version sur site ou Cloud d'IBM Control Desk.

Procédure

Suivez l'une des procédures suivantes :

- Pour ouvrir des tickets dans votre version sur site d'IBM Control Desk V 7.6, procédez comme suit :
  1. Configurez votre compte de messagerie électronique IBM SmartCloud Notes pour Control Desk afin d'utiliser un client de messagerie IMAP. Durant la configuration, prenez soin de sélectionner **Enable IMAP Access Now**. Pour plus d'informations, voir Enabling IMAP access dans le Knowledge Center d'IBM Connections Social Cloud.
  2. Dans la console Cloud APM, cliquez sur **Configuration système** > **Configuration avancée**, puis définissez les paramètres suivants :

     Adresses e-mail cible
     Spécifiez l'adresse électronique SmartCloud Notes qui est utilisée pour créer des tickets de demande de service.

     Ligne objet de l'e-mail
     Spécifiez une ligne objet pour le message électronique, par exemple, `Evénement PMaaS`.
  3. Accédez au Support Marketplace. et sélectionnez **Service Request** pour soumettre un ticket de demande de service afin de procéder à votre activation.

     Fournissez les informations suivantes dans votre ticket :

     – Adresse électronique SmartCloud Notes

Par exemple, `user@ibmserviceengage.com`.

- Mode de passe de l'adresse électronique SmartCloud Notes
- Nom qualifié complet du serveur de messagerie électronique SmartCloud Notes

  Par exemple, `imap.notes.na.collabserv.com`.
- Numéro de port de l'adresse électronique SmartCloud Notes

  Par exemple, 993.
- URL IBM Control Desk du client

  Indiquez le lien au format suivant : `https://<ID-abonné>.sccd.ibmserviceengage.com/maximo_t4hj/webclient/login/login.jsp?welcome=-true`

4. Pour configurer le port d'écoute de messagerie de sorte à analyser le courrier électronique et à le gérer de manière appropriée lorsque vous voulez affecter des tickets à d'autres groupes dans IBM Control Desk on Cloud, voir Configuring e-mail listeners.

- Pour ouvrir des tickets dans votre environnement cloud IBM Control Desk, procédez comme suit :

1. Accédez au Support Marketplace. et sélectionnez **Service Request** pour soumettre un ticket de demande de service afin de procéder à votre activation.

   Fournissez les informations suivantes dans votre ticket :

   - Adresse électronique SmartCloud Notes

     Par exemple, `user@ibmserviceengage.com`.
   - Mode de passe de l'adresse électronique SmartCloud Notes
   - Nom qualifié complet du serveur de messagerie électronique SmartCloud Notes

     Par exemple, `imap.notes.na.collabserv.com`.
   - Numéro de port de l'adresse électronique SmartCloud Notes

     Par exemple, 993.
   - URL IBM Control Desk du client

     Indiquez le lien au format suivant : `https://<ID-abonné>.sccd.ibmserviceengage.com/maximo_t4hj/webclient/login/login.jsp?welcome=-true`
2. Pour configurer le port d'écoute de messagerie de sorte à analyser le courrier électronique et à le gérer de manière appropriée lorsque vous voulez affecter des tickets à d'autres groupes dans IBM Control Desk on Cloud, voir Configuring e-mail listeners.

Intégration à IBM Cloud

Vous pouvez afficher les informations de surveillance relatives à vos applications dans l'environnement IBM Cloud à l'aide des collecteurs de données sélectionnés.

Lorsqu'il est configuré pour collecter les données d'une application IBM Cloud, un collecteur de données permet l'intégration des fonctionnalités de surveillance à IBM Cloud. Les collecteurs de données transfèrent les données de surveillance et de diagnostic des ressources relatives à vos applications IBM Cloud au serveur Cloud APM. Le serveur Cloud APM reçoit et traite les informations de surveillance qui sont collectées par les collecteurs de données. Les types d'applications IBM Cloud suivants peuvent être surveillés :

- Applications Liberty
- Applications Node.js
- Applications Python
- Applications Ruby

Après configuré correctement un collecteur de données, vous pouvez afficher les données de surveillance sur la console Cloud APM. Pour obtenir des instructions de configuration, voir «Procédure générale de configuration des collecteurs de données», à la page 189.

Intégration à IBM Agent Builder

Vous pouvez créer, modifier, déboguer et conditionner des agents à l'aide d'Agent Builder qui étend les fonctionnalités de surveillance d'un environnement IBM Tivoli Monitoring ou IBM Cloud Application Performance Management. Un agent personnalisé utilise ces environnements pour surveiller tout type de logiciel interne ou personnalisé.

Pour des détails, voir le document IBM Agent Builder - Guide d'utilisation.

Chapitre 9. Gestion

Démarrage de la console Cloud APM

Connectez-vous à la console Cloud APM depuis votre navigateur afin de consulter l'état de vos applications dans les tableaux de bord.

Avant de commencer

- Activez votre compte à l'aide du lien fourni dans l'e-mail de confirmation que vous avez reçu à la suite de votre première inscription au service.
- Pour être sûr que l'interface utilisateur ne soit pas tronquée, utilisez une résolution minimale de 1280 x 1024.
- Pour des performances optimales, utilisez l'un des navigateurs pris en charge. Pour une liste des navigateurs pris en charge, accédez à la page System requirements (APM Developer Center). Sélectionnez l'un des liens du produit IBM Cloud Application Performance Management et cliquez sur le lien "Serveur". Dans le rapport qui s'affiche, cliquez sur "Navigateurs Web" ou faites défiler l'écran jusqu'à cette option.

Procédure

1. Pour accéder à la console Cloud APM, utilisez le lien fourni dans l'e-mail vous signalant que votre service est prêt.
2. Vous pouvez également accéder à votre console à partir du site Web d'IBM Marketplace :
   a. Accédez à Produits et services sur le site Web IBM Marketplace.
   b. Connectez-vous avec le nom d'utilisateur et le mot de passe que vous avez utilisés pour vous enregistrer pour le service.
   c. Sur la ligne serveur Cloud APM, cliquez sur **Launch**.

Résultats

Une fois que vous vous êtes connecté, la page **Mise en route** s'affiche avec des options d'apprentissage pour **Tâches de l'utilisateur** et **Tâches de l'administrateur** et permet d'accéder à **Ressources communautaires**.

Que faire ensuite

- Familiarisez-vous avec les éléments de l'interface utilisateur en cliquant sur le lien hypertexte pour effectuer une visite du tableau de bord Cloud APM. Regardez les vidéos des tâches d'utilisateur et des tâches d'administrateur pour vous aider à démarrer le système en utilisant et en personnalisant votre environnement Cloud APM.
- Ajoutez des applications pour afficher les tableaux de bord de vos ressources suivant des regroupements logiques, tels que Commande en ligne. Pour plus d'informations, voir «Gestion des applications», à la page 1129.
- Créez des seuils pour le test des conditions qui, lorsqu'ils sont atteints, ouvrent un événement. Par exemple, un seuil peut ouvrir un événement lorsque l'espace de stockage est utilisé à 90 %. Pour plus d'informations, voir «Gestionnaire de seuils», à la page 1014.
- Ajoutez et affectez des utilisateurs à des groupes d'utilisateurs et des rôles pour contrôler l'accès aux ressources gérées et aux fonctions de la console Cloud APM. Pour plus d'informations, voir «Gestion des accès utilisateur», à la page 1030.

- Pour plus d'informations sur la surveillance de la Liste d'applications Java IBM et la Pile d'intégration IBM, voir «Scénarios», à la page 90.
- Si, au lieu de la page de mise en route ou du Tableau de bord d'Application Performance, votre navigateur accède au site Web d'IBM, votre identificateur utilisateur n'a aucun droit sur la console Cloud APM. Vous devez demander l'accès à votre administrateur.
- Si aucun indicateur n'apparaît pour une source de données, consultez le forum Cloud Application Performance Management sur developerWorks. Recherchez le terme "tableau de bord" dans le forum, répondez à une entrée pour poser une question associée ou créez une entrée et décrivez le symptôme.
- Si vous démarrez la console Cloud APM depuis Internet Explorer 8, 9 ou 10 et que vous obtenez une erreur signalant que `la page ne peut pas s'afficher`, vous devrez peut-être activer l'option de sécurité, TLS 1.2. Pour plus d'informations, recherchez "tls" sur le forum forum Cloud Application Performance Management.

Seuils et groupes de ressources

Les seuils déterminent certaines conditions, telles que le nombre de transactions par minute inférieur à 100 et ouvrent un événement quand les conditions ont été remplies. Utilisez des seuils pour surveiller les problèmes réels et éventuels sur vos ressources surveillées. Affectez des seuils aux groupes de ressources pour la surveillance sur tous les systèmes gérés du même type qui appartiennent au groupe.

Informations de référence

Examinez les informations de référence pour en savoir plus sur les seuils, les seuils prédéfinis pour les agents, les groupes de ressources auxquels ils sont affectés et la personnalisation des seuils.

Seuils prédéfinis

Vos agents de surveillance sont fournis avec des *seuils prédéfinis* activés et démarrés avec l'agent. La première fois que vous ouvrez le **Gestionnaire de seuils**, après avoir installé l'agent, la liste de seuils qui s'affiche pour le type de source de données sélectionné correspond aux seuils prédéfinis. Ces seuils prédéfinis sont affectés au groupe de ressources système par défaut de l'agent et indiqués dans la colonne **Groupes affectés**.

Si vous modifiez un seuil prédéfini, que ce soit pour changer le nom ou la condition, le seuil n'est plus considéré comme un seuil prédéfini mais comme un *seuil personnalisé*. Cependant, vous pouvez redéfinir le groupe de ressources affecté pour un seuil prédéfini du groupe de systèmes par défaut sur un groupe défini par l'utilisateur et il reste un seuil prédéfini.

Si vous préférez ne pas utiliser les seuils prédéfinis, vous pouvez les désactiver dans la page **Configuration avancée** (voir «Activation des seuils», à la page 1106). La désactivation des seuils prédéfinis n'a pas pour effet de les supprimer du **gestionnaire de seuils** ; elle supprime uniquement leur affectation de groupe et les rend ainsi inactifs. Après avoir désactivé les seuils prédéfinis, vous pouvez ouvrir le **gestionnaire de seuils** et vous rendre compte que la colonne **Groupes affectés** est vide pour chaque seuil prédéfini (voir «Exemples de seuils désactivés», à la page 1006).

Vous pouvez activer le seuil comme seuil personnalisé en l'affectant à n'importe quel groupe de ressources disponible.

Seuils personnalisés

Les nouveaux seuils que vous créez sont les seuils personnalisés, comme indiqué dans la colonne **Origine** du **gestionnaire de seuils**. Si vous modifiez un seuil prédéfini, ce devient également un seuil personnalisé et son origine passe de "Prédéfini" à "Personnalisé".

Exécution d'une commande

Une fois qu'un événement a été ouvert pour un seuil défini sur true, vous pouvez exécuter automatiquement une commande ou un script de commandes sur le système surveillé pour lequel l'événement a été ouvert. Vous pouvez par exemple vouloir consigner des informations, déclencher un bip audible ou arrêter un travail qui consomme trop ressources.

La commande respecte la syntaxe suivante :

```
&{jeu_données.attribut}
```

où *jeu_données* est le nom du jeu de données et *attribut* est le nom d'attribut tel qu'affiché dans l'éditeur de seuil. Si le jeu de données ou le nom d'attribut contient un espace, remplacez l'espace par un trait de soulignement.

L'exemple suivant montre comment transmettre le paramètre de nom de disque à une ressource gérée :

```
/scripts/clean_logs.sh &{disque_KLZ.nom_disque}
```

Vous pouvez transférer un ou plusieurs attributs depuis le jeu de données. S'ils sont spécifiés, les attributs multiples sont transférés dans la commande dans l'ordre ($1, $2, etc.).

La commande s'exécute à partir de la ligne de commande avec le même compte utilisateur que celui avec lequel l'agent ou le collecteur d'agent a démarré. Par exemple, si l'agent s'exécute en tant que superutilisateur, le superutilisateur exécute la commande sur le système géré.

Les options suivantes contrôlent la fréquence d'exécution de la commande :

Sélectionnez ☐ **Lors du premier événement uniquement** si l'ensemble de données renvoie plusieurs lignes et que vous souhaitez n'exécuter la commande que pour la première occurrence de l'événement dans l'échantillon de données. Décochez cette case pour exécuter la commande pour chaque ligne qui génère un événement.

Sélectionnez ☐ **Pour chaque intervalle vrai consécutif** pour exécuter la commande chaque fois que le seuil est défini sur true. Décochez cette case pour exécuter la commande lorsque le seuil a la valeur true, mais pas une deuxième fois tant que le seuil n'a pas la valeur false, suivi par une autre évaluation true dans un intervalle ultérieur.

Groupes de ressources

Les groupes de ressources représentent une collection de systèmes gérés et déterminent comment les seuils sont répartis. Vous affectez un seuil au groupe de ressources qui inclut les systèmes gérés où il doit s'exécuter.

Tous les seuils prédéfinis ont une affectation de groupe de ressources par défaut, qui est le groupe défini par le système pour le type d'agent, tel que Db2 et Microsoft IIS.

Vous pouvez créer des groupes de ressources personnalisées et sélectionner les systèmes gérés à inclure dans chaque groupe. Vous pouvez avoir plusieurs types d'agent dans un groupe de ressources personnalisées ; les seuils affectés au groupe sont distribués uniquement aux systèmes gérés du même type d'agent. Par exemple, un seuil qui est créé avec des attributs de système d'exploitation Linux OS affecté à un groupe de ressources de systèmes gérés Linux OS, MongoDB et Python est distribué aux systèmes gérés Linux OS.

Pour plus d'informations, voir «Gestionnaire de groupes de ressources», à la page 1008.

Statut des événements dans le Tableau de bord d'Application Performance

Les gravités de statut affichées dans le Tableau de bord d'Application Performance indiquent la gravité d'événement la plus élevée pour l'application, le groupe, le sous-groupe et l'instance de système géré sélectionnés.

Après avoir sélectionné une application depuis le navigateur ou une zone récapitulative dans le tableau de bord **Toutes mes applications**, un tableau de bord à onglets présente les différentes facettes de votre application. L'onglet **Evénements** fournit des informations sur les événements pour l'élément de navigateur sélectionné, comme décrit dans «Statut de l'événement», à la page 1140.

Les modifications de seuil affectent également les autres seuils associés au même agent de surveillance

Après la création, la modification ou la suppression d'une définition de seuil, ou la modification de la liste des seuils qui sont distribués sur un agent de surveillance, tous les événements échantillonnés sont fermés pour les agents sur lesquels le seuil a été distribué. Après la fermeture des événements, les agents de surveillance rouvrent les événements dès lors qu'une condition de seuil est évaluée à true. Sur la console Cloud APM, les événements fermés disparaissent de la console jusqu'à ce qu'ils

soient rouverts avec une nouvelle valeur d'**horodatage**. Si vous recevez les notifications d'événement par courrier électronique, vous recevrez les notifications des événements ouverts et fermés par ce biais.

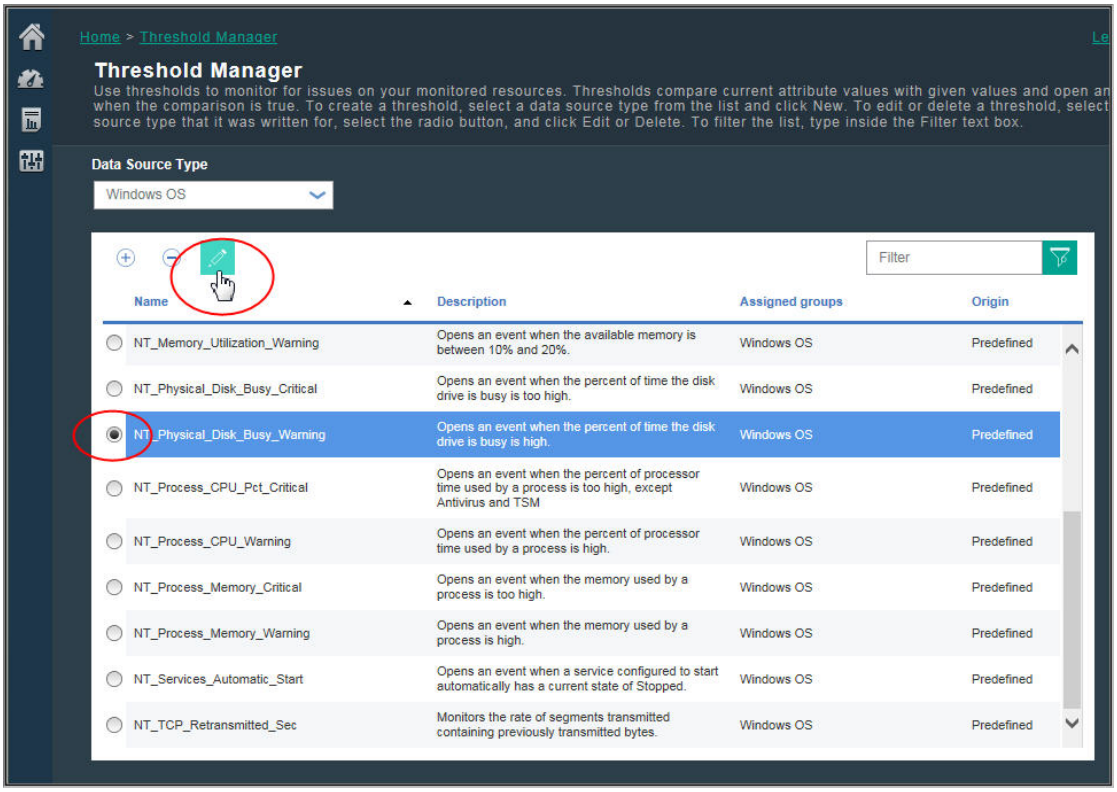
Imaginez, par exemple, que vous disposez d'un groupe de ressources personnalisées intitulé Systèmes de site, auquel vous affectez des seuils et des agents de système d'exploitation Linux et WebSphere Applications. Vous créez un nouveau seuil de système d'exploitation Linux et l'affectez à Systèmes de site. Tous les événements échantillonnés ouverts sur les agents de système d'exploitation Linux qui sont affectés à Systèmes de sites sont fermés. Ensuite, les événements échantillonnés sont rouverts si les conditions de seuil sont encore à true.

Exemples de seuils désactivés

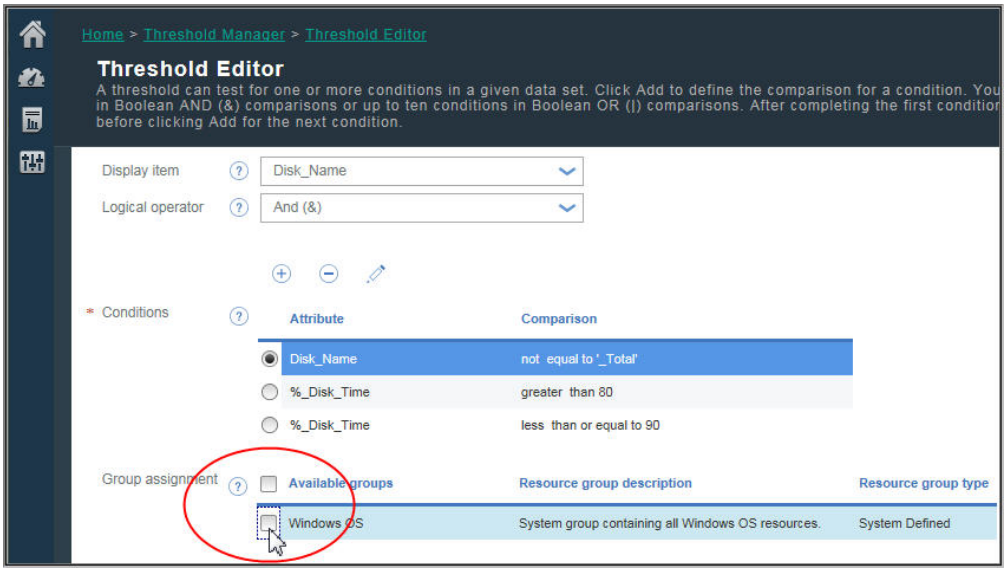
Vous pouvez désactiver les seuils prédéfinis pour tous les agents dans votre environnement. Vous pouvez également désactiver des seuils séparément, qu'ils soient prédéfinis ou personnalisés. Lorsqu'un seuil est désactivé, il ne s'exécute pas sur les systèmes gérés et aucun événement n'est ouvert.Pour désactiver un seuil, supprimez ses affectations de groupe de ressources. Un paramètre de **Configuration avancée** est également disponible pour désactiver tous les seuils prédéfinis pour tous les agents.

Désactivation d'un seuil unique

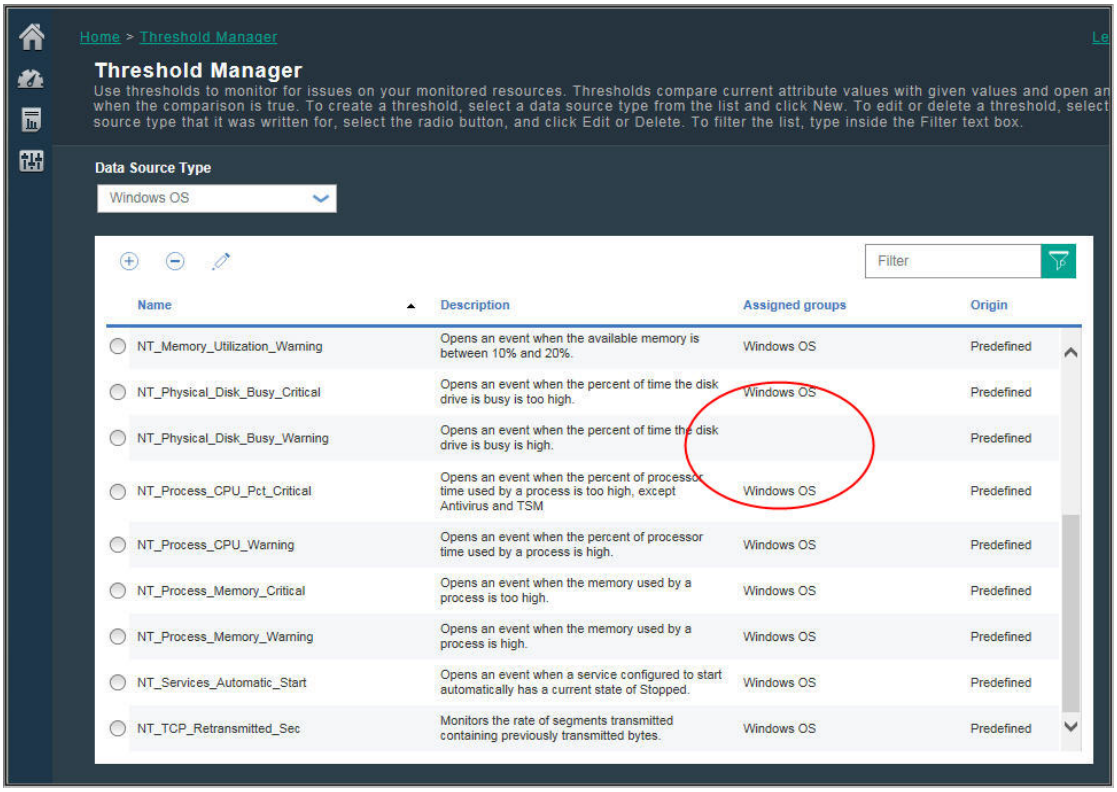
Dans cette image, le seuil à désactiver est sélectionné dans le **Gestionnaire de seuils** et l'utilisateur clique sur **Editer** :



Le seuil est ouvert dans l'éditeur de seuil. L'utilisateur décoche la case du groupe de ressources affecté dans la zone **Affectation de groupes** :

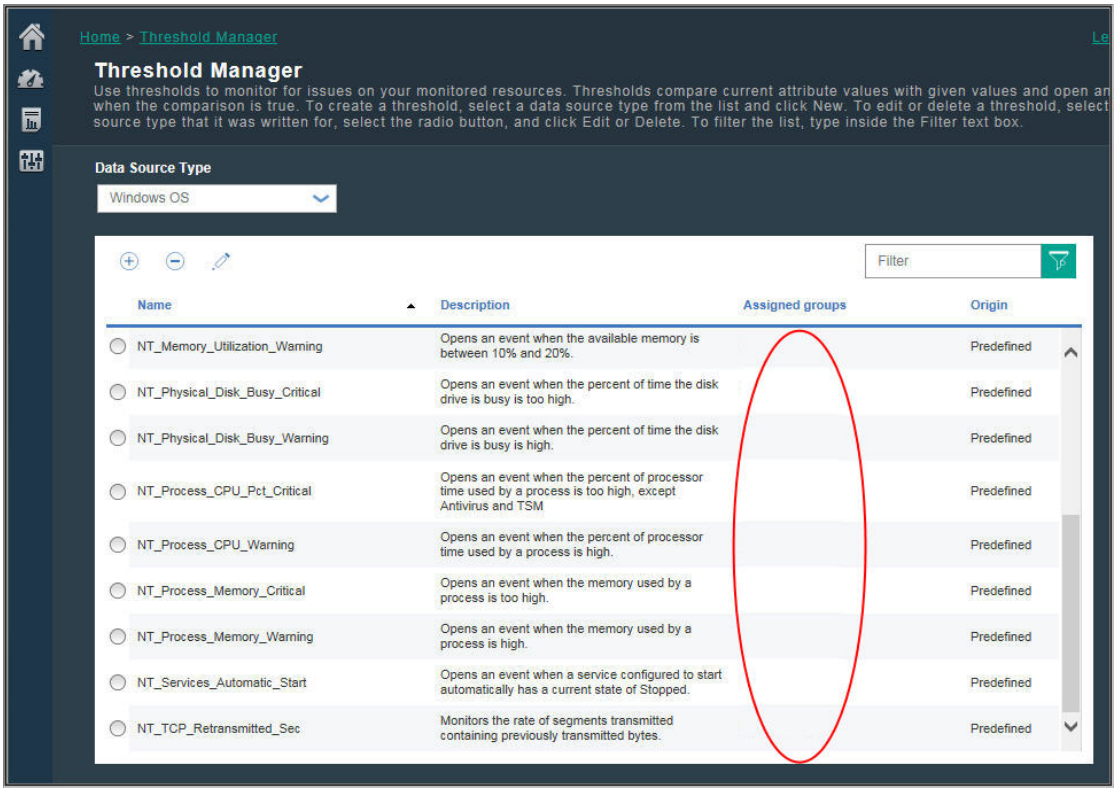


Une fois que l'utilisateur a cliqué sur **Sauvegarder**, le **gestionnaire de seuil** est affiché. Le seuil est désactivé, et la colonne **Groupes affectés** est vide :



Désactivation de tous les seuils prédéfinis

Désactivez tous les seuils prédéfinis pour tous les agents de surveillance sur la page **Configuration avancée**, comme décrit dans «Activation des seuils», à la page 1106. Lorsque vous ouvrez ensuite le **gestionnaire de seuil**, la colonne **Groupes affectés** est vide pour chaque seuil prédéfini, indiquant que les seuils sont inactifs :



Concepts associés

«Informations de référence», à la page 1004
Examinez les informations de référence pour en savoir plus sur les seuils, les seuils prédéfinis pour les agents, les groupes de ressources auxquels ils sont affectés et la personnalisation des seuils.

Référence associée

«Gestionnaire de seuils», à la page 1014

Gestionnaire de groupes de ressources

Votre environnement surveillé peut comporter plusieurs systèmes gérés pouvant être catégorisés par objectif. Ces systèmes possèdent souvent les mêmes exigences de seuil. Utilisez le **gestionnaire de groupes de ressources** pour organiser les systèmes gérés en groupes auxquels vous pouvez affecter des seuils. Vous pouvez également créer des groupes de ressources correspondant à vos stratégies de contrôle d'accès basé sur les rôles.

Une fois que vous avez cliqué sur **Configuration du système** > **Gestionnaire de groupes de ressources**, la page s'affiche avec une table des groupes de ressources. Dans un premier temps, un groupe de systèmes prédéfini s'affiche pour chaque type d'agent de surveillance installé, comme `Windows OS`. Chaque groupe de systèmes contient tous les seuils prédéfinis de l'agent.

Votre accès au **gestionnaire de groupes de ressources** et aux groupes de ressources est contrôlé par vos droits d'utilisateur. Pour pouvoir afficher un groupe de ressources, vous devez disposer des droits d'affichage correspondants ; de la même manière, pour pouvoir créer, modifier ou supprimer un groupe de ressources, vous devez disposer de droits de modification.

Cette table contient des outils permettant de gérer les groupes de ressources.

- **Nouveau** ouvre l'**Editeur de groupe de ressources** pour affecter des systèmes gérés et des seuils.
- Sélectionnez un groupe de ressources pour afficher les ressources affectées et les seuils affectés au groupe dans la sous-fenêtre adjacente.
- Sélectionnez un groupe de ressources et cliquez sur **Editer** afin d'ouvrir l'**Editeur de groupe de ressources** pour modifier les affectations de système géré et de seuil.

- Sélectionnez un groupe de ressources dont vous ne voulez plus et cliquez sur **Supprimer**. Après confirmation de la suppression, les seuils qui étaient affectés au groupe doivent être affectés à un autre groupe si vous voulez qu'ils continuent à s'exécuter sur vos systèmes gérés.
- Vous pouvez cliquer dans la zone de texte du filtre et entrer la valeur du filtre. Au fur et à mesure de la saisie, les lignes qui ne répondent pas aux critères sont filtrées. Pour effacer le filtre, cliquez sur dans la zone de filtre ou appuyez sur la touche Retour arrière.

Le tableau contient les groupes de ressources disponibles :

Nom du groupe de ressources
Les groupes prédéfinis sont nommés en fonction de leur type d'agent ; les groupes personnalisés sont nommés par l'auteur.

Description du groupe de ressources
Un groupe prédéfini est décrit comme étant un *groupe de systèmes* pour la ressource surveillée ; les groupes personnalisés sont décrits par l'auteur.

Un groupe de systèmes, tel que `Linux OS`, inclut tous les seuils prédéfinis pour l'agent et tous les systèmes gérés sur lesquels l'agent est installé. Vous pouvez éditer un groupe de systèmes pour affecter ou supprimer des seuils, mais vous ne pouvez pas affecter ou supprimer des systèmes gérés. Les systèmes gérés sont affectés automatiquement à un groupe de systèmes du même type, y compris ceux issus de votre domaine Tivoli Monitoring si une Passerelle hybride est configurée.

Certains groupes de ressources système ont un lien avec les agents qui prennent en charge les sous-noeuds. En fonction du type d'agent, les sous-noeuds et/ou le noeud agent peuvent être ajoutés aux applications. Si seuls les sous-noeuds peuvent être ajoutés aux applications définies, vous ne pouvez pas visualiser les événements associés aux seuils qui ont été définis pour le noeud agent. Toutefois, les événements peuvent être transférés à un gestionnaire d'événements tel que Netcool/OMNIbus. De même, les abonnés IBM Cloud Application Performance Management peuvent configurer Alert Notification.

Type du groupe de ressources
Les groupes prédéfinis sont *définis par le système*. Un groupe prédéfini est associé à chaque type d'agent que vous avez installé dans votre environnement.

Les groupes personnalisés que vous, ou tout autre utilisateur, créez dans votre environnement sont *définis par l'utilisateur*.

Editeur de groupe de ressources

Une fois que vous avez cliqué sur **Nouveau** pour ajouter un groupe ou après avoir sélectionné un groupe et cliqué sur **Editer** pour éditer un groupe, l'**Editeur de groupe de ressources** s'affiche et comporte les zones suivantes :

Nom du groupe
Le nom du groupe est obligatoire. Vous pouvez modifier un nom de groupe personnalisé existant, et toutes les références à ce groupe sont mises à jour automatiquement lorsque vous sauvegardez vos modifications.

Description du groupe
Facultative pour les groupes personnalisés. Ajoutez une description de l'organisation du groupe. Cette description est affichée dans le **Gestionnaire de groupes de ressources**.

Affectation de ressource
Tous les systèmes gérés qui sont disponibles pour ajout au groupe sont répertoriés dans la liste d'agent par leur nom de système géré, nom d'hôte, type d'agent et domaine. Vous pouvez cliquer sur un en-tête de colonne pour trier la liste par nom d'agent, nom d'hôte, type ou domaine.

Pour alimenter le groupe, cochez la case correspondant à un ou plusieurs systèmes gérés.

Vous pouvez sélectionner **Afficher uniquement les ressources sélectionnées** afin de masquer les systèmes gérés non affectés.

Si vous avez configuré la Passerelle hybride d'IBM Cloud Application Performance Management, vous pouvez ajouter des systèmes gérés issus de votre domaine IBM Tivoli Monitoring aux groupes de

ressources définis par l'utilisateur. Vous ne pouvez ni ajouter des systèmes gérés Tivoli Monitoring aux groupes définis par le système, ni créer de seuils pour ces derniers.

Affectation de seuil

Tous les seuils qui ont été prédéfinis ou ajoutés via le **gestionnaire de seuils** sont répertoriés dans la liste des seuils par leur nom et leur type d'agent. Vous pouvez cliquer sur l'en-tête d'une colonne pour trier la liste.

Pour ajouter un seuil au groupe, cochez la case en regard du nom ; pour retirer un seuil du groupe, décochez la case. Pour que le **gestionnaire de seuils** ajoute ou retire des seuils, vous devez disposer de droits d'affichage. Lorsque vous ajoutez des seuils à un groupe de systèmes, les seuils disponibles sont ceux dont l'ensemble de données est adapté au groupe de systèmes.

Les seuils que vous affectez au groupe sont distribués à chacun des systèmes gérés du groupe de même type d'agent. Même si vous pouvez affecter des seuils de tout type d'agent de surveillance à un groupe, les seuils affectés sont distribués uniquement aux systèmes gérés de même type qui sont membres du groupe. Par exemple, si vous affectez le seuil `MySQL_Process_Down` au groupe, il est inclus dans le groupe, mais n'est distribué qu'aux systèmes gérés par Monitoring Agent for MySQL qui appartiennent au groupe.

Vous pouvez sélectionner **Afficher uniquement les seuils sélectionnés** pour masquer les seuils non affectés. Si vous filtrez la liste, cliquez sur dans la zone de filtre pour effacer le filtre et activer la case à cocher.

Vous pouvez également affecter un groupe de ressources à un seuil à partir du **Gestionnaire de seuils**.

Configuration de la notification par courrier électronique

Disponible avec IBM Cloud Application Performance Management : Cliquez sur **Configurer la notification par courrier électronique** pour ouvrir l'application IBM Alert Notification dans un nouvel onglet ou une nouvelle fenêtre de navigation. Utilisez Alert Notification pour créer des utilisateurs et associer leurs adresses électroniques à des groupes de ressources pour que ceux-ci reçoivent des notifications d'événements par courrier électronique.

Avertissement : Si votre navigateur n'autorise pas les fenêtres en incrustation, la fenêtre Alert Notification ne peut pas s'ouvrir. Vous devez configurer le navigateur de manière à autoriser la fenêtre Alert Notification à s'ouvrir pour pouvoir configurer la notification par courrier électronique d'un groupe de ressources.

Lorsque vous cliquez sur **Sauvegarder**, le groupe de ressources est sauvegardé avec la liste des groupes de ressources et apparaît dans le tableau du **gestionnaire de groupes de ressources**.

Tâches associées

«Intégration à Alert Notification», à la page 998

«Exploration des API», à la page 1103

Référence associée

«Gestionnaire de seuils», à la page 1014

Tutoriel : Définition d'un seuil

Les seuils sont le mécanisme d'alerte des problèmes réels et potentiels liés à vos ressources gérées. Utilisez le tutoriel pour connaître les étapes de base de définition d'un seuil afin de déclencher une alarme lorsque la condition se produit.

Pourquoi et quand exécuter cette tâche

Ce tutoriel s'appuie sur l'agent Linux OS pour montrer comment définir un seuil dans le **Gestionnaire de seuils** et afficher l'alarme déclenchée dans le Tableau de bord d'Application Performance. Votre ID utilisateur doit disposer du droit d'affichage du **Gestionnaire de seuils** pour effectuer ces étapes.

Procédure

1. Dans la barre de navigation, cliquez sur **Configuration du système** > **Gestionnaire de seuils**.
2. Cliquez sur la zone de liste **Type de source de données** et sélectionnez le type de données **Linux OS**.

Les seuils qui sont définis pour l'agent Linux OS sont affichés dans le tableau.

3. Cliquez sur **Nouveau** pour ouvrir l'**éditeur de seuil** afin de définir le seuil.
4. Définissez un seuil pour déclencher une alarme de gravité Inconnue lorsque l'UC moyenne est en-dessous de 75 % :
   a) Dans la zone **Nom**, entrez `CPU_average_below_75_percent`.
   b) Dans la zone **Description**, entrez `Tutoriel : Seuils`.
   c) Conservez les valeurs par défaut dans les zones **Gravité**, **Intervalle** et **Echantillons consécutifs requis**.
   d) Dans la zone **Ensemble de données**, sélectionnez **Moyennes UC KLZ**.
   e) Dans la zone **Conditions**, cliquez sur **Nouveau**, puis ajoutez la comparaison dans la boîte de dialogue qui apparaît :
      1) Dans la zone **Attribut**, sélectionnez **CPU_Usage_Current_Average**
      2) Dans la zone **Opérateur**, sélectionnez **Inférieur à**.
      3) Dans la zone **Valeur**, entrez 75.

      Lorsque vous cliquez sur **OK**, l'attribut et la comparaison s'affichent dans la zone **Conditions**.
   f) Dans la zone **Affectation de groupes**, sélectionnez le groupe système **Linux OS**.
   g) Cliquez sur **Sauvegarder** pour terminer la définition et revenir à la page **Gestionnaire de seuils**.

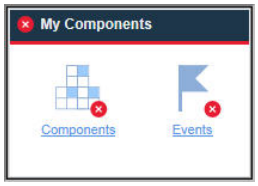
   `CPU_average_below_75_percent` apparaît dans la liste des seuils qui sont définis pour la source de données Linux OS.

Résultats

Vous avez défini un seuil qui déclenche une alarme lorsque l'utilisation de l'UC moyenne sur n'importe lequel de vos systèmes gérés Linux OS est en-dessous de 75 %.

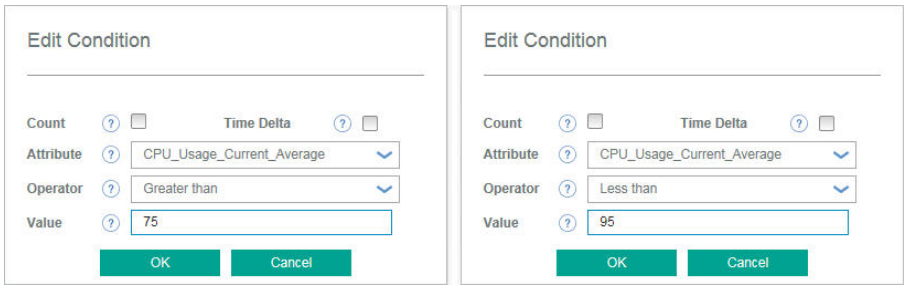
Que faire ensuite

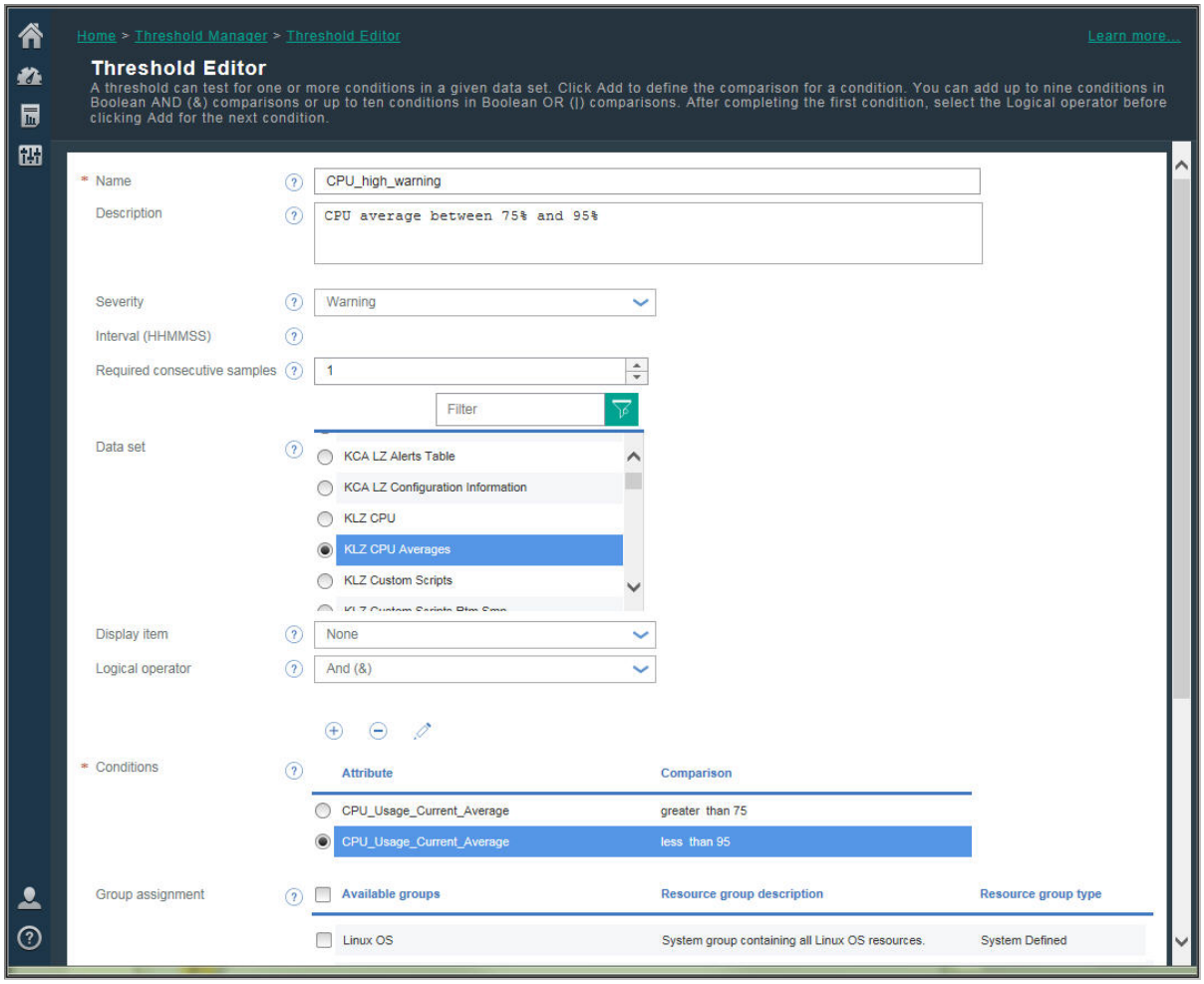
- Affichez l'événement :
  1. Dans la barre de navigation, cliquez sur **Performance** > **Tableau de bord d'Application Performance**.
  2. Dans la zone de récapitulatif **Mes composants**, cliquez sur le lien **Evénements**.

  3. Dans l'onglet **Evénements** qui s'ouvre, recherchez le seuil `CPU_average_below_75_percent` dans la liste. Le déclenchement de l'alarme peut prendre 1 ou 2 minutes. Si l'UC moyenne est au-dessus de 75 %, aucune alarme n'est déclenchée.
- Editez le seuil :
  1. Dans la barre de navigation, cliquez sur **Configuration du système** > **Gestionnaire de seuils**.
  2. Cliquez sur la zone de liste **Type de source de données**, puis sélectionnez le type de données **Linux OS**.
  3. Sélectionnez le seuil `CPU_average_below_75_percent` dans la liste, puis cliquez sur **Editer**.
  4. Modifiez l'une des zones d'une condition pour laquelle vous voulez être alerté. Par exemple, vous pouvez changer **Nom** en `CPU_high_warning`, changer **Gravité** en **Avertissement**, remplacer la condition par **Supérieur à 75** et ajouter une condition **Inférieur à 95**. Pour éditer la comparaison, cliquez sur **Editer**, changez **Opérateur** en **Supérieur à** et cliquez sur **OK**. Pour ajouter la nouvelle condition, laissez la zone **Opérateur logique** définie sur la valeur par défaut **Et**

(&), cliquez sur **Nouveau** pour créer une nouvelle condition, sélectionnez l'**Opérateur** **Inférieur à**, puis entrez la **Valeur** 95.





- Examinez les seuils prédéfinis pour vos agents et adaptez toutes les valeurs de comparaison en fonction de votre environnement.
- Créez de nouveaux seuils pour déclencher des alarmes sur d'autres conditions dont vous voulez être alerté.

Référence associée

«Gestionnaire de seuils», à la page 1014

Tutoriel : Définition d'un seuil pour exécuter une commande sur la ressource gérée

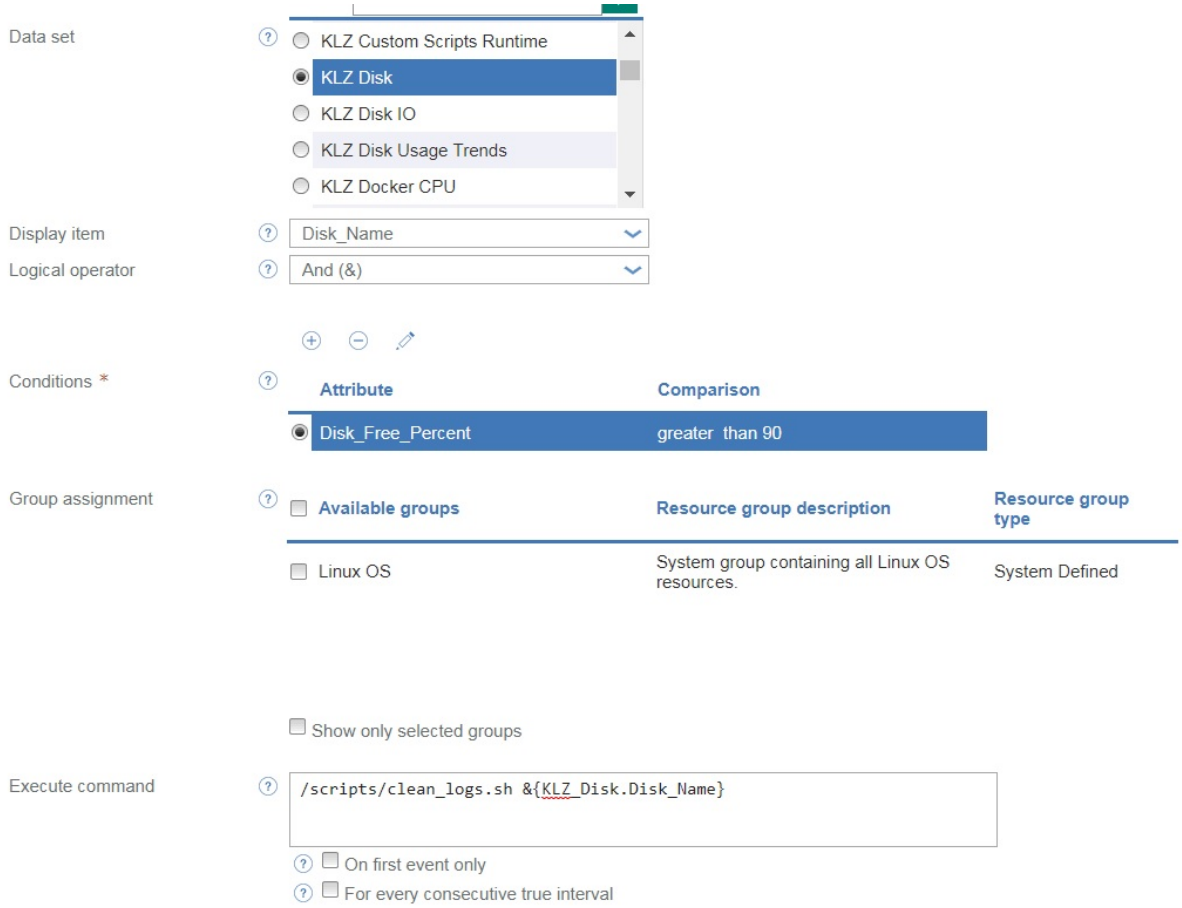
Vous pouvez utiliser l'**éditeur de seuil** pour transmettre certains paramètres aux agents. Vous avez la possibilité de spécifier les commandes ou un script des commandes qui s'exécuteront automatiquement lors du déclenchement d'un événement.

Pourquoi et quand exécuter cette tâche

Ce tutoriel montre l'utilisation de la zone **Exécuter la commande** pour transmettre un paramètre à votre agent IBM Cloud Application Performance Management.

Procédure

1. Ouvrez le **Gestionnaire de seuils** en cliquant sur **Configuration du système** > **Gestionnaire de seuils**.
2. Sélectionnez *Linux OS* dans la zone **Type de source de données**.
   Les seuils qui sont définis pour l'agent Linux OS sont affichés dans le tableau.
3. Cliquez sur **Nouveau** pour ouvrir l'**éditeur de seuil** afin de définir le seuil.
4. Définissez le seuil et les conditions en spécifiant des valeurs pour les différents paramètres tels que **Nom**, **Gravité** et **Conditions**.
5. Sélectionnez *KLZ Disk* dans la zone **Jeu de données**.



6. Entrez la commande suivante dans la zone **Exécuter la commande** :

```
/scripts/clean_logs.sh &{KLZ_Disk.Disk_Name}
```

Vous devez remplacer l'espace dans le nom du jeu de données *KLZ Disk* par un trait de soulignement. Le disque *KLZ_Disk.Disk_Name* est transmis dans le script de commandes.

Résultats
Votre script de commandes est configuré pour s'exécuter automatiquement lorsque le seuil défini est atteint. Les commandes sont exécutées sur le système contrôlé pour lequel les événements sont déclenchés.
Référence associée
«Gestionnaire de seuils», à la page 1014

Gestionnaire de seuils

Le **Gestionnaire de seuils** permet de consulter les seuils prédéfinis d'un agent de surveillance et de créer et d'éditer des seuils.Les seuils sont utilisés pour comparer la valeur d'échantillon d'un attribut avec la valeur définie dans le seuil. Si la valeur d'échantillon satisfait la comparaison, un événement est ouvert. L'événement se ferme automatiquement lorsque la comparaison de seuils n'est plus vraie.

Une fois que vous avez cliqué sur **Configuration du système** > **Gestionnaire de seuils**, la page est affichée avec une table des seuils définis pour le type de source de données sélectionné.

Les types de données qui s'affichent lorsque vous cliquez sur la zone de liste **Type de source de données** sont pour les types d'agents de surveillance et de collecteurs de données installés dans votre environnement géré. Sélectionnez le type de données pour lequel vous souhaitez créer ou afficher des seuils.

Ce tableau répertorie l'ensemble des seuls créées pour le type de données sélectionné et comporte des outils pour la gestion des seuils.

- **Nouveau** ouvre l'**Editeur de seuils**, qui permet de définir un seuil pour le type de données sélectionné.
- Sélectionnez un seuil et cliquez sur **Editer** pour ouvrir l'**Editeur de seuils** qui permet d'éditer la définition.
- Sélectionnez un seuil dont vous ne voulez plus et cliquez sur **Supprimer**. Une fois que vous avez confirmé que vous souhaitez supprimer le seuil, ce dernier est supprimé de la liste et des groupes de ressources auxquels il était affecté. Tous les événements ouverts pour le seuil sont fermés.
- Pour une liste longue, vous pouvez cliquer dans la zone de texte du filtre et taper le début de la valeur du filtre. Au fur et à mesure de la saisie, les lignes qui ne répondent pas aux critères sont filtrées. Pour effacer le filtre, cliquez sur dans la zone de filtre ou appuyez sur la touche Retour arrière.

Pour plus d'informations sur les seuils prédéfinis et sur les seuils personnalisés affichés dans le tableau, ainsi que sur la signification de l'affectation de groupe de ressources (ou sur l'absence de signification), voir «Informations de référence», à la page 1004. Pour une leçon pratique rapide, voir «Tutoriel : Définition d'un seuil», à la page 1010.

Editeur de seuils

Après avoir cliqué sur **Nouveau** ou sélectionné un seuil et cliqué sur **Editer**, l'Editeur de seuils s'affiche et comporte les zones suivantes :

Nom
Entrez un nom unique pour le seuil. Ce nom doit commencer par une lettre et peut contenir jusqu'à 31 lettres, nombres et traits de soulignement. Par exemple, "Average_Processor_Speed_Warning". Le nom du seuil apparaît dans l'onglet **Evénements** du Tableau de bord d'Application Performance et dans certaines tables du tableau de bord.

Description
Facultatif. La description est utile pour enregistrer l'objectif du seuil que les utilisateurs peuvent voir dans le **Gestionnaire de seuils**.

Gravité
Sélectionnez la gravité d'événement appropriée dans la liste : Fatal, Critique, Mineur, Avertissement, ou Inconnu.

Les gravités sont consolidées pour être affichées dans le Tableau de bord d'Application Performance : les événements Fatal et Critique sont affichés sous ; les événements Mineur et Avertissement sont affichés sous et les événements Inconnu sont affichés sous (voir «Statut de l'événement», à la page 1140).

Acheminer l'événement de fonction d'intégration d'événements ?

Si vous avez configuré la transmission des événements sur la page **Configuration système** > **Configuration avancée** («Gestionnaire d'événements», à la page 1104), les événements ouverts sont transmis par défaut aux destinations d'événement que vous avez configurées, comme les cibles d'événement EIF, Cloud Event Management ou Alert Notification par exemple. Spécifiez la valeur **Non** si vous ne souhaitez pas transmettre les événements de ce seuil à une destination d'événement.

Si vous avez configuré la transmission des événements sur la page **Configuration système** > **Configuration avancée** (Event Manager), les événements ouverts sont transmis à un récepteur EIF par défaut. Spécifiez la valeur **Non** si vous ne souhaitez pas transmettre les événements de ce seuil à un récepteur EIF.

Pour personnaliser le mappage des seuils aux événements transmis et remplacer ainsi le mappage par défaut entre les seuils et les événements transmis au serveur d'événements, cliquez sur **Personnalisation de l'attribut EIF**. Pour plus d'informations, voir «Personnalisation d'un événement à transmettre à un récepteur EIF», à la page 1019.

Intervalle

Entrez ou sélectionnez le délai d'attente entre les prises d'échantillons de données au format *HHMMSS*, par exemple, 00 15 00 pour 15 minutes. Pour les seuils d'événement échantillonnés, l'intervalle minimum est 000030 (30 secondes) et l'intervalle maximum est 235959 (23 heures, 59 minutes, 59 secondes).

La valeur 000000 (six zéros) indique un seuil d'événement *pur*. Les événements purs sont des notifications non sollicitées. Aucun intervalle d'échantillonnage n'est défini pour les seuils des événements purs et il n'est donc pas possible de surveiller les valeurs en cours d'un indicateur constant. Les événements purs sont fermés après 24 heures ou après la valeur définie dans la zone **Heures avant la fermeture des événements purs** de la page **Configuration avancée**, catégorie «Gestionnaire d'événements», à la page 1104.

Echantillons consécutifs requis

Indiquez le nombre d'échantillons de seuil consécutifs devant avoir la valeur vrai pour qu'un événement soit généré : lorsqu'un seuil est défini à la valeur 1 et qu'un échantillon est à la valeur vrai, un événement est généré immédiatement. Lorsque le seuil est défini à la valeur 2, deux échantillons de seuil consécutifs doivent avoir la valeur vrai pour qu'un événement soit généré.

Ensemble de données

Sélectionnez l'ensemble de données (groupe d'attributs) pour le type de données à échantillonner. Les attributs disponibles qui peuvent être inclus dans la condition proviennent de l'ensemble de données choisi. Si le seuil comporte plusieurs conditions, ces dernières doivent toutes provenir du même ensemble de données.

Pour obtenir une brève description d'un ensemble de données, déplacez la souris sur son nom. Vous pouvez obtenir la description complète de l'ensemble de données et des attributs en cliquant sur le lien "En savoir plus" de l'infobulle. Vous pouvez également cliquer sur l'**Aide** > **Contenu de l'aide** ou sur l'**Aide** > **Documentation** dans la barre de navigation et ouvrir l'aide ou télécharger Le guide de référence de l'agent de surveillance.

Certains agents sont catégorisés comme agents multinoeuds. Ils possèdent des sous-noeuds pour surveiller plusieurs ressources d'agent. Il se pourrait qu'un agent multinoeud dispose d'ensembles de données qui peuvent être utilisés dans un seuil ; toutefois, tout événement ouvert pour le seuil ne s'affiche pas dans le Tableau de bord d'Application Performance. Un message vous notifie de la limitation. De tels événements peuvent être transférés au gestionnaire d'événements IBM Netcool/OMNIbus.

Elément affiché

Facultatif. Pour les ensembles de données à plusieurs lignes uniquement. Lorsqu'une évaluation de ligne ouvre un événement, aucun autre événement ne peut être ouvert pour ce seuil sur le système géré jusqu'à ce que l'événement soit fermé. En sélectionnant un élément affiché, vous autorisez le seuil à continuer l'évaluation des autres lignes dans l'échantillon de données et à ouvrir d'autres événements si d'autres lignes sont qualifiées. En outre, l'élément affiché l'est dans l'onglet **Evénements** du Tableau de bord d'Application Performance pour que vous puissiez facilement distinguer les lignes pour lesquelles des événements ont été ouverts. La liste contient seulement les attributs que vous pouvez désigner comme éléments d'affichage.

Opérateur logique

Ignorez cette zone si votre seuil ne contient qu'une condition. Si vous mesurez plusieurs conditions, sélectionnez l'un des opérateurs suivants avant de cliquer sur **Nouveau** pour ajouter une second, troisième (ou plus) condition :

And (&) si la condition précédente et la condition suivante sont remplies pour que le seuil soit dépassé

Or (|) si une seule de ces conditions doit être remplie pour que le seuil soit dépassé

La combinaison d'opérateurs logiques n'est pas prise en charge. Utilisez tous les opérateurs And ou tous les opérateurs Or. Le seuil peut comporter jusqu'à neuf conditions si l'opérateur Or est utilisé et jusqu'à 10 conditions si l'opérateur And est utilisé.

Si vous utilisez la fonction `Manquant` (décrite plus tard dans la section **Opérateur**), vous ne pouvez utiliser que l'opérateur And dans la formule.

Conditions

La définition de seuil peut inclure logiquement plusieurs seuils ou conditions simultanés.

Cliquez sur **Nouveau** pour ajouter une condition. Sélectionnez une condition et cliquez sur **Editer** pour modifier l'expression ou cliquez sur **Supprimer** pour supprimer l'expression.

Une fois que vous avez cliqué sur **Nouveau** ou **Editer**, renseignez les zones de la boîte de dialogue **Ajouter une condition** ou **Modifier la condition** qui s'ouvre :

☐ **Nombre**

Pour les ensembles de données qui retournent plusieurs lignes pour chaque échantillon de données, vous pouvez comptabiliser chaque ligne qui répond aux critères de la condition. Un événement est ouvert dès que la **Valeur** de comptage est atteinte et que les autres conditions dans la formule sont remplies. Par exemple, si le nombre de processus "zombie" dépasse 10, générez une alerte.

Dans l'exemple suivant, la condition est vraie lorsque plus de 10 lignes sont comptées : **Attribut** Horodatage, **Opérateur** Supérieur à, **Valeur** 10.

Cochez la case **Nombre**, sélectionnez l'**attribut** à comptabiliser, l'**opérateur** relationnelle et la **valeur** de Nombre.

Si la formule comporte plusieurs conditions, chacune doit utiliser l'opérateur booléen **And**. Les fonctions **Nombre** et **Delta heure** sont mutuellement exclusives : si vous cochez la case d'une fonction, l'autre est désactivée. L'attribut ne peut correspondre à un identificateur système, tel que Nom de serveur ou ORIGINNODE, être spécifié comme **Elément affiché** ou provenir d'un ensemble de données pour lequel le seuil ouvre des événements purs.

☐ **Delta heure**

Utilisez la fonction **Delta heure** dans une condition pour comparer l'échantillon d'horodatage (tel que l'heure d'enregistrement) au décalage horaire spécifié.

Une fois que vous avez coché la case **Delta heure**, la zone Delta heure est affichée afin que vous puissiez combiner le signe + (plus) ou - (moins) avec le nombre de jours, d'heures, de minutes ou de secondes. Sélectionnez **Heure d'échantillonnage** ou **Heure spécifique** comme valeur à utiliser dans la comparaison.

Dans l'exemple de journal des événements ci-après, la formule compare l'heure à laquelle l'événement a été consigné à l'horodatage de l'échantillon de données. Si l'événement s'est produit sept jours auparavant, la comparaison est true. Si l'opérateur relationnel était changé en Inférieur ou égal à, la comparaison serait true après 8 jours, 9 jours, etc. :

Attribut : Horodatage
Retardement : -7 jours
Opérateur : Egal à
Valeur : Date de saisie

Attribut
Sélectionnez l'attribut que vous souhaitez comparer dans cette condition. Pour afficher une brève description d'un attribut, déplacez la souris sur son nom dans la liste.

Opérateur
Sélectionnez l'opérateur relationnel pour le type de comparaison :

```
Egal
Différent
Supérieur à
Supérieur ou égal à
Inférieur à
Inférieur ou égal
Regular expression contains
Regular expression does not contain
```

`Regular expression contains` et `Regular expression does not contain` recherchent un critère de concordance dans l'expression. Plus la mise en correspondance d'une chaîne avec l'expression est aisée, plus la charge de travail est efficace au niveau de l'agent. L'expression n'a pas besoin de correspondre à la ligne entière, seulement à la sous-chaîne de l'expression. Par exemple, dans `See him run`, vous voulez savoir si la chaîne contient `him`. Vous pourriez composer l'expression régulière avec `him`, mais vous pourriez également utiliser `.*him.*`. Si vous recherchez `See`, vous pourriez saisir `See`, ou `^See` pour confirmer qu'il se trouve au début de la ligne. La saisie des caractères génériques `.*` est moins efficace et augmente la charge de travail. Pour plus d'informations sur les expressions régulières, consultez la rubrique developerWorks® technical library ou recherchez `regex` dans votre navigateur.

Vous pouvez également sélectionner la fonction `Manquant`, qui compare la valeur de l'attribut spécifié à une liste de valeurs que vous fournissez. La condition prend la valeur True lorsque la valeur ne correspond à aucune valeur de la liste. Cette fonction est utile lorsque vous souhaitez savoir s'il manque quelque chose sur votre système. Conditions et restrictions :

1. L'indicateur sélectionné doit être un attribut de texte : les attributs d'heure et les attributs numériques ne peuvent pas être utilisés.
2. Séparez les valeurs par une virgule (,). Par exemple, `fred,mary,jean`.
3. Vous ne pouvez avoir qu'une seule condition `Manquant` dans un seuil.
4. `Manquant` doit être la dernière condition dans la formule. Si d'autres conditions sont requises, entrez-les avant d'ajouter la fonction Manquant et utilisez uniquement l'opérateur **And (&)** dans la formule. Sinon, toutes les lignes suivantes sont désactivées.

Valeur
Entrez la valeur à comparer en utilisant le format autorisé pour l'indicateur, par exemple, 20 pour 20% ou 120 pour 2 minutes.

Affectation de groupes
Affectez un groupe de ressources de sorte que le seuil soit distribué aux systèmes gérés de même type dans le groupe de ressources. Les groupes de ressources disponibles sont les groupes définis par l'utilisateur pour lesquels vous disposez des droits de modification et les groupes de systèmes (pour le type d'agent) pour lesquels vous disposez des droits d'affichage. Les groupes de systèmes disponibles sont également ceux qui sont adaptés à l'ensemble de données sélectionné.

Un seuil auquel aucun groupe n'est affecté n'est distribué à aucun système surveillé et reste arrêté jusqu'à ce qu'il soit distribué à un groupe de ressources.

Un groupe de systèmes, tel que `Linux OS` ou `Serveur HTTP`, distribue le seuil sur tous les systèmes gérés où cet agent est installé. Par défaut, chaque seuil prédéfini est affecté au groupe de systèmes pour cet agent. (Vous pouvez désactiver tous les seuils prédéfinis dans la page **Configuration avancée**, comme décrit à la section «Activation des seuils», à la page 1106.)

A l'exception des systèmes gérés issus du domaine IBM Tivoli Monitoring : les systèmes gérés issus du domaine Tivoli Monitoring doivent être surveillés et inclure des situations qui ont été distribuées dans votre environnement Tivoli Monitoring.

Pour affecter des groupes au seuil, cochez les cases d'un ou plusieurs groupes de ressources. Si la liste des groupes affectés est longue, vous pouvez sélectionner ☐ **Afficher uniquement les groupes sélectionnés**.

Si vous ne trouvez aucun groupe de ressources auquel vous souhaitez affecter le seuil, vous pouvez sauvegarder la définition de seuil et cliquer sur **OK** lorsque vous êtes invité à confirmer que vous voulez sauvegarder le seuil sans l'affecter à un groupe. Vous pouvez ensuite créer un groupe dans le **gestionnaire de groupes de ressources** et lui affecter un seuil dans l'**Editeur de groupe de ressources**. Pour plus d'informations, voir «Gestionnaire de groupes de ressources», à la page 1008.

Exécution d'une commande

Une fois qu'un événement a été ouvert pour un seuil défini sur true, vous pouvez exécuter automatiquement une commande ou un script de commandes sur le système surveillé pour lequel l'événement a été ouvert. Vous pouvez par exemple vouloir consigner des informations, déclencher un bip audible ou arrêter un travail qui consomme trop ressources.

La commande respecte la syntaxe suivante :

```
&{jeu_données.attribut}
```

où *jeu_données* est le nom du jeu de données et *attribut* est le nom d'attribut tel qu'affiché dans l'éditeur de seuil. Si le jeu de données ou le nom d'attribut contient un espace, remplacez l'espace par un trait de soulignement.

L'exemple suivant montre comment transmettre le paramètre de nom de disque à une ressource gérée :

```
/scripts/clean_logs.sh &{disque_KLZ.nom_disque}
```

Vous pouvez transférer un ou plusieurs attributs depuis le jeu de données. S'ils sont spécifiés, les attributs multiples sont transférés dans la commande dans l'ordre ($1, $2, etc.).

La commande s'exécute à partir de la ligne de commande avec le même compte utilisateur que celui avec lequel l'agent ou le collecteur d'agent a démarré. Par exemple, si l'agent s'exécute en tant que superutilisateur, le superutilisateur exécute la commande sur le système géré.

Les options suivantes contrôlent la fréquence d'exécution de la commande :

Sélectionnez ☐ **Lors du premier événement uniquement** si l'ensemble de données renvoie plusieurs lignes et que vous souhaitez n'exécuter la commande que pour la première occurrence de l'événement dans l'échantillon de données. Décochez cette case pour exécuter la commande pour chaque ligne qui génère un événement.

Sélectionnez ☐ **Pour chaque intervalle vrai consécutif** pour exécuter la commande chaque fois que le seuil est défini sur true. Décochez cette case pour exécuter la commande lorsque le seuil a la valeur true, mais pas une deuxième fois tant que le seuil n'a pas la valeur false, suivi par une autre évaluation true dans un intervalle ultérieur.

Une fois que vous avez cliqué sur **Sauvegarder**, le seuil est appliqué à tous les systèmes gérés dont le type de données est le même dans les groupes de ressources affectés.

Conseil : Vous pouvez contrôler le comportement de transmission des événements à l'aide des options du **Gestionnaire d'événements** dans la page **Configuration avancée**. Voir «Configuration avancée», à la page 1104 .

Remarque : Pour afficher la liste des attributs qui conviennent à l'inclusion dans la définition de seuil, créez une table avec le fichier que vous prévoyez d'utiliser. .

Concepts associés

«Informations de référence», à la page 1004
Examinez les informations de référence pour en savoir plus sur les seuils, les seuils prédéfinis pour les agents, les groupes de ressources auxquels ils sont affectés et la personnalisation des seuils.

Tâches associées

«Tutoriel : Définition d'un seuil», à la page 1010

«Tutoriel : Définition d'un seuil pour exécuter une commande sur la ressource gérée», à la page 1013
Vous pouvez utiliser l'**éditeur de seuil** pour transmettre certains paramètres aux agents. Vous avez la possibilité de spécifier les commandes ou un script des commandes qui s'exécuteront automatiquement lors du déclenchement d'un événement.

«Intégration à Netcool/OMNIbus», à la page 992
Vous pouvez réacheminer les événements de IBM Cloud Application Performance Management vers votre gestionnaire d'événements IBM Tivoli Netcool/OMNIbus sur site.

Personnalisation d'un événement à transmettre à un récepteur EIF

Vous pouvez personnaliser les événements de seuil envoyés à un récepteur Event Integration Facility (EIF), tel que Netcool/OMNIbus ObjectServer, à Cloud Event Management ou à Alert Notification. Utilisez la fenêtre **Personnalisation de l'attribut EIF** pour personnaliser le contenu des événements transmis aux destinations d'événement et remplacer ainsi le mappage par défaut. Vous pouvez créer des définitions de mappe pour les événements de seuil envoyés au récepteur Event Integration Facility. Utilisez la fenêtre **Personnalisation de l'attribut EIF** pour personnaliser la façon dont les événements sont mappés aux événements EIF transmis et remplacer ainsi le mappage par défaut. En personnalisant le modèle de message, vous pouvez ajouter des informations sur le problème identifié par l'événement et les données spécifiques de l'événement.En personnalisant le modèle de message, vous pouvez ajouter des informations sur le problème identifié par l'événement et inclure des données spécifiques de l'événement.

Pourquoi et quand exécuter cette tâche

Vous pouvez personnaliser l'emplacement de base EIF. Cet emplacement **msg** prédéfini envoie la formule de seuil à une destination d'événement. Vous pouvez également ajouter un ou plusieurs emplacements personnalisés EIF à l'événement. Si vous utilisez Netcool/OMNIbus ObjectServer, vous devez mettre à jour le fichier de règles d'analyse EIF et les déclencheurs d'ObjectServer si vous souhaitez que les emplacements personnalisés s'affichent dans l'interface utilisateur Netcool/OMNIbus.

Vous pouvez personnaliser l'emplacement de base de la fonction d'intégration d'événements (EIF), qui est un emplacement **msg** prédéfini envoyant la formule de seuil au récepteur EIF. Vous pouvez également ajouter un ou plusieurs attributs personnalisés de la fonction d'intégration d'événements, ce qui requiert une mise à jour du récepteur EIF et des fichiers de règles de sonde.

Procédure

Pour personnaliser le mappage des événements du seuil actuel aux événements transmis, procédez comme suit :

1. Si le **Gestionnaire de seuils** n'est pas ouvert, cliquez sur **Configuration du système** > **Gestionnaire de seuils**.
2. Cliquez sur la zone de liste **Type de source de données**, puis sélectionnez le type de données à utiliser.
3. S'il s'agit d'un nouveau seuil, cliquez sur **Nouveau** ; sinon, sélectionnez un seuil et cliquez sur **Editer**.

4. Pour personnaliser le mappage des événements de ce seuil aux événements transmis, vérifiez que **EIF Forwarder** est défini sur Yes, cliquez sur **Personnalisation de l'attribut EIF**, puis effectuez l'une des étapes suivantes :
   - **Attributs EIF de base** : pour personnaliser l'emplacement de base, sélectionnez le bouton d'option de **msg** et cliquez sur **Editer**.
   - **Attributs EIF personnalisés** : pour ajouter un emplacement personnalisé, cliquez sur **Ajouter** : pour éditer un emplacement personnalisé, sélectionnez le bouton d'option de l'emplacement et cliquez sur **Editer**.

   La fenêtre **Editer un attribut** ou **Ajouter un attribut** s'ouvre.
5. Renseignez les zones pour personnaliser les valeurs d'emplacement :

Zone	Description	Restriction
Slot name	Nom de l'emplacement de la fonction d'intégration d'événements personnalisé, qui doit commencer par un caractère.	L'emplacement de base de la fonction d'intégration d'événements est **msg** et ne peut pas être modifié.
Slot type	Type d'emplacement personnalisé de la fonction d'intégration d'événements : **String Type** ou **Number Type**.	L'emplacement de base de la fonction d'intégration d'événements est **String Type** et ne peut pas être modifié.
Subtype	Valeur affectée à l'emplacement, qui correspond au type d'emplacement : • **Mapped attribute** active la zone **Mapped attribute** pour ajouter la valeur de l'attribut sélectionné au moment où l'événement se produit • **Literal Value** active la zone **Literal value** pour ajouter du texte au modèle de message • **Literal Value + Mapped Attribute** active les zones **Literal value** et **Mapped attribute** pour ajouter du texte et des valeurs d'attribut au modèle de message et active le bouton **Ajouter** pour ajouter plusieurs valeurs de texte et/ou d'attribut. Un espace est ajouté après chaque valeur littérale ou attribut. Une utilisation type de l'emplacement de base de la fonction d'intégration d'événements **msg** consiste à spécifier une combinaison **Literal Value + Mapped Attribute** pour le modèle de message.	Un emplacement **Number Type** ne peut utiliser que **Mapped Attribute**.
Ajouter	Si vous souhaitez envoyer plusieurs valeurs littérales ou valeurs d'attribut dans le message transmis, cliquez sur **Ajouter** pour ajouter un autre ensemble de zones **Literal value** et **Mapped attribute**. Chaque fois que vous sélectionnez **Ajouter**, ces zones sont ajoutées au panneau. Pour supprimer un ensemble de zones **Literal value** et **Mapped attribute**, effacez le contenu de ces zones avant de cliquer sur **OK**. Voir Exemple.	Activée uniquement si la valeur de **Subtype** est **Literal Value + Mapped Attribute**. Six ensembles de zones **Literal value** et **Mapped attribute** au maximum. Si vous ne parvenez pas à voir les zones que vous avez ajoutées, utilisez la fonction de zoom arrière du navigateur (Ctrl -) pour

Zone	Description	Restriction
		réduire la présentation à la taille de la boîte de dialogue.
Literal value	Texte à inclure dans le modèle de message. Par exemple, la valeur littérale `L'utilisation de la mémoire est élevée à ` , associée à l'attribut mappé **`Utilisation de la mémoire (%)`**, se présente dans l'interface utilisateur **Gestionnaire d'événements** sous la forme `L'utilisation de la mémoire est élevée à 97,3 %`. Le modèle de message se compose du texte du message fixe et de références de substitution de variable ou de symboles. Le symbole fait référence à des données d'emplacement commun ou d'événement ou à une référence spéciale à la formule de seuil. Les emplacements communs correspondent aux emplacements inclus dans tous les événements transmis, tels que *threshold_name* ; les emplacements d'événement correspondent aux emplacements spécifiques au seuil `msg`.	Désactivée si la valeur de **Subtype** est **`Mapped Attribute`**.
Mapped attribute	Attribut dont vous souhaitez ajouter la valeur au modèle de message. Les attributs disponibles proviennent de l'ensemble de données sélectionné pour le seuil. Par exemple, pour un seuil qui surveille les temps de processeur élevés, vous pouvez mapper l'attribut de pourcentage du temps utilisateur.	Six zones **Mapped attribute** au maximum. Désactivée si la valeur de **Subtype** est **`Literal Value`**. Si la valeur de **Slot type** est **`Number Type`**, seuls les attributs numériques sont disponibles.
Multiplier	Le multiplicateur correspond à la valeur définie une fois que vous avez personnalisé la valeur numérique d'origine de l'attribut mappé par un multiplicateur : valeur de l'emplacement = *attribute1* * *n*. Par exemple, pour convertir les minutes en secondes dans l'événement de la fonction d'intégration d'événements, indiquez un multiplicateur de 60. La valeur du multiplicateur peut être une fraction, exprimée sous forme de valeur décimale, telle que 0.5 ou 5.4.	Activée uniquement pour les attributs numériques (**Slot type** est **`Number Type`**).

Une fois que vous avez cliqué sur **OK** pour fermer la fenêtre, la fenêtre **Personnalisation de l'attribut EIF** répertorie le nom d'emplacement et indique s'il est personnalisé.

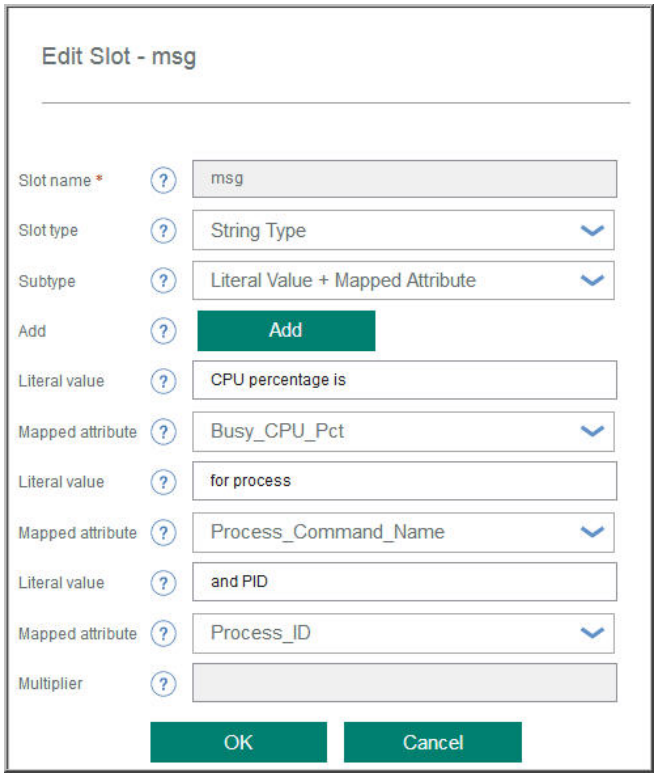
6. Une fois que vous avez terminé d'éditer l'emplacement de base de la fonction d'intégration d'événements ou d'ajouter, de supprimer ou d'éditer des emplacements personnalisés de la fonction d'intégration d'événements pour le seuil, cliquez sur **OK**.
7. Après avoir modifié le seuil, cliquez sur **Sauvegarder**.

   Pour plus d'informations, voir «Gestionnaire de seuils», à la page 1014.

Exemple

Le seuil `Linux_BP_ProcHighCpu_Critical` vérifie si la consommation d'unité centrale est supérieure ou égale à 95 %. Pour ajouter le pourcentage d'unité centrale occupée, le nom de commande du

processus et l'ID processus au message récapitulatif, (contenu dans l'emplacement msg), l'emplacement msg a été personnalisé avec trois ensembles de zones **Literal value** et **Mapped attribute** :



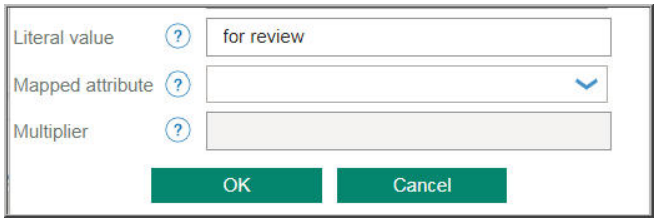
Le modèle de message se présente comme suit :

```
CPU percentage is Busy_CPU_Pct for process Process_Command_Name and PID Process_ID
```

Le message résultant affiché dans Event Manager peut se présenter comme suit :

```
CPU percentage is 97 for process large.exe and PID 9876
```

Vous pouvez également ajouter les zones **Literal value** et **Mapped attribute** et laisser une zone vide. Par exemple, pour ajouter "for review" au modèle de message, cliquez sur **Ajouter** et entrez `for review` pour **Literal value**.



Le modèle de message se présente maintenant comme suit :

```
CPU percentage is Busy_CPU_Pct for process Process_Command_Name and PID Process_ID for review
```

Le message résultant affiché dans **Event Manager** peut se présenter comme suit :

```
CPU percentage is 96 for process big.exe and PID 5432 for review
```

Que faire ensuite

Si vous avez créé des attributs personnalisés de la fonction d'intégration d'événements, vous devez identifier les nouveaux attributs dans la table `alerts.status` sur votre serveur d'objets Netcool/OMNIbus, puis mettre à jour le fichier de configuration `itm_apm_event.rules` qui a été installé au cours de l'intégration de Netcool/OMNIbus avec Cloud APM.

Ajout d'attributs personnalisés EIF à la base de données du serveur d'objets Netcool/OMNIbus

Lorsque vous ajoutez de nouveaux attributs personnalisés EIF pour les seuils, vous devez les identifier dans votre récepteur EIF pour pouvoir afficher les événements transmis qui les utilisent. Si Netcool/

OMNIbus est intégré à Cloud APM, mettez à jour la table `alerts.status` pour définir les nouveaux attributs.

Pourquoi et quand exécuter cette tâche

Lorsque vous avez configuré l'intégration de Netcool/OMNIbus à Cloud APM, à l'étape «4», à la page 996, vous avez chargé `itm_apm_db_update.sql`. La procédure ci-après exige que vous utilisiez l'interface interactive SQL pour mettre à jour la table `alerts.status` dans la base de données `itm_apm_db_update.sql`.

Procédure

Suivez cette procédure sur le serveur d'objets Netcool/OMNIbus pour définir les nouveaux attributs personnalisés EIF que vous avez créés dans l'**éditeur de seuils** :

1. Démarrez l'interface interactive SQL pour modifier la base de données :

   Linux

   ```
   $OMNIHOME/bin/nco_sql -user nom_utilisateur -password mot_de_passe
   -server nom_serveur > itm_apm_db_update.sql
   ```

   Exemple :

   ```
   $OMNIHOME/bin/nco_sql -user smadmin -password passw0rd -server NCOMS >
   /tmp/apm/itm_apm_db_update.sql
   ```

   Windows

   ```
   itm_apm_db_update.sql | %OMNIHOME%\..\bin\isql -U nom_utilisateur
   -P mot_passe -S nom_serveur
   ```

   Exemple :

   ```
   \temp\apm\itm_apm_db_update.sql | %OMNIHOME%\..\bin\isql -U smadmin
   -P passw0rd -S NCOMS
   ```

2. Pour chaque emplacement EIF personnalisé, entrez la commande SQL **ALTER TABLE** avec le nom d'emplacement personnalisé et le type d'emplacement au format suivant, appuyez sur la touche Entrée, puis entrez go et appuyez sur Entrée :

   - Pour un type d'attribut chaîne,

     ```
     alter table alerts.status add nom_attribut_personnalisé varchar(512);
     ```

   - Pour un type d'attribut numérique,

     ```
     alter table alerts.status add nom_attribut_personnalisé integer;
     ```

   où *nom_attribut_personnalisé* est le nom de l'attribut personnalisé EIF tel qu'il a été entré dans la zone **slotName** de la fenêtre **Ajouter un attribut** dans l'**éditeur de seuils**.

Exemple

L'exemple présente les commandes **alter table** permettant d'ajouter les attributs personnalisés **BusinessApplication** et **GenericMetric**.

```
alter table alerts.status add BusinessApplication varchar(512);
```

```
alter table alerts.status add GenericMetric integer;
```

Que faire ensuite
Mettez à jour le fichier de configuration `itm_apm_event.rules` qui a été installé dans le cadre de l'intégration de Netcool/OMNIbus à Cloud APM. Pour plus d'informations, voir «Ajout d'attributs personnalisés EIF aux règles d'événement de récepteur EIF», à la page 1024.

Ajout d'attributs personnalisés EIF aux règles d'événement de récepteur EIF

Si vous avez défini de nouveaux attributs personnalisés EIF pour les seuils, vous devez mettre à jour le fichier de règles pour identifier ces nouveaux attributs auprès du récepteur EIF.

Pourquoi et quand exécuter cette tâche

Ces étapes vous amènent à mettre à jour le fichier `itm_apm_event.rules` dans Probe for Tivoli EIF Netcool/OMNIbus afin d'identifier chaque nouvel attribut personnalisé EIF. Si vous utilisez un autre récepteur EIF, mettez à jour les fichiers de règles comme l'exige le récepteur.

Procédure

1. Sur le système où Probe for Tivoli EIF est installé, accédez au répertoire d'installation.

   Linux cd *rép_install*`/tivoli/netcool/omnibus/probes/linux2x86`

   Windows cd *rép_install*`\Tivoli\Netcool\omnibus\probes\win32`

   où *rép_install* est le répertoire par défaut `/opt/IBM/` ou `C:\IBM\` ou le répertoire que vous avez indiqué lors de l'installation de la sonde.
2. Effectuez une copie de sauvegarde du fichier `itm_apm_event.rules`.
3. Ouvrez le fichier Probe for Tivoli EIF `itm_apm_event.rules` dans un éditeur de texte.

   Le fichier se compose de trois parties que vous modifiez pour ajouter le(s) attribut(s) personnalisé(s) EIF que vous avez créé(s).
4. Ajoutez les instructions **`if`** avec une nouvelle instruction pour chaque attribut personnalisé EIF qui utilise le format suivant :

   ```
   if(exists($nom_attribut_personnalisé))
   {
       if(regmatch($nom_attribut_personnalisé, "^'.*'$"))
       {
           $SourceType = extract($nom_attribut_personnalisé, "^'(.*)'$")
       }
   }
   ```

   où *nom_attribut_personnalisé* est le nom de l'attribut personnalisé EIF tel qu'il a été entré dans la zone **slotName** de la fenêtre **Ajouter un attribut**.
5. Ajoutez la liste des entrées `@` avec une nouvelle ligne pour chaque attribut personnalisé EIF qui utilise le format suivant :

   ```
   @nom_attribut_personnalisé=$nom_attribut_personnalisé
   ```

   où *nom_attribut_personnalisé* est le nom de l'attribut personnalisé EIF.
6. Ajoutez la liste des entrées `$tmpEventData` avec une nouvelle ligne pour chaque attribut personnalisé EIF qui utilise le format suivant :

   ```
   $tmpEventData = nvp_remove( $tmpEventData, "nom_attribut_personnalisé")
   ```

   où *nom_attribut_personnalisé* est le nom de l'attribut personnalisé EIF.
7. Sauvegardez et fermez le fichier `itm_apm_event.rules`.
8. Redémarrez Probe for Tivoli EIF pour implémenter vos mises à jour.

Résultats
Le fichier de règles est mis à jour et Probe for Tivoli EIF peut maintenant traiter les événements de seuil qui utilisent les nouveaux attributs personnalisés EIF et transmettent les détails des événements au serveur d'objets Netcool/OMNIbus.

Exemple

Voici un extrait du fichier `itm_apm_event.rules` une fois qu'il a été modifié dans le but d'ajouter ces attributs personnalisés EIF : **`BusinessApplication`** et **`GenericMetric`** (en italique).

```
# ------------------------------------------------------------
    if(exists($SourceID))
    {
        if(regmatch($SourceID, "^'.*'$"))
        {
            $SourceID = extract($SourceID, "^'(.*)'$")
        }
    }
    ...
    ...
    ...
    if(exists($ManagedSystemGroups))
    {
        if(regmatch($ManagedSystemGroups, "^'.*'$"))
        {
            $SourceType = extract($ManagedSystemGroups, "^'(.*)'$")
        }
    }
    if(exists($BusinessApplication))
    {
        if(regmatch($BusinessApplication, "^'.*'$"))
        {
            $SourceType = extract($BusinessApplication, "^'(.*)'$")
        }
    }
     if(exists($GenericMetric))
    {
        if(regmatch($GenericMetric, "^'.*'$"))
        {
            $SourceType = extract($GenericMetric, "^'(.*)'$")
        }
    }

 @SourceID=$SourceID
 @URL=$ManagementURL
 @Service=$Service
 @SourceType=$SourceType
 @SubscriberID=$TenantID
 @APMHostname=$apm_hostname
 @ManagedSystemGroups=$ManagedSystemGroups
 @BusinessApplication=$BusinessApplication
 @GenericMetric=$GenericMetric

 # ------------------------------------------------------------------
 # -  RTC 66157
 # ------------------------------------------------------------------
 if ( exists ( $appl_label ) )
 {
    if ( match($appl_label, "PI:A:S"))
    {
        @Class = 87723
    }
 }
 # ------------------------------------------------------------------
 # -  RTC 48775 - APM FP5 agents do not populate data in email of EMaaS Basic
 # ------------------------------------------------------------------
 if (match( $situation_eventdata, "~" ) )
 {
    # Dump all fields into the ITMEventData field
    $tmpEventData = nvp_add($*)
    # Remove the duplicated fields
    $tmpEventData = nvp_remove( $tmpEventData, "appl_label")
    $tmpEventData = nvp_remove( $tmpEventData, "control")
    ...
    ...
    ...
    $tmpEventData = nvp_remove( $tmpEventData, "ManagedSystemGroups")
    $tmpEventData = nvp_remove( $tmpEventData, "EventSeqNo")
```

```
    $tmpEventData = nvp_remove( $tmpEventData, "BusinessApplication")
    $tmpEventData = nvp_remove( $tmpEventData, "GenericMetric")
       @ITMEventData = $tmpEventData
```

Envoi d'un courrier électronique en réponse à un événement

Si votre environnement géré comprend IBM Alert Notification, vous pouvez proposer la notification par courrier électronique lorsque les performances de l'application dépasse les seuils.

Pourquoi et quand exécuter cette tâche

Pour configurer la notification par courrier électronique, vous devez activer la fonctionIBM Alert Notification, tel que décrit dans Ensemble de rubriques Alert Notification dans l'IBM Knowledge Center. Ajoutez ensuite l'application surveillée aux groupes de ressources. Pour chaque groupe de ressources, vous pouvez configurer une ou plusieurs adresses électroniques. Lorsque les performances d'une application dans un groupe dépasse un seuil, vous obtenez une notification par courrier électronique aux adresses configurées pour le groupe.

Procédure

1. Cliquez sur **Configuration système** > **Gestionnaire de groupes de ressources**.
2. Cliquez sur **Nouveau** pour créer un groupe de ressources pour lequel vous souhaitez configurer la notification par courrier électronique, ou sélectionnez un groupe existant et cliquez sur **Editer**. L'**éditeur de groupe de ressources** s'ouvre.
3. Cliquez sur **Configurer la notification par courrier électronique** pour ouvrir l'application IBM Alert Notification dans un nouvel onglet ou une nouvelle fenêtre de navigation. Utilisez Alert Notification pour créer des utilisateurs et associer leurs adresses électroniques à des groupes de ressources pour que ceux-ci reçoivent des notifications d'événements par courrier électronique.

Utilisation de l'API Resource Group Management Service

Utilisez l'API Resource Group Management Service pour gérer le cycle de vie des groupes de systèmes gérés à partir de la ligne de commande.

Pourquoi et quand exécuter cette tâche

Effectuez des tâches de groupe de ressources telles que la création, l'affichage, la mise à jour et la suppression de groupes de systèmes gérés. Ajoutez et supprimez des systèmes individuels dans les groupes personnalisés. Affichez une liste des systèmes que vous avez ajoutés à un groupe de ressources personnalisées spécifique et qui sont automatiquement ajoutés aux groupes intégrés tels que le groupe de ressources système.

Vous pouvez créer des scripts d'automatisation de tâches telles que la définition de groupes de ressources et l'affectation d'agents à ces groupes. Les groupes de ressources peuvent être des cibles de distributions de seuil et/ou des stratégies de contrôle d'accès.

Les opérations suivantes sont décrites dans l'Explorateur d'API et dans la section Exemple qui se trouve à la fin de cette rubrique.

- Renvoyer tous les groupes de ressources ou agents, ou un groupe de ressources ou un agent donné.
- Créer un groupe de ressources personnalisées ou mettre à jour la définition d'un groupe existant.
- Supprimer un groupe de ressources personnalisées spécifié.
- Ajouter des agents à un groupe de ressources personnalisées.
- Supprimer des agents d'un groupe de ressources personnalisées.

Procédure

Pour définir et modifier des groupes de ressources personnalisées à l'aide de l'API Resource Group Management Service, procédez comme suit. Les agents et groupes de ressources système ne peuvent pas être modifiés.

1. Effectuez les étapes 1 à 9 décrites dans la rubrique Exploration des API.

   L'étape 10 et l'étape 11 fournissent des détails supplémentaires.
2. Cliquez sur **USE** et sélectionnez une clé (**Key1** par exemple).

   Remarque : cliquez sur **Masquer** pour afficher votre ID client et votre secret client. Relevez-les car vous en aurez besoin si vous effectuez des appels d'API avec des outils externes en dehors de l'Explorateur d'API. Cliquez ensuite sur **Afficher** pour les masquer.
3. Renseignez tous les en-têtes requis (signalés par un astérisque).

   L'en-tête X-IBM-Service-Location
   * correspond à l'emplacement géographique de votre abonnement (par exemple, na pour l'Amérique du Nord).

   Autorisation
   * correspond à votre chaîne codée en base64 de l'ID IBM et du mot de passe. Lorsque vous codez l'ID IBM et le mot de passe dans l'outil based64-encoder, le format doit être *IBMid:password*. Par exemple, `Basic YXBtYWRtaW46YXBtcGFzcw==!`.
4. Vous devez inclure un en-tête de référenceur dans toutes les demandes POST, PUT et DELETE. La valeur de l'en-tête de référenceur est toujours :

   ```
   -H 'Referer: https://api.ibm.com'
   ```
5. Faites défiler l'écran pour rechercher **Test** et cliquez dessus.

Résultats

Les modifications que vous apportez aux groupes de ressources personnalisées dans l'API entrent en vigueur immédiatement et sont affichées dans le **Gestionnaire de groupes de ressources** (voir «Gestionnaire de groupes de ressources», à la page 1008).

Exemple

Cette commande renvoie les noms, les identificateurs uniques, le statut, le nom d'hôte, la version et le type d'agent pour tous les agents :

```
GET /1.0/topology/mgmt_artifacts?_filter=entityTypes=Agent&_field=keyIndexName&
_field=online&_field=hostname&_field=version&_field=productCode&_field=description
```

Cette commande renvoie une liste de tous les agents de système d'exploitation Linux :

```
GET /1.0/topology/mgmt_artifacts?_filter=entityTypes=Agent&_filter=description=
"Linux OS"&_field=keyIndexName
```

Cette commande renvoie une liste des groupes de systèmes et des groupes personnalisés :

```
GET /1.0/topology/mgmt_artifacts?_filter=entityTypes:AgentGroup,
AgentSystemGroup&_field=keyIndexName&_field=displayLabel
```

Cette commande renvoie la liste des agents affectés à un groupe présentant l'identificateur unique {id} :

```
GET /1.0/topology/mgmt_artifacts/{id}/references/to/contains
```

L'exemple suivant utilise la commande curl pour créer un groupe personnalisé.

```
POST /1.0/topology/mgmt_artifacts
```

Remarque : Le corps de la requête POST doit contenir un objet JSON qui définit le groupe tel qu'indiqué par le paramètre **-d**.

```
curl -X POST \
  https://api.ibm.com/perfmgmt/run/1.0/topology/mgmt_artifacts \
  -H 'Referer: https://api.ibm.com' \
  -H 'authorization: Basic REPLACE_BASE64_ENCODED_STRING' \
  -H 'content-type: application/json' \
  -H 'x-ibm-client-id: REPLACE_KEY_VALUE' \
  -H 'x-ibm-client-secret: REPLACE_KEY_VALUE' \
  -d '{
  "keyIndexName": "customGroup",
  "description": "Description du groupe personnalisé",
  "displayLabel": "customGroupLabel",
  "entityTypes": [
    "AgentGroup"
  ],
  "arbitraryStringProperty": "Your custom property value"
}'
```

Cette commande ajoute un agent avec l'identificateur unique {otherid} à un groupe personnalisé présentant l'identificateur unique {id} :

```
POST /1.0/topology/mgmt_artifacts/{id}/references/to/contains/{otherid}
```

Cette commande supprime un agent avec l'identificateur unique {otherid} d'un groupe personnalisé présentant l'identificateur unique {id} :

```
DELETE /1.0/topology/mgmt_artifacts/{id}/references/to/contains/{otherid}
```

Utilisation de l'API Threshold Management Service

Utilisez l'API Threshold Management Service pour gérer le cycle de vie de la surveillance des seuils à partir de la ligne de commande.

Pourquoi et quand exécuter cette tâche

Effectuez des tâches du gestionnaire de seuils telles que la création, l'affichage, la mise à jour et la suppression de seuils. Affectez des groupes de ressources à ces seuils. Affichez une liste de l'ensemble des seuils et des affectations de ressources. Affichez une liste de tous les seuils affectés à un groupe de ressources donné.

Vous pouvez créer des scripts d'automatisation de tâches telles que la définition de seuils et l'affectation de ces derniers à des groupes de ressources.

Les opérations suivantes sont décrites dans l'Explorateur d'API et dans la section Exemple qui se trouve à la fin de cette rubrique.

- Renvoyer tous les seuils ou obtenir un seuil spécifique. Vous pouvez filtrer la demande avec ces attributs : **label**, qui correspond au nom de seuil, **_appliesToAgentType**, qui correspond à un code produit de 2 caractères, et **_uiThresholdType**, qui correspond au type de seuil qui est affiché dans les pages Gestionnaire de seuils et Editeur de groupe de ressources de la console Cloud APM. Vous pouvez utiliser **_offset** ou **_limit** lorsque vous obtenez les seuils
- Créer un seuil ou mettre à jour la définition d'un seuil existant. Vous devez inclure l'en-tête X-HTTP-Method-Override réglé sur PATCH pour la demande de mise à jour
- Supprimer un seuil spécifié
- Renvoyer toutes les affectations de ressources ou une affectation de ressource spécifique qui montre les seuils affectés à chaque groupe de ressources. Vous pouvez filtrer la demande avec ces attributs : **resource._id** et **threshold._id** ; et utilisez ces opérateurs **=** (égal) et **!=** (non égal) pris en charge
- Créer une affectation de ressources qui affecte un seuil unique à un groupe de ressources unique
- Supprimer une affectation de ressources, ce qui supprime un seuil unique à partir d'un seul groupe de ressources

Procédure

1. Effectuez les étapes 1 à 9 décrites dans la rubrique Exploration des API.
   L'étape 10 et l'étape 11 fournissent des détails supplémentaires.
2. Cliquez sur **USE** et sélectionnez une clé (**Key1** par exemple).

   Remarque : cliquez sur **Masquer** pour afficher votre ID client et votre secret client. Relevez-les car vous en aurez besoin si vous effectuez des appels d'API avec des outils externes en dehors de l'Explorateur d'API. Cliquez ensuite sur **Afficher** pour les masquer.
3. Renseignez tous les en-têtes requis (signalés par un astérisque).

   L'en-tête X-IBM-Service-Location
   * correspond à l'emplacement géographique de votre serveur (par exemple, na pour l'Amérique du Nord).

   L'en-tête Autorisation
   * correspond à votre chaîne codée en base64 de l'ID IBM et du mot de passe. Lorsque vous codez l'ID IBM et le mot de passe dans l'outil based64-encoder, le format doit être *IDIBM:mot de passe*. Par exemple, `Basic YXBtYWRtaW46YXBtcGFzcw==!`.
4. Faites défiler l'écran pour rechercher **Test** et cliquez dessus.

Exemple

Cette commande renvoie tous les seuils qui sont inscrits sur le serveur :

```
GET /threshold_types/itm_private_situation/thresholds
```

Cette commande renvoie les informations pour le seuil avec l'étiquette (nom) `Mon_seuil`.

```
GET /threshold_types/itm_private_situation/thresholds?_filter=label%3DMon_seuil
```

Cette commande renvoie tous les seuils pour le type d'agent LZ, qui est le code composant pour l'Linux OS.

```
GET /threshold_types/itm_private_situation/thresholds?_filter=_appliesToAgentType%3DLZ
```

Cette commande a la même sortie que la commande précédente, mais le nom de l'agent est donné tel qu'il apparaît dans la console Cloud APM.

```
GET /threshold_types/itm_private_situation/thresholds?_filter=_uiThresholdType%3DLinux OS
```

Cette commande renvoie tous les groupes de ressources auxquels le seuil 123 est affecté :

```
GET /resource_assignments?_filter=threshold._id=123
```

L'exemple suivant utilise la commande curl pour créer un seuil.

```
POST /1.0/thresholdmgmt/threshold_types/itm_private_situation/thresholds
```

A faire : Le corps de la requête POST doit contenir un objet JSON qui définit le seuil tel qu'indiqué par le paramètre **-d**. Exemple :

```
curl -X POST\
 https://api.ibm.com/perfmgmt/run/1.0/thresholdmgmt/threshold_types/itm_private_situation/
thresholds  \
  -H 'authorization: Basic REPLACE_BASE64_ENCODED_STRING' \
  -H 'content-type: application/json' \
  -H 'x-ibm-client-id: REPLACE_KEY_VALUE' \
  -H 'x-ibm-client-secret: REPLACE_KEY_VALUE' \
  -d '{
  "label": "Nom_de_votre_seuil_Linux",
  "description": "Définition de votre seuil Linux",
  "configuration": {
    "type": "json",
    "payload": {
```

```
      "formulaElements": [
        {
          "function": "*MKTIME",
          "metricName": "KLZ_CPU.Timestamp",
          "operator": "*EQ",
          "threshold": "1455767100000",
          "timeDelta": {
            "operator": "+",
            "delta": "3",
            "unit": "Hours"
          }
        }
      ],
      "period": "011500",
      "periods": "3",
      "severity": "Fatal",
      "matchBy": "KLZCPU.CPUID",
      "operator": "*OR",
      "actions": [
        {
          "name": "command",
          "command": "ps -ef",
          "commandFrequency": "Y",
          "commandWhen": "Y",
          "commandWhere": "N"
        }
      ]
    }
  }
}'
```

Gestion des accès utilisateur

Utilisez les fonctions Contrôle d'accès basé sur les rôles de Cloud APM pour octroyer aux utilisateurs les droits d'accès dont ils ont besoin pour effectuer leur rôle.

La sécurité dans Cloud APM est basée sur les rôles. Un rôle est un groupe de droits d'accès qui contrôle les actions que vous pouvez effectuer dans Cloud APM. Vous pouvez créer des rôles personnalisés dans Cloud APM. Vous pouvez affecter des droits à des rôles personnalisés ou davantage de droits aux rôles par défaut existants. Vous pouvez affecter des utilisateurs et des groupes d'utilisateurs à des rôles par défaut existants ou à des rôles personnalisés. Vous pouvez affecter des utilisateurs et des groupes d'utilisateurs à plusieurs rôles. Les droits sont cumulatifs, un utilisateur ou un groupe est affecté à tous les droits de tous les rôles auxquels il est affecté.

L'authentification des utilisateurs dans Cloud APM est gérée par l'intermédiaire de IBM Marketplace ou peut l'être via Collaborative Operations si vous possédez un abonnement.

L'authentification des utilisateurs dans Performance Management nécessite un IBMid. Créez une identité IBM en sélectionnant le lien **Créer une identité IBM** sur la page **Se connecter à IBM**. Pour accéder à la page **Se connecter à IBM**, accédez à la page **Products and Services** (http://ibm.biz/my-prodsvcs) sur IBM Marketplace pour être redirigé vers la page **Se connecter à IBM** (vous devrez peut-être vous déconnecter et revenir à la page **Products and Services** (http://ibm.biz/my-prodsvcs)).

Dès lors que vous possédez une identité IBM, vous pouvez ouvrir une session sur Cloud APM directement ou à partir de Produits et services. L'autorisation d'accéder à une instance de Cloud APM est gérée par **Products and Services** ou par le biais de Collaborative Operations si vous possédez un abonnement. Par défaut, l'utilisateur qui demande un essai ou achète un abonnement a des privilèges d'administrateur.

Le propriétaire de l'abonnement Cloud APM correspond à l'utilisateur par défaut dans Cloud APM. Il s'agit de l'utilisateur qui demande un essai ou souscrit un abonnement. Cet utilisateur par défaut est membre du rôle Administrateur des rôles et a des privilèges d'administrateur qui lui permettent d'ajouter de nouveaux utilisateurs. Les utilisateurs qui suivent sont ajoutés par défaut au rôle Utilisateur de surveillance.

Si vous n'êtes pas membre d'un rôle et que vous essayez de vous connecter à Cloud APM, le message **Non autorisé** apparaît.

Pour ajouter un utilisateur Cloud APM :

1. Accédez à **Products and Services** sur IBM Marketplace, puis développez le widget **IBM Performance Management**.
2. Cliquez sur **Manage Authorizations**, puis entrez une identité IBM ou une adresse e-mail dans les zones **Add new user** ou **Search existing users**. Cliquez sur **Add user** pour ajouter l'utilisateur.

Le nombre d'utilisateurs que vous pouvez ajouter à un abonnement Cloud APM n'est pas limité.

Remarque : Les groupes d'utilisateurs ne sont pas pris en charge dans Cloud APM.

Pour plus d'informations sur les rôles, voir «Rôles et droits», à la page 1031.

Rôles et droits

Un *rôle* est un groupe de droits qui contrôle les actions que vous pouvez effectuer dans Cloud APM. Utilisez la page Contrôle d'accès à base de rôles pour gérer les utilisateurs et les rôles ou utilisez l'API d'autorisation pour effectuer des tâches de contrôle d'accès basé sur les rôles à partir de la ligne de commande.Pour plus d'informations, voir «Exploration des API», à la page 1103.

Cloud APM possède quatre rôles par défaut :

Administrateur de rôles
Ce rôle est destiné aux utilisateurs dont la fonction principale est de créer des règles de contrôle d'accès pour Cloud APM. Ce rôle possède tous les droits. Si vous modifiez l'utilisateur par défaut, le nouvel utilisateur par défaut est automatiquement membre du rôle Administrateur des rôles. Ce rôle ne peut pas être édité. Les administrateurs de rôles ne peuvent pas se supprimer eux-mêmes du rôle Administrateur des rôles. Cette restriction supprime le risque de supprimer accidentellement tous les utilisateurs du rôle Administrateur des rôles.

Administrateur de surveillance
Ce rôle est destiné aux utilisateurs dont la fonction principale est d'utiliser Cloud APM pour surveiller les systèmes. Les administrateurs de surveillance effectuent des tâches telles que l'ajout d'applications de surveillance, la création de seuils, l'ajout de groupes de ressources et la distribution des seuils à ces groupes de ressources. Ce rôle peut être édité.

Administrateur système
Ce rôle est destiné aux utilisateurs dont la fonction principale est d'effectuer des tâches d'administration pour le système Cloud APM. Les administrateurs système effectuent des tâches telles que la configuration du gestionnaire d'événements ou la configuration de la passerelle hybride. Ce rôle peut être édité.

Utilisateur de surveillance
Ce rôle est destiné aux utilisateurs dont la fonction principale est de configurer et gérer la santé et l'état des systèmes surveillés par Cloud APM. Ce rôle peut être édité.

Le tableau suivant décrit les droits que vous pouvez affecter aux rôles, ainsi que les quatre rôles par défaut disponibles et les droits associés :

Tableau 237. Rôles et droits

	Administrateur de rôles		Administrateur de surveillance		Administrateur système		Utilisateur de surveillance	
	Afficher	Modifier	Afficher	Modifier	Afficher	Modifier	Afficher	Modifier
Droits d'accès de la configuration système								
Configuration avancée	✓	N/A	–	N/A	✓	N/A	–	N/A
Configuration d'agent	✓	N/A	✓	N/A	–	N/A	–	N/A
Pages d'information	✓	N/A	✓	N/A	✓	N/A	✓	N/A
Fournisseur de recherche	✓	N/A	✓	N/A	–	N/A	–	N/A
Statistiques d'utilisation	✓	N/A	✓	N/A	–	N/A	–	N/A

Tableau 237. Rôles et droits (suite)								
	Administrateur de rôles		**Administrateur de surveillance**		**Administrateur système**		**Utilisateur de surveillance**	
	Afficher	**Modifier**	**Afficher**	**Modifier**	**Afficher**	**Modifier**	**Afficher**	**Modifier**
Droits d'accès aux ressources								
Tableau de bord des performances des applications	✓	✓	✓	✓	✓	–	✓	–
Applications	✓	✓	✓	✓	–	–	✓	–
Application individuelle	«Droits des groupes d'applications et de ressources», à la page 1036							
Tableau de bord de diagnostic	✓	N/A	–	N/A	–	N/A	–	N/A
Gestionnaire de groupes de ressources	✓	N/A	✓	N/A	–	N/A	–	N/A
Groupe de ressources individuelles	«Droits des groupes d'applications et de ressources», à la page 1036							
Groupes de ressources	✓	✓	✓	✓	–	–	–	–
Synthetic Script Manager	✓	N/A	–	N/A	–	N/A	–	N/A
Gestionnaire de seuils	✓	N/A	✓	N/A	–	N/A	–	N/A

Où

✓ indique que les membres de ce rôle disposent de ces droits.

– indique que les membres de ce rôle ne disposent pas de ces droits.

N/A indique ces droits n'existent pas

Remarque : Bien que les **`Statistiques d'utilisation`** soient affichées dans la liste des **Droits de la configuration système**, elles ne sont plus applicables à Cloud APM.

Le tableau suivant décrit les actions associées à chacun des droits :

Tableau 238. Droits	
Droit	**Description**
Configuration avancée	Si vous disposez des droits d'affichage, vous pouvez effectuer les tâches suivantes : • Afficher **Configuration système** > **Configuration avancée** dans la barre de menus. • Effectuer et sauvegarder des modifications dans la fenêtre **Configuration avancée**. • Afficher **Configuration système** > **Gestionnaire de passerelle hybride** dans la barre de menus. • Effectuer et sauvegarder des modifications dans la fenêtre **Gestionnaire de passerelle hybride**.

Tableau 238. Droits (suite)

Droit	Description
Configuration d'agent	Si vous disposez des droits d'affichage, vous pouvez effectuer les tâches suivantes : • Afficher **Configuration système** > **Configuration d'agent** dans la barre de menus. • Effectuer et sauvegarder des modifications dans la fenêtre **Configuration d'agent**.
Pages d'information	Si vous disposez des droits d'affichage, vous pouvez effectuer la tâche suivante : • Afficher **Mise en route** et **Aide** dans la barre de menus. **Remarque :** Lorsque la page **Mise en route** s'ouvre, si vous désélectionnez **Afficher cette page au démarrage**, une erreur de refus de droits s'affiche pour les connexions ultérieures. Cependant, vous pourrez toujours accéder à la page **Mise en route** et aux autres sections auxquelles vous êtes autorisé à accéder.
Fournisseur de recherche	Si vous disposez des droits d'affichage, vous pouvez effectuer les tâches suivantes : • Afficher **Configuration système** > **Configurer des fournisseurs de recherche** dans la barre de menus. • Effectuer et sauvegarder des modifications dans la page **Configurer des fournisseurs de recherche**.

Tableau 238. Droits (suite)	
Droit	**Description**
Tableau de bord des performances des applications	Si vous disposez des droits d'affichage, vous pouvez effectuer les tâches suivantes : • Afficher **Performance** > **Tableau de bord d'Application Performance** dans la barre de menus. • Afficher le Tableau de bord d'Application Performance et les applications prédéfinies **Mes composants** et **Mes transactions**. **Remarque :** Pour connaître les droits requis pour afficher les systèmes dans l'application Mes composants, voir «Droits des groupes d'applications et de ressources», à la page 1036. **Remarque :** L'application Mes transactions s'affiche uniquement si vous utilisez Web Site Monitoring. Toutes les transactions synthétiques Web Site Monitoring s'affichent dans l'application Mes transactions. • Ouvrir des pages personnalisées du tableau de bord dans l'onglet Vues personnalisées. • Créer des vues dans l'onglet Détails d'attribut et les sauvegarder pour votre propre usage. Si vous disposez des droits de modification, vous pouvez effectuer les tâches suivantes : • Afficher **Performance** > **Tableau de bord d'Application Performance** dans la barre de menus. • Afficher le Tableau de bord d'Application Performance et les applications prédéfinies **Mes composants** et **Mes transactions**. **Remarque :** Pour connaître les droits requis pour afficher les systèmes dans l'application Mes composants, voir «Droits des groupes d'applications et de ressources», à la page 1036. **Remarque :** L'application Mes transactions s'affiche uniquement si vous utilisez Web Site Monitoring. Toutes les transactions synthétiques Web Site Monitoring s'affichent dans l'application Mes transactions. • Créer et sauvegarder des pages personnalisées du tableau de bord dans l'onglet Vues personnalisées. • Créer des vues dans l'onglet Détails d'attribut et les partager avec d'autres utilisateurs. • Afficher l'option **Actions**>**Editer** dans les pages de composants ; cette option vous permet d'éditer les valeurs de seuil ainsi que d'autres paramètres des widgets de groupe qui affichent le tableau de bord Composants.
Applications	Si vous disposez des droits d'affichage, vous pouvez effectuer les tâches suivantes : • Afficher des applications dans le Tableau de bord des applications. Si vous disposez des droits de modification, vous pouvez effectuer les tâches suivantes : • Afficher des applications dans le Tableau de bord des applications • Créer, modifier et supprimer des applications avec les outils dans le Tableau de bord des applications.

Tableau 238. Droits (suite)	
Droit	**Description**
Application individuelle	Voir «Droits des groupes d'applications et de ressources», à la page 1036.
Gestionnaire de groupes de ressources	Si vous disposez des droits d'affichage, vous pouvez effectuer la tâche suivante : • Afficher **Configuration système** > **Gestionnaire de groupes de ressources** dans la barre de menus.
Groupes de ressources	Si vous disposez des droits d'affichage, vous pouvez effectuer les tâches suivantes : • Afficher les groupes de ressources et les systèmes qui y résident dans le gestionnaire de groupes de ressources si vous disposez également du droit d'affichage pour le gestionnaire de groupes de ressource. • Afficher les systèmes dans l'application prédéfinie Mes composants si vous disposez également du droit d'affichage ou de modification pour Application Performance Management • Afficher les systèmes dans la fenêtre **Ajouter une application** si vous disposez également du droit de modification des applications. Si vous disposez des droits de modification, vous pouvez effectuer les tâches suivantes : • Afficher les groupes de ressources et leur contenu dans le gestionnaire de groupes de ressources si vous disposez également du droit d'affichage pour le gestionnaire de groupes de ressources. • Afficher les systèmes dans l'application prédéfinie Mes composants si vous disposez également du droit d'affichage ou de modification pour Application Performance Management. • Afficher les systèmes dans la fenêtre **Ajouter une application** si vous disposez également du droit de modification des applications. • Créer, modifier et supprimer des groupes de ressources dans le gestionnaire de groupes de ressources si vous disposez également du droit d'affichage pour le gestionnaire de groupes de ressources. Pour affecter des seuils à un groupe de ressources, vous devez également être membre d'un rôle qui dispose du droit d'affichage du Gestionnaire de seuils. **Remarque :** Le gestionnaire de groupes de ressources permet d'organiser les systèmes surveillés en groupes, afin que des seuils puissent être affectés à ces groupes. Si vous ne disposez pas du droit d'affichage pour le gestionnaire de seuils, vous ne pourrez pas voir les seuils affectés aux groupes de ressources. Si vous affectez le droit de modification des groupes de ressources à un rôle, vous devez également affecter le droit d'affichage du gestionnaire de seuils au rôle.
Groupe de ressources individuelles	Voir «Droits des groupes d'applications et de ressources», à la page 1036.

Tableau 238. Droits (suite)	
Droit	**Description**
Gestionnaire de seuils	Si vous disposez des droits d'affichage, vous pouvez effectuer les tâches suivantes : • Afficher **Configuration système** > **Gestionnaire de seuils** dans la barre de menus. • Créer, modifier et supprimer des seuils dans le gestionnaire de seuils. • Afficher et éditer l'affectation des groupes de ressources pour les seuils dans le gestionnaire de seuils si vous disposez des droits appropriés pour le(s) groupe(s) de ressources. • Afficher et éditer éventuellement l'affectation des seuils des groupes de ressources dans le gestionnaire de groupes de ressources si vous disposez des droits appropriés pour le gestionnaire de groupes de ressources et pour le(s) groupe(s) de ressources, et du droit d'affichage pour le gestionnaire de seuils.
Synthetic Script Manager	Si vous disposez des droits d'affichage, vous pouvez effectuer les tâches suivantes : • Créer, modifier et supprimer des transactions synthétiques dans Synthetic Transaction Manager. **Remarque :** Pour utiliser des transactions synthétiques dans Synthetic Transaction Manager, vous devez également être membre d'un rôle qui dispose du droit d'affichage pour **Configuration d'agent**.
Tableau de bord de diagnostic	Si vous disposez des droits d'affichage, le bouton **Diagnostiquer** apparaît dans les tableaux de bord de diagnostic de l'Agent WebSphere Applications, de l'Agent Node.js, de l'Agent Ruby et de l'agent Microsoft .NET. Cliquez sur le bouton **Diagnostiquer** pour accéder aux tableaux de bord de diagnostic.

Droits des groupes d'applications et de ressources
Vous pouvez attribuer des droits à des groupes d'applications et de ressources individuels.

Droits relatifs aux applications

Dans Cloud APM, une application est constituée d'un groupe de composants et des instances qui résident dans ces composants. Utilisez la fenêtre **Ajouter une application** pour définir une application. Pour plus d'informations sur la définition d'une application, voir Gestion des applications.

Pour sélectionner **Performance** > **Tableau de bord d'Application Performance** dans la console Cloud APM, vous devez disposer du droit d'affichage ou de modification pour le Tableau de bord d'Application Performance. Ce droit vous permet également de visualiser les applications prédéfinies **Mes composants** et **Mes transactions**. L'application **Mes transactions** s'affiche uniquement si vous utilisez Web Site Monitoring. Pour visualiser d'autres applications personnalisées, vous devez disposer du droit d'affichage ou de modification pour l'ensemble des applications ou pour une application individuelle.

Remarque : Si une application est renommée, les droits ne sont pas conservés. Vous devez réaffecter les droits d'affichage et de modification.

Affichage

Le droit d'affichage pour une application est prioritaire sur tout autre type de droit. Pour afficher une application, il n'est pas nécessaire d'être membre d'un rôle qui dispose du droit d'affichage pour chaque composant et instance de composant de l'application. Le tableau suivant décrit les actions que vous pouvez effectuer si vous disposez du droit d'affichage pour une application :

Tableau 239. Droits d'affichage pour une application	
Action	**Droits disponibles**
Afficher tous les composants de prise en charge dans cette application.	✓
Afficher l'application et ses composants dans l'arborescence.	✓
Afficher les composants de l'application dans Mes composants.	✓
Afficher les pages de tableau de bord personnalisées associées à l'application.	✓
Ajouter ou supprimer des composants de l'application.	—
Affecter des seuils aux composants des applications.	—
Afficher les composants de prise en charge d'une application dans le gestionnaire de groupes de ressources.	—

Modification

Si vous êtes membre d'un rôle qui dispose des droits de modification pour une application individuelle, vous pouvez :

- Supprimer l'application.
- Créer des pages de tableau de bord personnalisées dans l'onglet Vues personnalisées. Voir «Vues personnalisées», à la page 1144 .
- Ajouter ou retirer des composants et des instances de composant à l'aide de la fenêtre **Modifier une application**. Les composants et les instances de composant disponibles pour vous dans la fenêtre **Modifier une application** sont filtrés en fonction des droits de votre rôle. Les composants suivants sont disponibles :
  - Les composants sur lesquels vous avez directement des droits d'accès dans les groupes de ressources système et le groupe de ressources personnalisées
  - Les composants dont vous avez indirectement hérité les autorisations basées sur d'autres applications sur lesquelles vous disposez d'une autorisation de modification

Droits relatifs à un groupe de ressources

Utilisez les groupes de ressources pour regrouper des composants par type ou par objectif. Pour plus d'informations sur la création de groupes de ressources, voir «Gestionnaire de groupes de ressources», à la page 1008.

Pour sélectionner **Configuration système** > **Gestionnaire de groupes de ressources**, vous devez disposer du droit d'affichage pour le gestionnaire de groupes de ressources. Pour visualiser les groupes de ressources dans le **gestionnaire de groupes de ressources** ou pour visualiser les membres d'un groupe de ressources dans l'application **Mes composants**, vous devez également disposer du droit d'affichage ou de modification pour l'ensemble des groupes de ressources ou pour des groupes de ressources individuels.

Il existe deux types de groupe de ressources différents : les groupes de ressources personnalisées et les groupes de ressources système.

Groupes de ressources définies personnalisées

Créez des groupes de ressources personnalisées dans le gestionnaire de groupes de ressources. Les groupes de ressources personnalisées permettent de regrouper des ressources en fonction de leur objectif.

Le tableau suivant décrit les actions que vous pouvez effectuer si vous disposez du droit d'affichage pour un groupe de ressources personnalisées :

Tableau 240. Droits d'affichage pour un groupe de ressources personnalisées

Action	Droits disponibles
Afficher le groupe de ressources personnalisées et les ressources de ce groupe dans le gestionnaire de groupes de ressources.	✓
Afficher des ressources qui font partie du groupe de ressources personnalisées dans la fenêtre **Ajouter une application** si vous disposez également du droit de modification pour les applications.	✓
Afficher des ressources qui font partie du groupe de ressources personnalisées dans l'application prédéfinie **Mes composants** si vous disposez également de l'un des droits pour le Tableau de bord d'Application Performance.	✓
Ajouter des ressources dans le groupe de ressources personnalisées.	–
Supprimer des ressources du groupe de ressources personnalisées.	–

Le tableau suivant décrit les actions que vous pouvez effectuer si vous disposez du droit de modification pour un groupe de ressources personnalisées :

Tableau 241. Droits de modification pour un groupe de ressources personnalisées

Action	Droits disponibles
Affecter des seuils au groupe de ressources personnalisées dans l'éditeur de seuils. **Remarque :** Pour affecter des seuils, vous devez également être membre d'un rôle qui dispose du droit d'affichage pour l'éditeur de seuils.	✓
Ajouter des ressources dans le groupe de ressources personnalisées.	✓
Supprimer des ressources du groupe de ressources personnalisées.	✓

Groupes de ressources système

Les groupes de ressources système sont définis automatiquement dans le cadre de la configuration de l'environnement Cloud APM. Les groupes de ressources système ne peuvent pas être créés, supprimés ou modifiés manuellement. Seul le droit d'affichage est disponible pour les groupes de ressources système ; le droit de modification n'est pas disponible.

Des groupes de ressources système sont définis pour chaque type de ressource au moment où la ressource est reconnue par le serveur Cloud APM. Un groupe de ressources système existe pour chaque type de ressource connecté au serveur Cloud APM.

Les agents Cloud APM sont un exemple d'une ressource. Par exemple, la première fois que vous téléchargez, installez et démarrez un agent Db2, un groupe de ressources système nommé Db2 est créé. Ce groupe contient tous les agents Db2 qui seront ultérieurement ajoutés à l'environnement Performance Management.

Le groupe de ressources système de chaque type de ressource contient toutes les ressources de ce type, y compris les ressources IBM Tivoli Monitoring. Si votre environnement dispose à la fois d'IBM Tivoli Monitoring et d'IBM Cloud Application Performance Management, vous pouvez installer la Passerelle hybride d'IBM Cloud Application Performance Management afin d'offrir une vue des agents des deux domaines. Les groupes de ressources définis par le système contiennent des agents des deux domaines. Pour plus d'informations, voir «Intégration à IBM Tivoli Monitoring V6.3 », à la page 975.

Certains groupes de ressources système sont basés sur des agents de sous-noeud. Bien que vous puissiez affecter des seuils à des groupes de ressources système basés sur des agents de sous-noeud, les événements ne s'affichent pas dans le Tableau de bord d'Application Performance. Les seuils sont affectés aux groupes de ressources système sur la base des agents de sous-noeud pour l'acheminement des événements. Les groupes de ressources système basés sur des agents de sous-noeud sont décrits comme suit dans le gestionnaire de groupes de ressources : 'les membres de ce groupe ne peuvent pas être ajoutés dans une application et les événements ne s'affichent pas dans la console Performance Management'. Pour plus d'informations, voir «Gestionnaire de groupes de ressources», à la page 1008.

Le tableau suivant décrit les actions que vous pouvez effectuer si vous disposez du droit d'affichage pour un groupe de ressources système :

Tableau 242. Droits d'affichage pour un groupe de ressources système

Action	**Droits disponibles**
Afficher le groupe de ressources système dans le gestionnaire de groupes de ressources.	✓
Afficher des ressources qui font partie du groupe de ressources système dans la fenêtre **Ajouter une application** si vous disposez également du droit de modification pour les applications.	✓
Afficher des ressources qui font partie du groupe de ressources système dans l'application prédéfinie **Mes composants** si vous disposez également de l'un des droits pour le Tableau de bord d'Application Performance	✓
Affecter des seuils au groupe de ressources système dans l'éditeur de seuils.	✓
Ajouter des ressources dans le groupe de ressources système.	–
Supprimer des ressources du groupe de ressources système.	–

Utilisation des rôles, des utilisateurs et des droits
La page Contrôle d'accès basé sur les rôles permet d'utiliser les rôles, les utilisateurs et les droits.

Avant de commencer
Vous pouvez également utiliser l'API d'autorisation pour effectuer des tâches de contrôle d'accès basées sur les rôles à partir de la ligne de commande. Pour plus d'informations, voir «Exploration des API», à la page 1103.

Remarque : Les groupes d'utilisateurs ne sont pas pris en charge dans Cloud APM.

Procédure

- Pour filtrer la liste des rôles, des utilisateurs ou des groupes d'utilisateurs répertoriés dans la page Contrôle d'accès basé sur les rôles, procédez comme suit :
  a) Sélectionnez **Configuration du système> Contrôle d'accès basé sur les rôles**.
  b) Cliquez dans la zone de texte **Filtre** et entrez le texte partiel ou complet qui servira de filtre.
  A mesure que vous tapez, les lignes qui ne contiennent pas ce que vous avez tapé dans la zone de filtre sont supprimées de la table.
  c) Pour supprimer le filtre rapide, supprimez la valeur ou cliquez sur "x".
  d) Pour appliquer le filtre, cliquez sur .
- Pour créer un rôle personnalisé, procédez comme suit :
  a) Sélectionnez **Configuration du système> Contrôle d'accès basé sur les rôles**.
  b) Dans l'onglet **Rôles**, cliquez sur . La page **Editeur de rôle** s'affiche.
  c) Dans l'onglet **Affecter des utilisateurs à des rôles**, sélectionnez l'onglet **Groupes d'utilisateurs** ou l'onglet **Utilisateurs individuels**, puis sélectionnez les utilisateurs et les groupes d'utilisateurs à ajouter au rôle.
  d) Dans l'onglet **Affecter des droits à des rôles**, sélectionnez l'onglet **Droits d'accès de la configuration système** ou l'onglet **Droits d'accès aux ressources**, puis sélectionnez les droits à affecter au rôle.
  e) Cliquez sur **Sauvegarder**.
- Pour éditer un rôle par défaut ou personnalisé existant, procédez comme suit :
  a) Sélectionnez **Configuration du système> Contrôle d'accès basé sur les rôles**.
  b) Dans l'onglet **Rôles**, cliquez sur . La page **Editeur de rôle** s'affiche.
  c) Dans l'onglet **Affecter des utilisateurs à des rôles**, cliquez sur l'onglet **Groupes d'utilisateurs** ou l'onglet **Utilisateurs individuels**, puis sélectionnez les utilisateurs ou les groupes d'utilisateurs à ajouter au rôle.
  d) Dans l'onglet **Affecter des droits à des rôles**, sélectionnez l'onglet **Droits d'accès de la configuration système** ou l'onglet **Droits d'accès aux ressources**, puis sélectionnez les droits à affecter au rôle.
  e) Cliquez sur **Sauvegarder**.
- Pour supprimer un rôle, procédez comme suit :
  a) Sélectionnez **Configuration du système> Contrôle d'accès basé sur les rôles**.
  b) Dans l'onglet **Rôles**, sélectionnez le rôle à supprimer, puis cliquez sur . Un message de confirmation s'affiche. Cliquez sur **OK**.

  Remarque : Lorsque vous supprimez un rôle, les utilisateurs membres de ce rôle ne sont pas supprimés. Ils restent disponibles dans l'onglet **Utilisateurs individuels** et peuvent être affectés à un autre rôle par l'administrateur des rôles.
- Pour éditer les droit d'accès d'un utilisateur individuel ou d'un groupe d'utilisateurs, procédez comme suit :
  a) Sélectionnez **Configuration du système> Contrôle d'accès basé sur les rôles**.
  b) Dans l'onglet **Utilisateur individuel** ou **Groupes d'utilisateurs**, sélectionnez l'utilisateur ou le groupe d'utilisateurs à éditer, puis cliquez sur . La page **Editeur d'utilisateur individuel** s'ouvre.
  c) Sélectionnez le ou les rôles à affecter à l'utilisateur.
  d) Cliquez sur **Sauvegarder**.
- Pour créer un fichier csv qui récapitule les droits d'un utilisateur individuel ou d'un groupe d'utilisateurs, procédez comme suit :

a) Dans l'onglet **Utilisateur individuel** ou **Groupes d'utilisateurs**, sélectionnez l'utilisateur ou le groupe d'utilisateurs requis, puis cliquez sur . La page **Editeur d'utilisateur individuel** ou **Editeur de groupe d'utilisateurs** s'ouvre.

b) Cliquez sur **Récapitulatif de l'exportation**.

c) Sélectionnez **Sauvegarder**, puis cliquez sur **OK**.

Un fichier CSV récapitulant les droits de l'utilisateur ou du groupe d'utilisateurs est sauvegardé dans l'emplacement spécifié.

Résultats

L'affectation des rôles et des droits est appliqué dès que vous avez cliqué sur **Sauvegarder**.

Accès et utilisation de l'API Role-Based Access Control Service

Utilisez l'API Role-Based Access Control Service pour gérer le cycle de vie des stratégies de contrôle d'accès basé sur les rôles à partir de la ligne de commande.

Pourquoi et quand exécuter cette tâche

Effectuez des tâches d'accès basé sur les rôles telles que la création, l'affichage, la mise à jour et la suppression de rôles. Ajoutez et supprimez un ensemble d'utilisateurs ou de groupes d'utilisateurs à partir d'un rôle donné. Accordez des droits à un rôle donné. Affichez une liste des rôles, utilisateurs, groupes d'utilisateurs et droits qui sont définis dans le système.

Vous pouvez créer des scripts d'automatisation de tâches telles que la définition de nouveaux rôles et l'affectation d'utilisateurs, de groupes d'utilisateurs et de droits à ces rôles.

Procédure

1. Effectuez les étapes 1 à 9 décrites dans la rubrique Exploration des API.
   L'étape 10 et l'étape 11 fournissent des détails supplémentaires.
2. Cliquez sur **USE** et sélectionnez une clé (**Key1** par exemple).

   Remarque : cliquez sur **Masquer** pour afficher votre ID client et votre secret client. Relevez-les car vous en aurez besoin si vous effectuez des appels d'API avec des outils externes en dehors de l'Explorateur d'API. Cliquez ensuite sur **Afficher** pour les masquer.
3. Renseignez tous les en-têtes requis (signalés par un astérisque).

   L'en-tête X-IBM-Service-Location
   * correspond à l'emplacement géographique de votre abonnement (par exemple, na pour l'Amérique du Nord).

   Autorisation
   * correspond à votre chaîne codée en base64 de l'ID IBM et du mot de passe. Lorsque vous codez l'ID IBM et le mot de passe dans l'outil based64-encoder, le format doit être *IBMid:password*. Par exemple, `Basic YXBtYWRtaW46YXBtcGFzcw==!`.
4. Vous devez inclure un en-tête de référenceur dans toutes les demandes POST, PUT et DELETE. La valeur de l'en-tête de référenceur est toujours :

   ```
   -H 'Referer: https://api.ibm.com'
   ```
5. Faites défiler l'écran pour rechercher **Test** et cliquez dessus.

Exemple

L'exemple suivant utilise la commande curl pour créer un rôle.

```
POST /1.0/authzn/roles
```

Remarque : Le corps de la requête POST doit contenir un objet JSON qui définit le rôle tel qu'indiqué par le paramètre **-d**.

```
curl -X POST \
  https://api.ibm.com/perfmgmt/run/1.0/authzn/roles  \
  -H 'Referer: https://api.ibm.com' \
  -H 'authorization: Basic REPLACE_BASE64_ENCODED_STRING' \
  -H 'content-type: application/json' \
  -H 'x-ibm-client-id: REPLACE_KEY_VALUE' \
  -H 'x-ibm-client-secret: REPLACE_KEY_VALUE' \
  -d '{
    "description": "Description de votre rôle",
    "id": "/authzn/roles/ID_de_votre_rôle",
    "label": "Nom de votre rôle"
}'
```

Administration de vos agents

Votre installation IBM Cloud Application Performance Management dispose d'outils permettant de gérer vos agents de surveillance.

Certains de ces outils sont également utilisés pendant la configuration initiale de vos systèmes gérés : «Utilisation des commandes de l'agent», à la page 181, «Page Configuration d'agent», à la page 187 et «Utilisation de la fenêtre IBM Cloud Application Performance Management sur les systèmes Windows», à la page 186.

Démarrage des agents en tant qu'utilisateur non superutilisateur

Si vous souhaitez démarrer des agents avec des utilisateurs différents, créez un groupe commun sur le système et affectez chaque utilisateur en tant que membre de ce groupe.

Avant de commencer

Si vous avez installé et configuré votre agent avec le même utilisateur non superutilisateur et que vous voulez le démarrer avec le même utilisateur, aucune action particulière n'est requise. Si vous avez installé et configuré votre agent en tant qu'utilisateur sélectionné et que vous voulez le démarrer en tant qu'un autre utilisateur, créez un groupe commun sur le système. Définissez tous les utilisateurs de gestion d'agent comme membres de ce groupe commun. Transférez la propriété de tous les fichiers et répertoires d'agent vers ce groupe.

Pourquoi et quand exécuter cette tâche

Un script de démarrage automatique est généré par une installation, une mise à niveau ou une configuration. Ce script, (nommé `ITMAgentsN` ou `rc.itmN` suivant le système d'exploitation UNIX), contient une entrée pour chaque application dans une installation particulière. Par défaut, tous les agents sont démarrés avec les droits d'accès de superutilisateur. Pour mettre à jour les scripts de démarrage du système et démarrer les agents en tant qu'utilisateur non superutilisateur, vous devez éditer le fichier `install_dir/config/kcirunas.cfg`, qui contient un sur-ensemble de la syntaxe XML. Chaque section **`productCode`** dans le fichier `kcirunas.cfg` est désactivée par défaut. Activez une section **`productCode`** pour votre agent en supprimant l'indicateur de commentaire dans **`!productCode`**. Les sections mises en commentaire ou désactivées sont ignorées. Les sections non mises en commentaire ou activées pour des applications qui ne sont pas installées sont ignorées.

Procédure

1. Installez vos agents de surveillance sous Linux ou UNIX, comme indiqué dans «Installation d'agents», à la page 128 sur des systèmes AIX ou dans «Installation d'agents», à la page 137 sur des systèmes Linux.
2. Facultatif : Au besoin, configurez vos agents de surveillance sous Linux ou UNIX (voir Chapitre 7, «Configuration de votre environnement», à la page 163).

3. Exécutez le script `./secure.sh` avec le nom de groupe de l'utilisateur non superutilisateur afin de sécuriser les fichiers et définissez la propriété de groupe de fichiers sur les fichiers.
   Par exemple : **`./secure.sh -g db2iadm1`**
4. Pour mettre à jour les scripts de démarrage du système, procédez comme suit :
   a) Mettez à jour le fichier `install_dir/config/kcirunas.cfg`. Activez les sections **productCode** pour vos agents. Pour les agents qui ne requièrent pas une valeur d'instance, indiquez le code_produit, l'instance et l'utilisateur, où *code_produit* correspond au code à deux lettres spécifié dans Tableau 11, à la page 182. Pour les agents qui requièrent une valeur d'instance, tels que l'agent de surveillance Db2 (code produit : ud), indiquez le code_produit, l'instance, l'utilisateur et le nom.
   Exemple :

```
<productCode>ud</productCode>
<instance>
<name>db2inst1</name>
<user>db2inst1</user>
</instance>
<instance>
<name>db2inst2</name>
<user>root</user>
</instance>
```

   b) Exécutez le script suivant avec les droits d'accès de superutilisateur ou d'utilisateur sudo :
   rép_install`/bin/UpdateAutoRun.sh`

Que faire ensuite

Pour plus d'informations sur le script **`./secure.sh`**, voir Securing the agent installation files.

Utilisez le même ID utilisateur pour l'installation et les mises à niveau des agents.

Seuils d'événement pour la surveillance des transactions

Vous pouvez utiliser des seuils d'événement afin de surveiller immédiatement votre environnement. Vous pouvez également créer des seuils d'événement personnalisés qui testent certaines conditions et déclenchent un événement lorsque des indicateurs clés de performance dépassent le seuil défini.

Evénements de Surveillance des temps de réponse

Des événements de temps de réponse sont créés lorsque des transactions Web dépassent un seuil de **temps de réponse**.

Après avoir cliqué sur **Configuration système** > **Gestionnaire de seuils**, sélectionnez **Temps de réponse** comme **type de source de données**. Tous les seuils d'événement de l'environnement de Surveillance des temps de réponse sont appliqués à l'ensemble des systèmes gérés de même type.

Les seuils prédéfinis suivants sont disponibles pour l'agent Surveillance des temps de réponse.

Tableau 243. Seuils de Surveillance des temps de réponse

Seuil	Description	Formule
`Response_Time_Availability_Crit`	Un pourcentage élevé de transactions Web a échoué.	Si la transaction WRT Status.Percent_Failed est supérieure à 10 et que la transaction WRT Status.Transaction_Definition_Name est différente de 'Ignore Resources' alors Response_Time_Availability_Crit est vrai

Tableau 243. Seuils de Surveillance des temps de réponse (suite)		
Seuil	**Description**	**Formule**
`Response_Time_Availability_Warn`	Un pourcentage moyen de transactions Web a échoué.	Si la transaction WRT Status.Percent_Failed est supérieure à 0 et que la transaction WRT Status.Percent_Failed est inférieure à 10 et la transaction WRT Status.Transaction_Definition_Name est différente de 'Ignore Resources' alors Response_Time_Availability_Warn est vrai
`Response_Time_Critical`	Un pourcentage élevé de transactions Web présente un temps de réponse lent.	Si la transaction WRT Status.Percent_Slow est supérieure à 5 et que la transaction WRT Status.Percent_Available est égale à 100 et la transaction WRT Status.Transaction_Definition_Name est différente de 'Ignore Resources' alors Response_Time_Critical est vrai
`Response_Time_Warning`	Un pourcentage modéré de transactions Web présente un temps de réponse lent.	Si la transaction WRT Status.Percent_Slow est supérieure à 1 et que la transaction WRT Status.Percent_Slow est inférieure à 5, la transaction WRT Status.Percent_Available est égale à 100 et la transaction WRT Status.Transaction_Definition_Name est différente de 'Ignore Resources' alors Response_Time_Warning est vrai

demandes correctes ont un temps de réponse inférieur à 10 secondes. Les *demandes lentes* ont un temps de réponse supérieur à 10 secondes. La valeur de 10 secondes utilisée pour déterminer si le temps de réponse est correct ou lent n'est pas configurable.

Evénements de Suivi des transactions

Des événements de Suivi des transactions sont créés lorsque des transactions de middleware dépassent un seuil de Suivi des transactions.

Pour afficher les seuils de Suivi des transactions par défaut, cliquez sur  **Configuration du système** > **Gestionnaire de seuils** et sélectionnez **Suivi des transactions** comme **Type de source de données**.

Conseil : Au besoin, vous pouvez créer vos propres seuils de Suivi des transactions.

Les seuils prédéfinis suivants sont disponibles pour des transactions de middleware.

Tableau 244. Seuils de Suivi des transactions

Seuil	Description	Formule
`Interaction_Avail_Critical`	Un pourcentage élevé d'interactions de middleware a échoué.	Si KTE INTERACTION AGGREGATE DATA.PERCENTAGE_FAILED est supérieur à 10 alors Interaction_Avail_Critical est vrai
`Interaction_Avail_Warning`	Un pourcentage moyen d'interactions de middleware a échoué.	Si KTE INTERACTION AGGREGATE DATA.PERCENTAGE_FAILED est supérieur à 0 et que KTE INTERACTION AGGREGATE DATA.PERCENTAGE_FAILED est inférieur ou égal à 10 alors `Interaction_Avail_Warning` est vrai
`Interaction_Time_Critical`	Un pourcentage élevé d'interactions de middleware présente un temps total lent.	Si KTE INTERACTION AGGREGATE DATA.PERCENTAGE_SLOW est supérieur ou égal à 5 et que KTE INTERACTION AGGREGATE DATA.PERCENTAGE_FAILED est égal à 0 alors Interaction_Time_Critical est vrai
`Interaction_Time_Warning`	Un pourcentage modéré d'interactions de middleware présente un temps total lent.	Si KTE INTERACTION AGGREGATE DATA.PERCENTAGE_SLOW est supérieur à 1 et que KTE INTERACTION AGGREGATE DATA.PERCENTAGE_SLOW est inférieur à 5 et KTE INTERACTION AGGREGATE DATA.PERCENTAGE_FAILED est égal à 0 alors Interaction_Time_Warning est vrai
`Transaction_Avail_Critical`	Un pourcentage élevé de transactions de middleware a échoué.	Si KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_FAILED est supérieur à 10 alors Transaction_Avail_Critical est vrai
`Transaction_Avail_Warning`	Un pourcentage moyen de transactions de middleware a échoué.	Si KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_FAILED est supérieur à 0 et que KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_FAILED est inférieur ou égal à 10 alors `Transaction_Avail_Warning` est vrai
`Transaction_Time_Critical`	Un pourcentage élevé de transactions de middleware présente un temps total lent.	Si KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_SLOW est supérieur ou égal à 5 et que KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_FAILED est égal à 0 alors Transaction_Time_Critical est vrai

Tableau 244. Seuils de Suivi des transactions (suite)		
Seuil	**Description**	**Formule**
`Transaction_Time_Warning`	Un pourcentage modéré de transactions de middleware présente un temps total lent.	Si KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_SLOW est supérieur à 1 et que KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_SLOW est inférieur à 5 et KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_FAILED est égal à 0 alors Transaction_Time_Warning est vrai

demandes correctes ont un temps de réponse inférieur à 10 secondes. Les *demandes lentes* ont un temps de réponse supérieur à 10 secondes. La valeur de 10 secondes utilisée pour déterminer si le temps de réponse est correct ou lent n'est pas configurable.

Création de seuils de génération d'événements pour la surveillance des transactions
Utilisez le gestionnaire de seuils pour créer des seuils pour des transactions. Les seuils sont utilisés pour comparer la valeur d'échantillon d'un attribut avec la valeur définie dans le seuil. Si la valeur d'échantillon répond à la comparaison, un événement de transaction est généré.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser des seuils pour déterminer quand les applications signalent des conditions spécifiques. Pour plus d'informations sur les seuils par défaut pour la surveillance des transactions, voir «Seuils d'événement pour la surveillance des transactions », à la page 1043.

Vous pouvez créer des seuils supplémentaires pour surveiller d'autres aspects d'une transaction. Par exemple, vous pouvez créer un seuil afin de surveiller le débit des événements de transaction du middleware. Et, si ce débit passe au-dessous du seuil spécifié, générer un événement.

Procédure

Pour créer un seuil et l'associer à une ou plusieurs transactions, procédez comme suit :

1. Dans la barre de navigation, cliquez sur l'icône **Configuration du système** > **Gestionnaire de seuils**. Définissez le **type de source de données** en tant que **suivi des transactions**.
2. Cliquez sur Ajouter pour créer un nouveau seuil.
3. Définissez une gravité pour l'événement qui dépasse ce seuil.
4. Pour associer le seuil à une transaction, définissez les valeurs suivantes :
   - Ensemble de données - `DONNEES AGREGATION TRANSACTION KTE`
   - Elément affiché - `valeur_ressource`
   - Opérateur logique - `And (&)`
5. Alternativement, pour associer le seuil à une interaction, définissez les valeurs suivantes :
   - Ensemble de données - `KTE INTERACTION AGGREGATE DATA`
   - Elément affiché - `Source_Resource_Value`
   - Opérateur logique - `And (&)`
6. Cliquez sur **Ajouter** pour ajouter une condition. Dans la zone **Ajouter une condition**, sélectionnez un attribut et un opérateur, puis entrez une valeur de seuil.

   Par exemple, pour ajouter une condition de seuil qui génère un événement de transaction lorsque le nombre de transactions par minute passe au-dessous de 100, définissez les valeurs suivantes, puis cliquez sur **OK**:

- Attribut - `débit_transactions`
- Opérateur - `Inférieur à`
- Valeur - `100`

Au besoin, répétez cette procédure pour ajouter d'autres conditions à votre seuil.

7. Dans la section Affectation de groupes, sélectionnez `Suivi des transactions` pour affecter le seuil à ce groupe de ressources.
8. Cliquez sur **Sauvegarder**.

Résultats

Vous venez de créer un seuil et vous l'avez associé à une transaction ou une interaction. Lorsque les conditions de seuil sont remplies, un événement est généré. Vous pouvez surveiller des événements dans l'onglet Evénements du tableau de bord des performances des applications.

Exemple

Pour créer des seuils pour l'agent Response Time Monitoring en vue de surveiller d'autres aspects d'une transaction Web en plus de ceux surveillés par défaut, procédez comme suit :

1. Dans le gestionnaire de seuils, associez le **type de source de données** à **Temps de réponse**.
2. Lorsque vous ajoutez le seuil, utilisez les paramètres suivants :
   - Ensemble de données - `Statut de transaction WRT`
   - Elément affiché - `Application`
   - Opérateur logique - `And (&)`
   - Affectation de groupes - `Temps de réponse Web`

Gestion des événements d'agent de système d'exploitation

Vous pouvez configurer l'agent de système d'exploitation pour gérer les événements.

Filtrage et récapitulatif des événements
Utilisez les options de filtrage et de récapitulatif des événements définies dans le fichier de configuration (`.conf`) pour contrôler la manière dont les événements en double sont traités par l'agent de système d'exploitation.

Lorsqu'un journal est surveillé, un événement peut rapidement s'afficher plusieurs fois. Cela peut se produire lorsque l'application qui génère le journal détecte une erreur et la consigne en continu jusqu'à ce que le seuil soit atteint. Lorsque ce type de consignation se produit, un nombre d'événements excessif est envoyé à l'infrastructure de Performance Management. Le volume d'événements a un impact négatif sur les performances.

Remarque : Les procédures de détection et de regroupement des événements sont prises en charge uniquement pour les événements envoyés à Performance Management. Vous ne pouvez donc pas exécuter ces procédures avec des événements envoyés à OMNIbus par la fonction EIF.

Détection et filtrage des événements en double
Vous pouvez configurer l'agent de système d'exploitation pour traiter les événements en double.

Pour résoudre le problème d'événements en double, vous devez définir ce que vous considérez comme des doublons dans le fichier `.conf` à l'aide de la balise `DupDetectionKeyAttributes`. Dans une liste séparée par des virgules, vous devez inclure un ou plusieurs attributs Performance Management définis que vous souhaitez utiliser pour déterminer si un événement est considéré comme un doublon. Dans l'exemple suivant, les événements possédant le même message et le même paramètre `CustomSlot1` sont considérés comme des doublons :

```
DupDetectionKeyAttributes=msg,CustomSlot1
```

Les événements en double sont détectés à partir des attributs Performance Management. Si vous souhaitez que la détection des doublons s'effectue sur des attributs spécifiques définis par vos soins, procédez comme suit :

1. Mappez la valeur d'attribut à un attribut Performance Management.
2. Mappez l'attribut Performance Management à la balise `DupDetectionKeyAttributes` dans le fichier `.conf`.

Dans l'exemple suivant, les attributs importants `eventclass` et `eventid` sont mappés aux paramètres *CustomSlot1* et *CustomSlot2* :

```
REGEX BaseAuditEvent
^([A-Z][a-z]{2} [0-9]{1,2} [0-9]{1,2}:[0-9]{2}:[0-9]{2}
 [0-9] {4}) [0-9] (\S+) (\S+) \
Microsoft-Windows-Security-Auditing (\S+) ([0-9]+) (.*)
timestamp $1
severity $2
eventclass $3 CustomSlot1
eventkeywords $4
eventid $5 CustomSlot2
msg $6
END
```

Si vous souhaitez définir certains événements comme des doublons, mappez les attributs Performance Management à la balise `DupDetectionKeyAttributes` dans le fichier `.conf`, comme indiqué ci-après :

```
DupDetectionKeyAttributes=CustomSlot1,CustomSlot2
```

Remarque :

1. Les noms d'attribut `CustomSlot` sont sensibles à la casse. Vous devez donc entrer le nom exactement comme décrit dans l'exemple précédent.
2. Si vous n'indiquez pas de liste d'attributs, les valeurs correspondent par défaut à `Class` et `Logname`.

Les événements pour lesquels ces attributs ont une correspondance sont considérés comme des doublons par l'agent.

Etant donné que la détection des doublons est globale, il est recommandé de choisir un ensemble d'attributs personnalisés (CustomSlots) à utiliser en tant que clés et de les utiliser de cette façon dans l'ensemble des instructions de formatage. Par exemple, vous pouvez utiliser les attributs 1 à 3 pour les clés. Si un format a besoin d'une seule clé et de plusieurs attributs, vous pouvez utiliser l'attribut 1 pour contenir la valeur de nom et les attributs 4 à n pour contenir les autres données.

Intervalle de récapitulatif
L'intervalle de récapitulatif désigne la période pendant laquelle s'exécute la procédure de détection de doublons.

Les événements en double sont comptabilisés au cours de cet intervalle à l'issue duquel ils sont réinitialisés. Le compteur recommence le décompte à partir de zéro au début de chaque nouvel intervalle de récapitulatif.

L'agent envoie un événement récapitulatif pour chaque événement défini qu'il surveille au cours de l'intervalle. L'événement récapitulatif contient les valeurs d'attribut du premier événement correspondant. Il contient également le nombre de doublons de cet événement qui se sont produits au cours de l'intervalle de récapitulatif.

L'intervalle de récapitulatif est défini dans le fichier de configuration (`.conf`) comme indiqué dans l'exemple suivant :

```
EventSummaryInterval=300
```

La valeur de l'intervalle de récapitulatif est exprimée en secondes. Dans cet exemple, l'intervalle de récapitulatif est donc de cinq minutes (300 / 60 = 5).

Filtrage des événements
Si le filtrage des événements est en cours d'exécution, le paramètre EventFloodThreshold du fichier (`.conf`) indique à l'agent quand l'événement est envoyé.

Le tableau suivant présente les valeurs EventFloodThreshold.

Tableau 245. Valeurs EventFloodThreshold

Valeurs EventFloodThreshold	**Description**
send_all	Le paramètre *send_all* est la valeur par défaut. Tous les événements sont envoyés (y compris les doublons).
send_none	Aucun événement n'est envoyé. Seuls les événements récapitulatifs sont envoyés.
send_first	Seul le premier événement rencontré est envoyé. Si des doublons se produisent sur une période spécifique, ils ne sont pas envoyés. Pour plus d'informations, voir «Intervalle de récapitulatif», à la page 1048.
n entier	L'événement est envoyé toutes les *n* occurrences (tous les *5* doublons, par exemple). Pour plus d'informations, voir «Intervalle de récapitulatif», à la page 1048.

Attributs de récapitulation
Les attributs Type d'événement et Nombre d'occurrences sont utilisés pour récapituler les événements.

Les attributs Type d'événement et Nombre d'occurrences prennent tout leur sens dans la récapitulation d'événements. L'attribut Type d'événement indique le type de l'événement (*Evénement* ou *Evénement récapitulatif*). Les événements généraux qui constituent des correspondances un à un d'événements trouvés dans le journal sont de type *Evénement*. Les événements récapitulatifs qui sont envoyés à l'issue de l'intervalle de récapitulatif sont de type *Evénement récapitulatif*.

L'attribut Nombre d'occurrences précise le volume total d'enregistrements en double trouvés dans le journal pour l'événement. Les événements récapitulatifs incluent ce nombre, car il indique le nombre d'événements reçus qui correspondaient à l'événement récapitulatif au cours de l'intervalle de récapitulatif précédent.

Seuils et événements récapitulatifs

Quelle que soit la valeur de filtre (pour les valeurs possibles, voir «Filtrage des événements», à la page 1049), les événements récapitulatifs figurent toujours à la fin de chaque intervalle de récapitulatif, pour tout événement qui s'est produit au moins une fois au cours de cet intervalle. Si vous n'attendez pas d'événements récapitulatif, les seuils peuvent être déclenchés accidentellement. Pour éviter le déclenchement accidentel d'un seuil, incluez une clause dans le seuil pour *`Type d'événement`*`==` *`Evénement`* ou *`Type d'événement`*`!=` *`Evénement récapitulatif`*.

Journal des événements Windows
L'agent de système d'exploitation utilise le fichier .conf pour surveiller les événements consignés dans l'historique des événements Windows.

L'agent de système d'exploitation continue à utiliser l'option `WINEVENTLOGS` du fichier de configuration (`.conf`) pour surveiller les événements consignés dans le journal des événements Windows. L'agent surveille une liste de journaux d'événements séparés par des virgules, comme indiqué dans l'exemple suivant :

```
WINEVENTLOGS=System,Security,Application
```

L'agent de système d'exploitation continue également d'utiliser le paramètre `WINEVENTLOGS=All`. Le paramètre `All` fait référence aux journaux d'événements standard suivants fournis avec les versions Windows antérieures à 2008 : Sécurité, Application, Système, Active Directory, DNS (Domain Name System) et FRS (File Replication Service). Cependant, tous les journaux des événements système ne sont pas vérifiés.

La balise du fichier de configuration `UseNewEventLogAPI` permet au journal des événements (journal des événements Windows 2008 ou version ultérieure) d'accéder à tous les nouveaux journaux ajoutés par Microsoft, ainsi qu'à l'ensemble des journaux d'événements Windows créés par d'autres applications ou par l'utilisateur. Les nouveaux journaux sont définis par le mot clé `WINEVENTLOGS`.

Dans l'exemple suivant, la balise `UseNewEventLogAPI` a pour valeur `y`.

```
UseNewEventLogAPI=y
WINEVENTLOGS=Microsoft-Windows-Hyper-V-Worker-Admin
```

Dans cet exemple, le journal `Microsoft-Windows-Hyper-V/Admin` est surveillé sur un système Windows possédant le rôle Hyper-V.

Dans le journal des événements Windows, chaque événement comporte les zones suivantes dans cet ordre :

- Date au format mois, jour, heure et année
- Catégorie d'événement sous forme d'entier
- Niveau d'événement
- Identificateur de sécurité Windows. Dans l'identificateur de sécurité Windows, tous les espaces sont remplacés par un trait de soulignement si le fichier de configuration (`.conf`) inclut le paramètre `SpaceReplacement=TRUE`.

  Remarque : `SpaceReplacement=TRUE` est la valeur par défaut si vous associez `UseNewEventLogAPI` à `y` dans le fichier (`.conf`) (en indiquant que vous utilisez le journal d'événements).
- Source Windows. Dans le source Windows, tous les espaces sont remplacés par un trait de soulignement si le fichier de configuration (`.conf`) comporte le paramètre `SpaceReplacement=TRUE`.
- Mots clés du journal d'événements Windows. Dans les mots clés du journal d'événements Windows, tous les espaces sont remplacés par un trait de soulignement si le fichier de configuration (`.conf`) inclut le paramètre `SpaceReplacement=TRUE`.

  Remarque : La zone de mots clés qui est décrite ici est nouvelle dans la version Windows 2008 du journal des événements. Etant donné qu'elle n'existait pas dans les précédentes versions du journal des événements, vous ne pouvez pas réutiliser directement vos anciennes instructions de format du journal des événements. Vous devez d'abord les modifier pour prendre en compte cette nouvelle zone.
- Identificateur d'événement Windows
- Texte du message

Par exemple, lorsqu'un administrateur se connecte à un système Windows 2008, un événement est généré dans le journal de sécurité, indiquant les privilèges associés à la session du nouvel utilisateur :

```
Mar 22 13:58:35 2011 1 Information N/A Microsoft-Windows-
Security-Auditing Audit_Success 4672 Special privileges assigned to new logon.
S-1-5-21-586564200-1406810015-1408784414-500    Account Name:
Administrator   Account Domain:     MOLDOVA     Logon ID:
0xc39cb8e    Privileges:        SeSecurityPrivilege
SeBackupPrivilege          SeRestorePrivilege
SeTakeOwnershipPrivilege            SeDebugPrivilege
SeSystemEnvironmentPrivilege            SeLoadDriverPrivilege
SeImpersonatePrivilege
```

Pour capturer tous les événements qui ont été créés par la source d'événement `Microsoft-Windows-Security-Auditing`, vous devez écrire une instruction de format comme indiqué ci-dessous :

```
REGEX BaseAuditEvent
^([A-Z][a-z]{2} [0-9]{1,2} [0-9]{1,2}:[0-9]{2}:[0-9]{2} [0-9]
{4}) [0-9] (\S+) (\S+) Microsoft-Windows-Security-Auditing (\S+)
([0-9]+) (.*)
timestamp $1
severity $2
login $3
eventsource "Microsoft-Windows-Security-Auditing"
eventkeywords $4
eventid $5
msg $6
END
```

L'exemple suivant indique les valeurs qui sont affectées aux attributs pour l'exemple d'événement précédent :

```
timestamp=Mar 22 13:58:35 2011
severity=Information
login=N/A
eventsource=Microsoft-Windows-Security-Auditing
eventid=4672
msg="Special privileges assigned to new logon.
S-1-5-21-586564200-1406810015-1408784414-500    Account Name:
Administrator   Account Domain:     MOLDOVA     Logon ID:
0xc39cb8e    Privileges:        SeSecurityPrivilege
SeBackupPrivilege          SeRestorePrivilege
SeTakeOwnershipPrivilege            SeDebugPrivilege
SeSystemEnvironmentPrivilege            SeLoadDriverPrivilege
SeImpersonatePrivilege
```

Comme il est difficile d'anticiper l'apparence de ces événements, vous pouvez écrire vos expressions régulières en capturant les événements réels dans un fichier. Il ne vous restera plus ensuite qu'à examiner le fichier, sélectionner les événements devant être capturés par l'agent et écrire les expressions régulières correspondant à ces événements. Pour capturer tous les événements à partir du journal des événements Windows, procédez comme suit :

1. Créez un fichier de format contenant un seul modèle qui ne correspond à rien. Par exemple :

   ```
   REGEX NoMatch
   This doesn't match anything
   END
   ```

2. Dans le fichier de configuration (`.conf`), ajoutez le paramètre :

   ```
   UnmatchLog=C:/temp/evlog.unmatch
   ```

3. Exécutez l'agent et capturez quelques événements échantillonnés.

Mappage d'événements
L'interface Tivoli Event Integration Facility (EIF) permet de réacheminer des événements de situation vers Tivoli Netcool/OMNIbus, Tivoli Enterprise Console ou Operations Analytics - Log Analysis.

Les événements EIF spécifient une classe d'événement et les données d'événement sont spécifiées sous la forme de paires nom/valeur identifiant le nom et la valeur d'un attribut d'événement. Une classe d'événement peut comporter des sous-classes. Performance Management fournit les définitions de classe d'événement de base ainsi qu'un ensemble d'emplacements de base inclus dans tous les événements de surveillance. Les agents étendent les classes d'événement de base afin de définir des sous-classes incluant des attributs spécifiques à l'agent. Pour les événements des fichiers journaux d'agent de système d'exploitation, les classes d'événement correspondent aux groupes d'attributs d'agent et les attributs d'agent correspondent aux attributs dans le groupe d'attributs.

Pour les événements générés par des seuils dans le groupe d'attributs LFAProfiles, les événements sont envoyés à l'aide de la classe d'événement ITM_KLO_LFAPROFILES. Cette classe d'événement contient les attributs suivants :

- node : STRING

- timestamp : STRING
- subnode_msn : STRING
- subnode_affinity : STRING
- subnode_type : STRING
- subnode_resource_name : STRING
- subnode_version : STRING
- subnode_config_file : STRING
- subnode_description : STRING
- subnode_description_enum : STRING

Pour les événements générés par des seuils dans le groupe d'attributs Log File RegEx Statistics, les événements sont envoyés à l'aide de la classe d'événement ITM_KLO_LOG_FILE_REGEX_STATISTICS. Cette classe d'événement contient les attributs suivants :

- node : STRING
- timestamp : STRING
- table_name : STRING
- attrib_name : STRING
- filter_number : INTEGER
- average_processor_time : REAL
- average_processor_time_enum : STRING
- total_processor_time : REAL
- total_processor_time_enum : STRING
- max_processor_time : REAL
- max_processor_time_enum : STRING
- min_processor_time : REAL
- min_processor_time_enum : STRING
- filter_count : REAL
- filter_count_matched : REAL
- filter_count_unmatched : REAL
- regex_pattern : STRING
- last_matched_time : STRING
- last_matched_time_enum : STRING
- last_unmatched_time : STRING
- last_unmatched_time_enum : STRING
- result_type : INTEGER
- result_type_enum : STRING

Pour les événements générés par des seuils dans le groupe d'attributs Log File Status, les événements sont envoyés à l'aide de la classe d'événement ITM_KLO_LOG_FILE_STATUS. Cette classe d'événement contient les attributs suivants :

- node : STRING
- timestamp : STRING

- table_name : STRING
- file_name : STRING
- regex_pattern : STRING
- file_type : INTEGER
- file_type_enum : STRING
- file_status : INTEGER
- file_status_enum : STRING
- num_records_matched : INTEGER
- num_records_not_matched : INTEGER
- num_records_not_matched_enum : STRING
- num_records_processed : INTEGER
- current_file_position : REAL
- current_file_position_enum : STRING
- current_file_size : REAL
- current_file_size_enum : STRING
- last_modification_time : STRING
- last_modification_time_enum : STRING
- codepage : STRING

Pour les événements générés par des seuils dans le groupe d'attributs LogfileEvents, les événements sont envoyés à l'aide de la classe d'événement ITM_KLO_LOGFILEEVENTS. Cette classe d'événement contient les attributs suivants :

- node : STRING
- timestamp : STRING
- klo_class : STRING
- logname : STRING
- eifevent : STRING
- klo_msg : STRING
- customslot1 : STRING
- customslot2 : STRING
- customslot3 : STRING
- customslot4 : STRING
- customslot5 : STRING
- customslot6 : STRING
- customslot7 : STRING
- customslot8 : STRING
- customslot9 : STRING
- customslot10 : STRING
- occurrence_count : INTEGER
- occurrence_count_enum : STRING

- event_type : INTEGER
- event_type_enum : STRING
- custominteger1 : REAL
- custominteger1_enum : STRING
- custominteger2 : REAL
- custominteger2_enum : STRING
- custominteger3 : REAL
- custominteger3_enum : STRING
- remotehost : STRING

Pour les événements générés par des seuils dans le groupe d'attributs LogfileProfileEvents, les événements sont envoyés à l'aide de la classe d'événement ITM_KLO_LOGFILEPROFILEEVENTS. Cette classe d'événement contient les attributs suivants :

- node : STRING
- timestamp : STRING
- klo_class : STRING
- logname : STRING
- eifevent : STRING
- klo_msg : STRING
- customslot1 : STRING
- customslot2 : STRING
- customslot3 : STRING
- customslot4 : STRING
- customslot5 : STRING
- customslot6 : STRING
- customslot7 : STRING
- customslot8 : STRING
- customslot9 : STRING
- customslot10 : STRING
- occurrence_count : INTEGER
- occurrence_count_enum : STRING
- event_type : INTEGER
- event_type_enum : STRING
- custominteger1 : REAL
- custominteger1_enum : STRING
- custominteger2 : REAL
- custominteger2_enum : STRING
- custominteger3 : REAL
- custominteger3_enum : STRING
- remotehost : STRING

Pour les événements générés par des seuils dans le groupe d'attributs Performance Object Status, les événements sont envoyés à l'aide de la classe d'événement ITM_KLO_PERFORMANCE_OBJECT_STATUS. Cette classe d'événement contient les attributs suivants :

- node : STRING
- timestamp : STRING
- query_name : STRING
- object_name : STRING
- object_type : INTEGER
- object_type_enum : STRING
- object_status : INTEGER
- object_status_enum : STRING
- error_code : INTEGER
- error_code_enum : STRING
- last_collection_start : STRING
- last_collection_start_enum : STRING
- last_collection_finished : STRING
- last_collection_finished_enum : STRING
- last_collection_duration : REAL
- average_collection_duration : REAL
- average_collection_duration_enum : STRING
- refresh_interval : INTEGER
- number_of_collections : INTEGER
- cache_hits : INTEGER
- cache_misses : INTEGER
- cache_hit_percent : REAL
- intervals_skipped : INTEGER

Pour les événements générés par des seuils dans le groupe d'attributs pro Performance Object Status, les événements sont envoyés à l'aide de la classe d'événement ITM_KLO_PRO_PERFORMANCE_OBJECT_STATUS. Cette classe d'événement contient les attributs suivants :

- node : STRING
- timestamp : STRING
- query_name : STRING
- object_name : STRING
- object_type : INTEGER
- object_type_enum : STRING
- object_status : INTEGER
- object_status_enum : STRING
- error_code : INTEGER
- error_code_enum : STRING

- last_collection_start : STRING
- last_collection_start_enum : STRING
- last_collection_finished : STRING
- last_collection_finished_enum : STRING
- last_collection_duration : REAL
- average_collection_duration : REAL
- average_collection_duration_enum : STRING
- refresh_interval : INTEGER
- number_of_collections : INTEGER
- cache_hits : INTEGER
- cache_misses : INTEGER
- cache_hit_percent : REAL
- intervals_skipped : INTEGER

Pour les événements générés par des seuils dans le groupe d'attributs Thread Pool Status, les événements sont envoyés à l'aide de la classe d'événement ITM_KLO_THREAD_POOL_STATUS. Cette classe d'événement contient les attributs suivants :

- node : STRING
- timestamp : STRING
- thread_pool_size : INTEGER
- thread_pool_size_enum : STRING
- thread_pool_max_size : INTEGER
- thread_pool_max_size_enum : STRING
- thread_pool_active_threads : INTEGER
- thread_pool_active_threads_enum : STRING
- thread_pool_avg_active_threads : REAL
- thread_pool_avg_active_threads_enum : STRING
- thread_pool_min_active_threads : INTEGER
- thread_pool_min_active_threads_enum : STRING
- thread_pool_max_active_threads : INTEGER
- thread_pool_max_active_threads_enum : STRING
- thread_pool_queue_length : INTEGER
- thread_pool_queue_length_enum : STRING
- thread_pool_avg_queue_length : REAL
- thread_pool_avg_queue_length_enum : STRING
- thread_pool_min_queue_length : INTEGER
- thread_pool_min_queue_length_enum : STRING
- thread_pool_max_queue_length : INTEGER
- thread_pool_max_queue_length_enum : STRING
- thread_pool_avg_job_wait : REAL

- thread_pool_avg_job_wait_enum : STRING
- thread_pool_total_jobs : INTEGER
- thread_pool_total_jobs_enum : STRING

Gestion des transactions et des événements synthétiques avec Website Monitoring

Créez des transactions synthétiques qui surveillent les performances et la disponibilité des applications internes, des applications externes, et des applications Web publiques externes à différents emplacements.

Créez une *transaction synthétique* dans Synthetic Script Manager. Générez des scripts simples dans Synthetic Script Manager pour tester la disponibilité d'une application, ou utilisez Selenium IDE pour enregistrer des scripts synthétiques répliquant différentes actions utilisateur effectuées sur une application. Configurez ensuite une transaction synthétique pour exécuter votre script à des intervalles et des emplacements d'exécution spécifiques.

Important : Seuls les utilisateurs existants du module complémentaire IBM Website Monitoring on Cloud peuvent utiliser Agent Synthetic Playback et Synthetic Script Manager. L'Website Monitoring est remplacé par IBM Cloud Availability Monitoring dans l'édition d'août 2017. Pour plus d'informations, voir «A propos d'Availability Monitoring», à la page 1076.

Vos emplacements d'exécution disponibles sont les emplacements où vous avez installé Monitoring Agent for Synthetic Playback et les 15 points de présence (PoP) fournis pour la surveillance des applications Web publiques externes. Des PoP sont disponibles pour les emplacements suivants :

- Amsterdam
- Chenaï
- Dallas
- Francfort
- Hong-Kong
- Londres
- Melbourne
- Mexico
- Paris
- San José
- Sao Paolo
- Singapour
- Tokyo
- Toronto
- Washington

Créez des seuils et des groupes de ressources pour déclencher des événements et notifier les parties prenantes lorsque vos applications sont lentes ou indisponibles. Visualisez les données de performance et générez des rapports d'historique dans le Tableau de bord d'Application Performance.

Si vous surveillez le temps de réponse utilisateur final d'une application à l'aide de l'agent Temps de réponse, vous pouvez afficher les indicateurs clés de performance des transactions utilisateur final et synthétiques dans le Tableau de bord d'Application Performance. Ajoutez les transactions synthétiques en tant que composants à l'application que vous surveillez avec l'agent Temps de réponse.

Remarque : Pour travailler dans Synthetics Script Manager, vous devez être membre d'un rôle qui dispose du droit d'affichage pour Synthetic Script Manager et Configuration d'agent. Pour plus d'informations, voir «Rôles et droits», à la page 1031.

Enregistrement de scripts synthétiques

Enregistrez un script synthétique à l'aide du navigateur Web Firefox et du module complémentaire Selenium IDE.Avec Selenium IDE, vous pouvez enregistrer des actions utilisateur sur une page Web, telles que le chargement d'une page, l'activation d'un lien ou la sélection d'un objet. Lorsque Selenium IDE procède à l'enregistrement, il génère une commande pour chaque action utilisateur dans un script. Ensuite, à l'aide de Synthetic Script Manager, vous pouvez configurer les scripts de sorte à simuler un comportement utilisateur sur votre site Web, à des intervalles définis et à des emplacements différents.

Avant de commencer

Vous devez utiliser le navigateur Web Firefox lors de l'enregistrement de scripts

Selenium IDE est uniquement disponible en tant que module complémentaire Firefox. Si Selenium IDE n'est pas installé ou en cours d'exécution, procédez comme suit :

1. Vérifiez que vous exécutez une version de Firefox 60 ou ultérieure prenant en charge Selenium IDE 3.2.X ou 3.3.X. Une version ultérieure de Selenium IDE n'est pas prise en charge. Vous devez donc la désinstaller et installer la version 3.2.X ou 3.3.X.

   Remarque : Une fois cette dernière installée, Selenium IDE est mis à jour automatiquement par défaut. Désactivez les mises à jour automatiques pour Selenium IDE pour empêcher les mises à niveau de version.
2. Téléchargez et installez Selenium IDE 3.2.X ou 3.3.X à partir de la page d'accueil de **Selenium** (https://addons.mozilla.org/firefox/addon/selenium-ide/versions/). Autorisez Selenium IDE à installer tous les plug-in.
3. Lorsque Selenium IDE est installé, redémarrez Firefox.
4. Accédez à la page Web que vous souhaitez tester, puis fermez tous les autres onglets. Pour ouvrir Selenium IDE, cliquez sur **Outils** > **Selenium IDE**. Dans la fenêtre **Selenium IDE**, vérifiez que la zone **Base URL** contient l'adresse URL de la page Web affichée. Selenium IDE commence à enregistrer toutes les actions utilisateur sur la page Web affichée.

Format de script Selenium .side

Les scripts créés avec les nouvelles versions de Selenium utilisent le format `.side`. Avec Selenium IDE 3.2.X ou 3.3.X, vous pouvez importer d'anciens scripts créés au format `.html` et les sauvegarder au format `.side`. Pour plus d'informations, voir «Mise à jour des scripts à partir des versions Selenium IDE antérieures», à la page 1061.

Si vous comptez utiliser des scripts Selenium `.side`, installez au préalable les mises à jour suivantes :

- Correctif temporaire 5 ou ultérieur de IBM Cloud Application Performance Management version 8.1.4.0 Agent Synthetic Playback sur les systèmes où vous avez installé l'Agent Synthetic Playback.
- Prenez contact avec IBM pour vous assurer que votre abonnement Cloud APM a été mis à jour avec le correctif temporaire 8 ou ultérieur d'IBM IBM Cloud Application Performance Management, Private Cloud APM version 8.1.4.0.
- Si vous utilisez un point de présence privé (PoP) Availability Monitoring, vérifiez que le numéro de version de ce point de présence synthétique est `APM_201903090832` ou ultérieur en entrant la commande **`cat build.info`** à partir du répertoire d'installation PoP. Le format `.side` n'est pas pris en charge dans les versions antérieures.

Les correctifs temporaires de Cloud APM version 8.1.4.0 peuvent être téléchargés depuis Support IBM > Fix Central > IBM APM 8.1.4.0.

Pourquoi et quand exécuter cette tâche

Dans cette tâche, vous effectuez des actions utilisateur sur une page Web et utilisez Selenium IDE pour enregistrer ces actions sous la forme de commandes dans un script simple. Vous pouvez utiliser des scripts pour surveiller les performances et la disponibilité de votre application Web dans le Tableau de bord d'Application Performance.

Procédure

Pour enregistrer un script d'actions utilisateur sur une page Web, procédez comme suit :

1. Cliquez sur **Record** pour démarrer l'enregistrement d'un script. Effectuez des actions utilisateur sur votre page Web, par exemple, cliquer sur un lien.

   Pour chaque action utilisateur sur une page Web, Selenium IDE enregistre une commande et l'ajoute à un script.

   Ainsi, pour enregistrer dans un script le chargement par un utilisateur de la page Web IBM Marketplace et avoir accès à un essai gratuit de Cloud APM, procédez comme suit :

Tableau 246. Actions utilisateur enregistrées et commandes Selenium IDE

Action utilisateur	**Commandes ajoutées au script**
Pour enregistrer à quel moment la page Web Cloud APM sur le site Web IBM Marketplace s'ouvre, ouvrez la page Web IBM Marketplace. Cliquez avec le bouton droit de la souris sur un point quelconque de la page Web affichée, puis sélectionnez **open**.	`open`
Pour vérifier que le script contrôle le chargement de la page Web, cliquez avec le bouton droit de la souris sur le titre de la page Web (IBM Cloud Application Performance Management), puis cliquez sur **Afficher toutes les commandes disponibles** > **verifyTitle IBM Cloud Application Performance Management**.	`verifyTitle`
Pour enregistrer à quel moment l'utilisateur clique sur un lien pour afficher des détails sur Cloud APM, cliquez sur le lien **Détails**. La page **Détails** se charge.	`clickAndWait`
Pour vérifier que le script contrôle le chargement de la page Web **Détails**, cliquez avec le bouton droit de la souris sur l'en-tête "Feature spotlights" et sélectionnez **Afficher toutes les commandes disponibles** > **verifyText css=h2.heading--TERTIARY**.	`verifyText`
Pour enregistrer à quel moment l'utilisateur clique sur un lien pour afficher des détails relatifs à l'achat de Cloud APM, cliquez sur le lien **Acheter**. La page **Acheter** se charge.	`clickandWait`
Pour enregistrer les clics de l'utilisateur sur le bouton permettant de s'inscrire pour un essai gratuit de Cloud APM, cliquez sur le bouton **Essai gratuit**.	`click`

2. Dans la fenêtre Selenium IDE, cliquez sur **Record** pour arrêter l'enregistrement. Cliquez sur l'outil **Save Project**, donnez un nom significatif à votre script et sauvegardez en tant que fichier `.side` (par exemple, `open_webpage.side`).
3. Dans la fenêtre Selenium IDE, passez en revue le script enregistré. Cliquez sur l'onglet **Table** pour afficher le script dans un tableau. Dans la fenêtre Selenium IDE, cliquez sur **Play Current Test Case** pour tester la diffusion du script que vous avez enregistré.

   Dans cet exemple, Selenium IDE affiche le script des actions utilisateur sur le site Web IBM Marketplace, comme indiqué à l'étape 1.

Tableau 247. Exemple d'enregistrement de script Selenium IDE consignant les actions utilisateur sur le site Web IBM Marketplace

Commande	**Cible**	**Valeur**
`open`	`/`	
`verifyTitle`	`IBM Cloud Application Performance Management`	

Tableau 247. Exemple d'enregistrement de script Selenium IDE consignant les actions utilisateur sur le site Web IBM Marketplace (suite)

Commande	Cible	Valeur
clickAndWait	css=ul > #details > a	
verifyText	css=h2.heading--TERTIARY	Feature spotlights
clickAndWait	css=ul > #purchase > a	
click	link=Essai gratuit	

Résultats
Vous venez d'enregistrer un script que vous pouvez utiliser pour surveiller les performances et la disponibilité d'une application Web.

Que faire ensuite

Si vous avez enregistré un script complexe, vous pouvez organiser votre script en scripts plus simples. Chaque script représentera un processus métier ou une action utilisateur spécifique sur votre application Web.

Utilisez Synthetic Script Manager pour transférer votre fichier script vers une transaction synthétique nouvelle ou existante.

Structuration des scripts complexes
Organisez un script complexe en plusieurs scripts, puis sauvegardez les scripts ensemble dans une collection de scripts appelée *suite de tests*.

Pourquoi et quand exécuter cette tâche

Si vous créez un script complexe, vous pouvez l'organiser en plusieurs scripts simples qui représentent différents processus métier ou utilisateur dans votre application Web. Sauvegardez les scripts ensemble en tant que suite de tests. Vous pouvez alors utiliser ces scripts pour surveiller les performances et la disponibilité de votre application Web en réponse à des actions utilisateur spécifiques dans le Tableau de bord d'Application Performance.

Il ne doit y avoir qu'une suite de tests et tous les tests doivent y être ajoutés.

Important : Il est recommandé d'organiser les scripts complexes en scripts distincts, chaque script représentant un processus utilisateur ou métier spécifique à surveiller. Par exemple, créez des scripts distincts qui enregistrent la recherche d'un élément ou la connexion, par un utilisateur, à un site Web. Si vous organisez vos scripts par processus utilisateur ou métier, vous pouvez alors surveiller la réponse de votre application Web à ces processus spécifiques dans le Tableau de bord d'Application Performance.

Procédure

Pour organiser un script complexe en scripts distincts et sauvegarder vos scripts en tant que suite de tests, procédez comme suit :

1. Pour créer un script distinct pour chaque processus utilisateur enregistré dans votre script, cliquez sur **Tests** > **+** Dans Selenium IDE. Attribuez à chaque script un nom significatif décrivant le processus utilisateur et sauvegardez chaque script en tant que fichier `.side`, par exemple, `load_homepage.side`.

   Pour plus d'informations, voir «Enregistrement de scripts synthétiques», à la page 1058.

   Important : Le nom attribué à votre script dans Selenium IDE est le nom qui identifie le processus métier ou utilisateur enregistré que vous surveillez dans le Tableau de bord d'Application Performance.
2. Dans Selenium IDE, ouvrez un script complexe déjà enregistré. Organisez vos commandes de script dans des scripts distincts, en fonction des différentes actions utilisateur. **Coupez** les commandes dans

le script complexe initial dans la fenêtre **Scénario de test**, et **Collez** les commandes la fenêtre **Scénario de test**.

Par exemple, l'exemple de script complexe de la rubrique Enregistrement de scripts synthétiques contient les commandes Selenium IDE associées aux trois processus utilisateur possibles.

- Ouvrez la page d'accueil Cloud APM sur le site Web IBM Marketplace.
- Ouvrez la page **Details** sur IBM Marketplace.
- Ouvrez la page **Tarification** et enregistrez l'ouverture par l'utilisateur de la page d'inscription à un essai gratuit.

Les actions utilisateur sont alors organisées selon trois scripts distincts.

Tableau 248. Exemple de script correspondant à l'ouverture de la page IBM Marketplace (`load_homepage.side`)

Commande	Cible	Valeur
`open`	`/`	
`verifyTitle`	`IBM Cloud Application Performance Management`	

*Tableau 249. Exemple de script correspondant à l'ouverture de la page **Détails** dans IBM Marketplace (`load_products.side`)*

Commande	Cible	Valeur
`clickAndWait`	`css=ul > #details > a`	
`verifyText`	`css=h2.heading--TERTIARY`	Feature spotlights

*Tableau 250. Exemple de script correspondant à l'ouverture de la page **Acheter** et de la page d'inscription à l'essai dans IBM Marketplace (`load_APM.side`)*

Commande	Cible	Valeur
`clickAndWait`	`css=ul > #purchase > a`	
`click`	`link=Essai gratuit`	

3. Pour ajouter des scénarios de test individuels à une suite de tests, accédez à la fenêtre **Suite de tests** et ajoutez des tests à la suite de tests en fonction de la séquence de logique métier. Enfin, cliquez sur l'outil **Sauvegarder le projet** pour sauvegarder la suite de tests et tous les tests de la suite de tests dans un fichier `.side`.
   Prenons l'exemple de la séquence logique `Load_URL`, `Select Manage inventory`, `Select IBM Machine Type`. Lorsque ces scénarios de test sont ajoutés à la suite de tests, `Load_URL` est d'abord vérifié, puis `Select Manage inventory`, et enfin `Select IBM Machine Type`.

Résultats
Vous venez d'enregistrer un ensemble de scripts que vous pouvez utiliser pour surveiller les performances et la disponibilité de vos applications Web. Utilisez Synthetic Script Manager pour transférer votre suite de tests de scripts `.side` vers une transaction synthétique nouvelle ou existante.

Mise à jour des scripts à partir des versions Selenium IDE antérieures
Les versions Selenium IDE 2.2.X et 3.2.X prises en charge utilisent le format `.side` pour enregistrer les scripts synthétiques, tandis que les versions plus anciennes emploient le format `.html`. Les scripts `.html` existants sont toujours utilisables. Ceux qui ont été créés avec d'anciennes versions de Selenium IDE peuvent ne pas être entièrement fonctionnels avec les derniers pilotes Firefox et Selenium utilisés par IBM Cloud Availability Monitoring. Dans certains cas, il peut s'avérer nécessaire de modifier les scripts `.html`, de les enregistrer à nouveau dans le nouveau format `.side` ou d'importer le script `.html` pour le sauvegarder au format `.side`.

Procédure

- Exception : Si vous souhaitez interagir avec l'élément `Select2`, n'utilisez pas la commande **`select`** (voir https://github.com/SeleniumHQ/selenium-ide).

  L'ancien script est

  ```
  <td>select</td>
  <td>id=country</td>
  <td>label=United States</td>
  ```

  It should be changed to

  ```
  <tr>
     <td>runScript</td>
     <td>window.scrollTo(0,810)</td>
     <td></td>
  </tr>
  <tr>
     <td>click</td>
     <td>id=select2-country-container</td>
     <td></td>
  </tr>
  <tr>
     <td>click</td>
     <td>xpath=(//ul[@id='select2-country-results']/li[text() = 'United States'])</td>
     <td></td>
  </tr>
  ```

- Limitation : les scripts `.side` enregistrés avec Selenium IDE 3.2.X ou 3.3.X sont pris en charge, contrairement au releveur de coordonnées **`linkText`**.

Gestion des transactions synthétiques
Utilisez Synthetic Script Manager pour créer, configurer et supprimer des transactions synthétiques.

Pour afficher Synthetic Script Manager, cliquez sur l'icône **Configuration du système** et sélectionnez **Synthetic Script Manager**. Pour travailler dans Synthetics Script Manager, vous devez être membre d'un rôle qui dispose du droit d'affichage pour **Synthetic Script Manager** et **Configuration d'agent**. Pour plus d'informations, voir «Rôles et droits», à la page 1031.

Vous pouvez afficher des données sur l'utilisation de vos transactions synthétiques pour le mois en cours, pour les applications Web à disposition du public. Affichez le nombre d'instances de réexécutions effectuées et d'instances de réexécutions prévues en fonction de votre configuration actuelle pour le mois en cours dans le tableau d'utilisation de la réexécution mensuelle de Synthetic Script Manager.

Important : Pour créer des transactions synthétiques pour les applications Web internes privées et les applications Web externes privées, vous devez installer l'Agent Synthetic Playback à chaque emplacement contenant une application Web que vous voulez surveiller.

Vous pouvez effectuer les tâches suivantes à l'aide de Synthetic Script Manager :

- Créer et éditer une transaction synthétique.
- Configurer des variables de transaction synthétique.
- Supprimer une transaction synthétique.

Création et édition d'une transaction synthétique
Pour visualiser les données relatives aux performances et à la disponibilité d'une application Web, vous devez commencer par créer une transaction synthétique dans Synthetic Script Manager.

Pourquoi et quand exécuter cette tâche
Utilisez Synthetic Script Manager pour créer, éditer et configurer une transaction synthétique. Entrez l'adresse URL d'une application Web dans Synthetic Script Editor pour générer un script simple pour votre transaction synthétique. Pour simuler des processus utilisateur complexes, transférez un script synthétique vers une transaction synthétique dans Synthetic Script Editor. Configurez ensuite votre transaction synthétique pour l'exécuter à intervalles réguliers et à différents emplacements.

Procédure

Pour créer une transaction ou éditer une transaction existante, procédez comme suit :

1. Facultatif : Si Synthetic Script Manager n'est pas affiché, cliquez sur l'icône **Configuration du système** et sélectionnez **Synthetic Script Manager**.
2. Pour créer une transaction, cliquez sur l'icône **Nouveau**. Pour modifier une transaction existante, cliquez sur l'icône **Editer**.
3. Dans **Synthetic Script Editor**, cliquez sur l'onglet **Upload a Script** et entrez un nom de transaction dans la zone de texte **Nom de transaction**. Entrez une description de votre transaction dans la zone de texte **Description**.

   Important : N'attribuez pas à votre transaction le même nom que celui d'une transaction que vous avez supprimée ces dernières 24 heures. Sinon, les données issues des deux transactions ne seront pas correctement attribuées à ce nom de transaction dans le Tableau de bord d'Application Performance.
4. Pour générer un script simple afin de tester une application Web, sélectionnez **Enter the URL of web page to test** et entrez une URL. Synthetic Script Manager génère un script synthétique simple en se basant sur cette URL.
5. Pour affecter un fichier script créé précédemment à votre transaction, sélectionnez **Upload script file**. Cliquez sur **Télécharger un script** pour parcourir les scripts sur votre système. Choisissez un script et cliquez sur **Ouvrir**.

   Important : Le fichier script synthétique doit être de l'un des types de fichier suivants :

   - `.html`
   - `.zip`

   Sauvegardez des scripts individuels simples (scénarios de test) sous la forme de fichiers `.html`. Compressez les scénarios de test et les suites de tests ensemble dans un fichier `.zip`.
6. Pour configurer une réexécution simultanée ou échelonnée d'une transaction synthétique, cliquez sur l'onglet **Planifier un script**. Sélectionnez **Simultanée** pour exécuter la transaction à partir de tous les emplacements simultanément, ou **Echelonnée** pour exécuter la transaction à partir d'un autre emplacement à chaque intervalle.
7. Pour choisir la fréquence d'exécution d'un script, cliquez sur l'onglet **Planifier un script**. Cliquez sur la zone de texte **Intervalle** et saisissez un nombre, en fonction de la fréquence de surveillance souhaitée de votre application Web. Choisissez une durée d'intervalle comprise entre 1 et 60 minutes.

   Remarque : Les scripts volumineux ou complexes peuvent prendre plus de temps à s'exécuter. Choisissez une durée d'intervalle plus longue pour les scripts volumineux ou complexes.
8. Pour choisir les emplacements d'exécution de votre script, cliquez sur l'onglet **Planifier un script**, puis sélectionnez les emplacements de centre de données et les emplacements d'installation de l'agent où vous voulez exécuter votre script.
9. Pour définir des seuils de temps de réponse pour les transactions et sous-transactions synthétiques, cliquez sur l'onglet **Paramètres avancés** ; cliquez ensuite sur une transaction synthétique et développez-la pour révéler toutes les sous-transactions. Cliquez deux fois sur la valeur du seuil de temps de réponse et entrez une valeur. Choisissez une valeur comprise entre `0` et `3600` secondes. Si vous ne souhaitez pas définir de seuil, entrez `0`. La valeur du seuil de temps de réponse par défaut est 10 secondes.

   Remarque : Certaines commandes peuvent prendre plus de temps que d'autres. Choisissez un seuil de temps de réponse qui convient à la commande que vous souhaitez tester. Si votre transaction teste le délai d'ouverture d'une page Web, choisissez un temps de réponse plus long.
10. Pour terminer la création ou l'édition de votre transaction, cliquez sur **Sauvegarder**.

Résultats
Vous venez de configurer une transaction synthétique. La transaction synthétique est à présent répertoriée dans Synthetic Script Manager.

Que faire ensuite
Vous pouvez visualiser les mesures et les indicateurs clés de performance enregistrés par une transaction synthétique dans le Tableau de bord d'Application Performance. Vous pouvez également ajouter des transactions sous la forme de composants à une application et visualiser toutes les transactions synthétiques associées à cette application.

Important : Lorsque vous ajoutez une transaction synthétique pour la première fois, un espace vide peut apparaître dans le widget de groupe **Disponibilité dans le temps** du Tableau de bord d'Application Performance. L'espace vide disparaît rapidement lorsque le serveur reçoit les premiers résultats d'exécution de la transaction.

Configuration des variables de transaction synthétique
Utilisez Synthetic Script Manager pour mettre à jour des valeurs de variable, telles que des noms et des mots de passe d'utilisateur stockés dans des scripts synthétiques, sans avoir à éditer les fichiers script. Les valeurs des variables doivent être uniques pour chaque site d'exécution.Configurez des variables pour vos scripts synthétiques lorsque vos applications Web requièrent différentes valeurs de variables sur différents sites. Par exemple, si votre application Web ne permet pas d'avoir les mêmes détails de connexion sur différents sites, utilisez Synthetic Script Manager pour fournir des détails de connexion différents sur chaque site. Vous pouvez créer des variables dans des scripts synthétiques à l'aide de la commande `store` dans le plug-in Selenium-IDE.

Pourquoi et quand exécuter cette tâche

Dans cette tâche, utilisez Synthetic Script Manager pour configurer des variables stockées dans votre script synthétique.

Procédure

Pour configurer les variables d'une transaction synthétique, procédez comme suit :

1. Si Synthetic Script Manager n'est pas affiché, cliquez sur l'icône **Configuration du système** et sélectionnez **Synthetic Script Manager**. Sélectionnez une transaction synthétique dans la liste et cliquez sur l'icône **Editer** .
2. Sélectionnez les sites d'exécution de votre transaction synthétique.
3. Cliquez sur l'onglet **Paramètres avancés**. Si le script synthétique contient des variables, vous pouvez éditer ces variables dans la fenêtre **Configurer les substitutions de variable pour les différents sites**. Pour éditer une variable, cliquez deux fois sur la valeur. Pour terminer, cliquez sur **Sauvegarder**.

   Par exemple, le script suivant contient les variables *nom_utilisateur* et *mot_de_passe*. Les valeurs de ces variables, `user1` et `pass`, sont enregistrées à l'aide de la commande `store` dans Selenium-IDE. Les variables ont la même valeur sur deux sites, Dallas et San Jose.

   Tableau 251. Exemple de script contenant des variables

Commande	Cible	Valeur
`store`	`user1`	*nom_utilisateur*
`store`	`pass`	*mot_de_passe*
`type`	`id=j_username`	*${nom_utilisateur}*
`type`	`id=j_password`	*${mot_de_passe}*

   Les valeurs des variables de script sont affichées dans la fenêtre **Configurer les substitutions de variable pour les différents emplacements**. Remplacez la valeur `user1` de *nom_utilisateur* utilisée

sur le site `Dallas` par la valeur `admin1` de sorte que la transaction synthétique utilise des détails de connexion différents sur chaque site.

Tableau 252. Valeurs de variables de script à différents emplacements

Emplacement	nom d'utilisateur	mot de passe
San Jose	user1	pass
Dallas	admin1	pass

Résultats
Vous venez de configurer les variables d'une transaction synthétique. Vous pouvez désormais utiliser cette transaction synthétique pour tester les performances et la disponibilité d'une application Web sur différents sites.

Que faire ensuite
Vous pouvez visualiser les mesures et les indicateurs clés de performance enregistrés par une transaction synthétique dans le Tableau de bord d'Application Performance. Vous pouvez également ajouter des transactions sous la forme de composants à une application et visualiser toutes les transactions synthétiques associées à cette application.

Filtrage des URL et des noms de domaine pour vos transactions synthétiques
Utilisez Synthetic Script Manager pour autoriser ou bloquer l'accès à des URL et des domaines spécifiques en ajoutant des règles à la liste blanche et la liste noire pour votre test.

Pourquoi et quand exécuter cette tâche

Vous pouvez contrôler les dépendances et les ressources qui contribuent aux temps de réponse de vos applications Web testées. Utilisez la liste noire pour filtrer les requêtes des domaines spécifiés afin de retirer ces requêtes de vos temps de réponse mesurés. Utilisez la liste blanche pour inclure les requêtes des domaines spécifiés afin d'ajouter ces requêtes à vos temps de réponse mesurés. Utilisez la liste noire et la liste blanche pour filtrer ou inclure les dépendances associées à votre application Web, telles que des indicateurs tiers.

La zone **Liste noire** contient une liste de règles qui bloquent l'accès aux URL et aux domaines spécifiés.

La zone **Liste blanche** contient une liste de règles qui autorisent l'accès aux URL et aux domaines spécifiés.

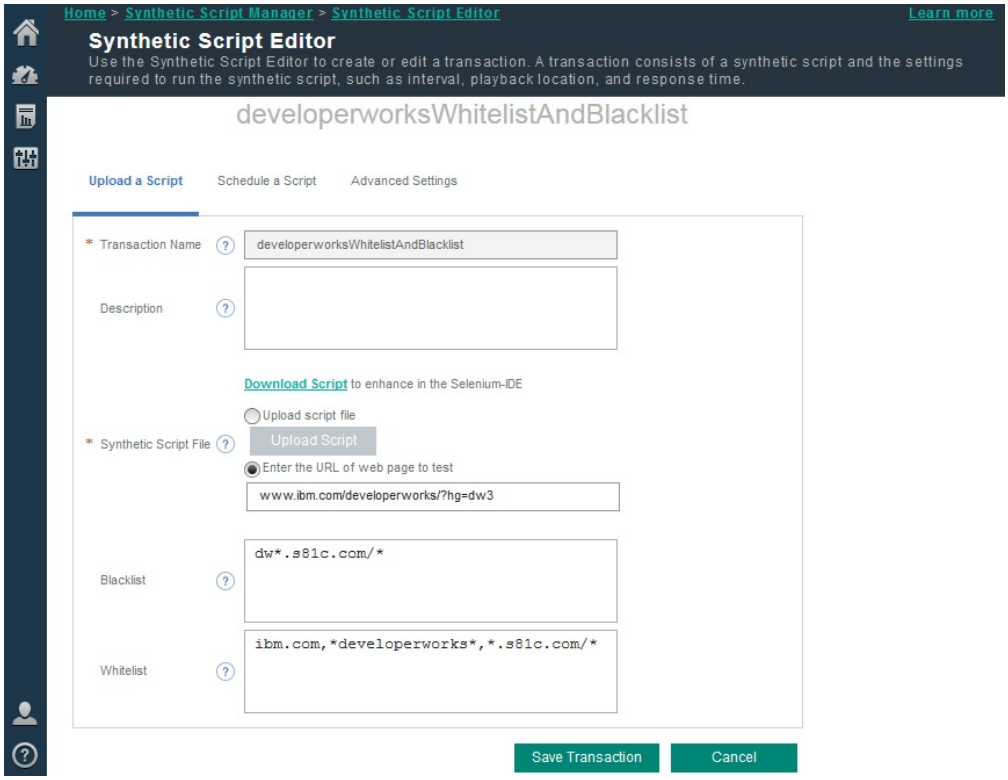
Utilisez des virgules (,) pour séparer les règles dans votre liste noire et votre liste blanche. Utilisez le symbole de caractère générique (*) pour filtrer les noms de domaines et d'URL. Par exemple, `ibm.com, *.bluemix.net, *developerworks*, *.profile.*.cloundfront.net/*.png`.

Remarque : Si vous configurez une liste noire et une liste blanche pour votre transaction synthétique, la liste noire a une priorité plus élevée.

Procédure

Pour ajouter une règle à la liste noire ou la liste blanche pour votre transaction synthétique, procédez comme suit :

1. Si Synthetic Script Manager n'est pas affiché, cliquez sur l'icône **Configuration du système** et sélectionnez **Synthetic Script Manager**.
2. Pour configurer votre liste noire ou liste blanche pour une transaction existante, cliquez sur l'icône **Editer**. Si aucune transaction n'est listée, cliquez sur l'icône **Nouveau** pour créer une nouvelle transaction.
3. Dans **Synthetic Script Editor**, cliquez sur l'onglet **Upload a Script** et entrez un nom de transaction dans la zone de texte **Nom de transaction**. Ajoutez des règles aux zones de texte **Liste noire** et **Liste blanche**.



Résultats
Votre transaction synthétique filtre maintenant les demandes indésirables pour votre application Web et autorise l'accès à d'autres requêtes spécifiques.

Instructions pour masquer les mots de passe dans Synthetic Script Manager
Stockez les mots de passe sous forme de variables dans vos scripts synthétiques pour masquer leurs valeurs dans Synthetic Script Manager.

Avant de commencer
Cette procédure requiert la modification d'un script synthétique. Enregistrez un script synthétique à l'aide de Selenium IDE. Pour plus d'informations, voir «Enregistrement de scripts synthétiques», à la page 1058.

Pourquoi et quand exécuter cette tâche

Modifiez manuellement vos scripts synthétiques dans Selenium IDE pour stocker votre mot de passe sous forme de variable. Vous pourrez ensuite créer des transactions synthétiques avec des mots de passe masqués dans Synthetic Script Manager. Les mots de passe masqués s'affichent sous forme d'astérisques dans Synthetic Script Manager.

Important : Il est recommandé de stocker vos mots de passe dans des scripts synthétiques de sorte que leurs valeurs n'apparaissent pas dans Synthetic Script Manager. Les autres utilisateurs ne pouvant pas les voir, les mots de passe masqués offrent une sécurité supplémentaire pour vos applications Web.

Procédure

1. Ouvrez le script que vous voulez modifier dans Selenium-IDE. Utilisez la commande `store` pour affecter un mot de passe à la variable *mot_de_passe*, selon l'exemple décrit dans cette étape. Ensuite, enregistrez le script.

   Important : Vous devez stocker le mot de passe sous le nom de variable *mot_de_passe* afin qu'il ne s'affiche pas dans Synthetic Script Manager.

Par exemple, le script synthétique ci-dessous contient un nom d'utilisateur *test@exemple.com* et une valeur de mot de passe *valeur4-ibm*.

```
<tr>
   <td>type</td>
   <td>id=nom_utilisateur</td>
   <td>test@exemple.com</td>
</tr>
<tr>
   <td>type</td>
   <td>id=mot_de_passe</td>
   <td>valeur4-ibm</td>
</tr>
```

Le script ci-dessous indique comment affecter la valeur de mot de passe *valeur4-ibm* à la variable *mot_de_passe* à l'aide de la commande `store`.

```
<tr>
   <td>store</td>
   <td>valeur4-ibm</td>
   <td>mot_de_passe</td>
</tr>
<tr>
   <td>type</td>
   <td>id=username</td>
   <td>test@exemple.com</td>
</tr>
<tr>
   <td>type</td>
   <td>id=mot_de_passe</td>
   <td>$(mot_de_passe)</td>
</tr>
```

2. Facultatif : Pour masquer le mot de passe au niveau du script, affectez une valeur vide à la variable *mot_de_passe* à l'aide de la commande `store`, puis enregistrez le script.

   Vous pouvez définir le mot de passe ultérieurement dans Synthetic Script Manager.

   Par exemple, le script ci-dessous indique comment affecter une valeur vide à la variable *mot_de_passe* à l'aide de la commande `store`.

```
<tr>
   <td>store</td>
   <td></td>
   <td>mot_de_passe</td>
</tr>
<tr>
   <td>type</td>
   <td>id=nom_utilisateur</td>
   <td>test@exemple.com</td>
</tr>
<tr>
   <td>type</td>
   <td>id=mot_de_passe</td>
   <td>$(mot_de_passe)</td>
</tr>
```

3. Connectez-vous à la console Cloud APM et ouvrez **Synthetic Script Manager**. Créez une transaction et téléchargez votre script dans cette transaction. Cliquez sur l'onglet **Paramètres avancés**.

   Le mot de passe est masqué pour chaque localisation. Vous pouvez modifier le mot de passe pour chaque localisation. Pour plus d'informations, voir «Gestion des transactions synthétiques», à la page 1062.

Suppression d'une transaction synthétique

Utilisez Synthetic Script Manager pour supprimer des transactions synthétiques.

Procédure

Pour supprimer une transaction synthétique, procédez comme suit :

1. Si une transaction synthétique est affectée à une application, vous devez commencer par supprimer la transaction de cette application. Sur le Tableau de bord d'Application Performance, cliquez sur **Toutes**

mes applications et développez, puis cliquez sur l'application qui est associée à la transaction synthétique que vous voulez supprimer. Cliquez sur l'icône **Editer** . Dans la fenêtre **Modification d'application**, supprimez le composant de transaction synthétique de l'application. Pour plus d'informations, voir Gestion des applications.

La transaction synthétique peut désormais être supprimée.

2. Dans la barre de navigation, cliquez sur l'icône **Configuration système** et sélectionnez **Synthetic Script Manager**. Sélectionnez une transaction synthétique, puis cliquez sur l'icône **Supprimer** . Pour confirmer que vous souhaitez supprimer cette transaction synthétique, cliquez sur **OK**.

Résultats
La transaction synthétique est supprimée.

Affichage des données d'une transaction synthétique dans le Tableau de bord d'Application Performance

Affichez les données de transaction synthétique dans le Tableau de bord d'Application Performance. Associez les transactions synthétiques à une application nouvelle ou existante et affichez toutes les transactions synthétiques associées dans le Tableau de bord d'Application Performance.

Pourquoi et quand exécuter cette tâche

Vous pouvez afficher les données de transaction synthétique dans la fenêtre **My Transactions** du Tableau de bord d'Application Performance.

Vous pouvez également créer des groupes de transactions synthétiques en associant vos transactions à une application. Utilisez l'outil **Ajouter une application** ou **Modifier une application** du Tableau de bord d'Application Performance pour ajouter des transactions synthétiques sous la forme de composants à une application Web nouvelle ou existante. Vous pouvez ensuite afficher les données de toutes les transactions synthétiques qui sont associées à cette application dans le Tableau de bord d'Application Performance.

Si vous utilisez déjà l'agent Temps de réponse pour surveiller le temps de réponse utilisateur pour une application, vous pouvez ajouter une transaction synthétique à cette application. Vous pouvez alors visualiser des mesures et des indicateurs clés de performance supplémentaires pour cette application dans le Tableau de bord d'Application Performance.

Procédure

- Pour afficher les transactions synthétiques, procédez comme suit :
  a) Cliquez sur l'icône **Performance** et sélectionnez **Tableau de bord d'Application Performance**. Dans la fenêtre **Applications**, développez **Toutes mes applications** et sélectionnez **My Transactions**. Dans la fenêtre **Groupes**, développez **Transactions** et sélectionnez **Transactions synthétiques**.
  b) Cliquez sur une transaction synthétique pour afficher les données de disponibilité et de performance de cette transaction, avec un graphique des temps de réponse pour les instances de transaction sur une période définie.
- Pour associer des transactions synthétiques à une application, procédez comme suit :
  a) Cliquez sur l'icône **Performance** et sélectionnez **Tableau de bord d'Application Performance**. Sélectionnez et éditez une application existante ou créez une application. Pour plus d'informations, voir Gestion des applications.
  b) Dans la fenêtre **Ajouter une application**, cliquez sur l'icône **Ajouter des composants** et sélectionnez **Transactions synthétiques** dans la liste des composants. Dans la fenêtre **Editeur de composants**, sélectionnez une transaction synthétique et cliquez sur **Ajouter** pour associer la transaction synthétique à l'application.
  c) Cliquez sur **Précédent**. Cliquez sur **Fermer** pour fermer la fenêtre **Editeur de composants**. Cliquez sur **Sauvegarder**. Pour ajouter une autre transaction synthétique sous la forme d'un composant, répétez les étapes 1 à 3.

Résultats
Vous venez d'associer une transaction synthétique à une application. Vous pouvez désormais afficher l'application et ses transactions synthétiques associées dans le Tableau de bord d'Application Performance. Pour plus d'informations, voir Gestion des applications.

Remarque : Lorsque vous associez une transaction synthétique à une application, la disponibilité initiale de cette application est inconnue. La mise à jour du statut peut prendre plusieurs minutes.

Gestion des événements synthétiques
Utilisez le gestionnaire de seuils et le gestionnaire de groupes de ressources pour configurer les seuils et les affecter à des transactions synthétiques. Les événements synthétiques sont générés lorsque la valeur d'un attribut de transaction correspond à la condition définie dans le seuil. Vous pouvez surveiller les événements synthétiques dans le Tableau de bord d'Application Performance.

Création d'un seuil pour les transactions synthétiques
Utilisez le gestionnaire de seuils pour créer des seuils destinés aux transactions synthétiques. Les seuils sont utilisés pour comparer les valeurs d'attribut aux valeurs définies dans le seuil. Si la valeur d'échantillon répond à la comparaison, un événement est généré.

Pourquoi et quand exécuter cette tâche

Les seuils permettent aux utilisateurs de surveiller la signalisation de conditions spécifiques par les applications. Par exemple, vous pouvez créer un seuil pour surveiller le délai utilisé par un site Web pour répondre à une commande utilisateur spécifique. Si le site Web met plus de temps que le délai spécifié par votre seuil, un événement synthétique est généré.

Procédure

Pour créer un seuil et l'associer à une ou plusieurs transactions synthétiques, procédez comme suit :

1. Dans la barre de navigation, cliquez sur l'icône **Configuration du système** et sélectionnez **Gestionnaire de seuils**. Définissez le type de **source de données** sur **Synthetic Transaction** (Transaction synthétique).
2. Créez un seuil. Pour plus d'informations, voir «Gestionnaire de seuils», à la page 1014.
3. Pour associer le seuil à une transaction, sélectionnez **KSO TRANSACTION** comme **Ensemble de données**, puis sélectionnez **TRANSNAME** comme **Elément affiché**. Pour l'**Opérateur logique**, sélectionnez **And (&)**.

   Remarque : Vous devez sélectionner **TRANSNAME** comme **Elément affiché**. Si vous ne sélectionnez pas **TRANSNAME**, vous ne pouvez pas visualiser les événements synthétiques dans le tableau de bord d'Application Performance.
4. Pour ajouter une condition, cliquez sur l'icône **Nouvelle condition**. Dans la zone New Condition, sélectionnez un **attribut** et un **opérateur**. Saisissez ensuite une valeur de seuil dans la zone **Valeur**. Pour ajouter cette condition au seuil, cliquez sur **OK**.

   Par exemple, pour ajouter une condition de seuil qui génère un événement synthétique lorsque plus de 50 % des transactions sont lentes, sélectionnez **PSLOW** comme **Attribut** et **Supérieur à** comme **Opérateur**. Pour définir le pourcentage de transactions lentes pour générer un événement, entrez 50 comme **Valeur**.
5. Pour définir plus d'attributs de seuil, ajoutez plus de conditions à votre seuil.
6. Une fois que vous avez terminé, cliquez sur **Sauvegarder**. Si vous ne souhaitez pas affecter le seuil à un groupe de ressources, cliquez sur **OK**.

Résultats
Vous venez de créer un seuil et l'avez associé à une transaction synthétique. Lorsque les conditions de seuil sont remplies, un événement est généré. Vous pouvez surveiller les événements dans l'onglet **Evénements** du Tableau de bord d'Application Performance.

Que faire ensuite
Vous pouvez regrouper vos transactions synthétiques en groupes de ressources.

Création d'un groupe de ressources pour les transactions synthétiques
Organisez vos transactions synthétiques dans un groupe de ressources et appliquez des seuils à toutes les transactions de ce groupe de ressources.

Avant de commencer
Créez un seuil à appliquer à toutes les transactions synthétiques de votre groupe de ressources.

Pourquoi et quand exécuter cette tâche

Vous pouvez organiser vos transactions synthétiques en groupes de ressources et appliquer des seuils à chaque transaction synthétique de ce groupe de ressources. Utilisez le gestionnaire de groupes de ressources pour créer un groupe de ressources, et affectez un seuil à ce groupe de ressources. Affectez ensuite un ou plusieurs sous-noeuds de transactions synthétiques à ce groupe de ressources. Le seuil associé au groupe de ressources s'applique désormais à toutes les transactions synthétiques associées.

Procédure

Pour créer un groupe de ressources pour les transactions synthétiques, procédez comme suit :

1. Cliquez sur l'icône **Configuration système** et sélectionnez **Gestionnaire de groupes de ressources**. Créez un groupe de ressources ou éditez un groupe de ressources existant. Pour plus d'informations, voir «Gestionnaire de groupes de ressources», à la page 1008.

Pour créer un groupe de ressources pour les transactions synthétiques, procédez comme suit :

2. Attribuez un nom et une description à votre groupe de ressources. Dans la table **Threshold Assignment**, affectez un seuil à votre groupe de ressources, puis cliquez sur **Sauvegarder**. Dans le gestionnaire de groupes de ressources, sélectionnez à nouveau votre groupe de ressources et cliquez sur l'icône **Editer** .
3. Associez votre groupe de ressources aux sous-noeuds de transaction synthétique à partir de la table **Affectation de ressource** et cliquez sur **Sauvegarder**.

   Le format des sous-noeuds de transaction synthétique est S0:*NomTransaction*. Par exemple, si l'une de vos transactions se nomme open_webpage, le sous-noeud disponible porte le nom S0:open_webpage.

Résultats
Vous venez d'organiser vos transactions synthétiques dans un groupe de ressources et d'appliquer un seuil à chaque transaction de ce groupe de ressources.

Création de seuils critiques pour des transactions synthétiques simultanées et échelonnées
Utilisez le Gestionnaire de seuils pour créer des seuils critiques pour les transactions synthétiques simultanées et échelonnées.

Pourquoi et quand exécuter cette tâche

Créez des seuils qui informent les parties prenantes quand des transactions échelonnées consécutives échouent, ou quand des transactions simultanées échouent sur tous les emplacements de réexécution. Pour plus d'informations, voir «Création et édition d'une transaction synthétique», à la page 1062.

Procédure

Pour créer un seuil critique qui crée un événement quand des instances de réexécution de transaction échelonnée échouent, procédez comme suit :

1. Créez un seuil pour les transactions synthétiques dans le Gestionnaire de seuils. Pour plus d'informations, voir «Création d'un seuil pour les transactions synthétiques», à la page 1069.

2. Dans le Gestionnaire de seuils, sélectionnez **Critique** pour la **Gravité** et entrez 1 minute comme **Intervalle (HHMMSS)** de seuil. Employez la formule suivante pour déterminer les **Echantillons consécutifs requis** :

   Echantillons consécutifs requis = (intervalle de réexécution * échecs consécutifs attendus) - 1

   Par exemple, si l'intervalle de réexécution de la transaction synthétique que vous souhaitez surveiller est de 5 minutes, et que vous souhaitez détecter 8 échecs de réexécution consécutifs, vous devez définir **Echantillons consécutifs requis** sur (5 * 8) - 1 = 39.
3. Ajoutez une condition. Dans la zone Nouvelle condition, sélectionnez **LOCATION** en tant qu'**Attribut**, sélectionnez **Egal à** en tant qu'**Opérateur** et entrez Aucun en tant que **Valeur**. Ajoutez une deuxième condition et définissez **PFAILED** = 100. Sauvegardez le seuil.
4. Dans la barre de navigation, ouvrez le **Gestionnaire de groupes de ressources**. Créez un groupe de ressources. Affectez une ou plusieurs transactions synthétiques échelonnées à votre groupe de ressources, puis affectez le seuil que vous avez créé dans les étapes 1 à 3 à votre groupe de ressources. Sauvegardez le groupe de ressources. Pour plus d'informations, voir «Création d'un groupe de ressources pour les transactions synthétiques», à la page 1070.

Pour créer un seuil critique qui crée un événement quand des instances de réexécution de transaction simultanée échouent, effectuez les étapes suivantes :

5. Créez un seuil pour les transactions synthétiques dans le Gestionnaire de seuils. Pour plus d'informations, voir «Création d'un seuil pour les transactions synthétiques», à la page 1069.
6. Dans le Gestionnaire de seuils, sélectionnez **Critique** pour la **Gravité** et entrez 1 minute comme **Intervalle (HHMMSS)**. Définissez **Echantillons consécutifs requis** sur la même valeur que l'intervalle de réexécution de la transaction que vous voulez surveiller.

   Par exemple, si l'intervalle de réexécution de la transaction synthétique que vous voulez surveiller est de 5 minutes, définissez **Echantillons consécutifs requis** sur 5.
7. Ajoutez une condition. Dans la zone Nouvelle condition, sélectionnez **LOCATION** en tant qu'**Attribut**, sélectionnez **Egal à** en tant qu'**Opérateur** et entrez Aucun en tant que **Valeur**. Ajoutez une deuxième condition et définissez **PFAILED** = 100. Sauvegardez le seuil.
8. Créez un groupe de ressources. Affectez une ou plusieurs transactions synthétiques et le nouveau seuil critique à votre groupe de ressources. Pour plus d'informations, voir «Création d'un groupe de ressources pour les transactions synthétiques», à la page 1070.

Résultats

Vous avez créé un seuil critique pour une transaction synthétique échelonnée ou simultanée. Lorsque les conditions de seuil sont remplies, un événement est généré. Vous pouvez surveiller les événements dans l'onglet **Evénements** du Tableau de bord d'Application Performance.

Gestion des notifications par courrier électronique relatives aux événements synthétiques

Le gestionnaire de groupes de ressources et IBM Alert Notification génèrent des notifications par courrier électronique lorsque les performances de votre application dépassent le seuil.

Avant de commencer

Pour configurer des notifications par courrier électronique pour des événements synthétiques, vous devez d'abord activer Alert Notification dans le cadre de votre abonnement. Pour plus d'informations, voir Alert Notification dans l'IBM Knowledge Center.

Pourquoi et quand exécuter cette tâche

Dans le Gestionnaire de groupes de ressources, employez Alert Notification pour configurer des notifications par courrier électronique. Les notifications par courrier électronique sont générées lorsque les performances de vos applications remplissent les conditions définies par les seuils associés à votre groupe de ressources.

Procédure

Pour gérer les notifications par courrier électronique, procédez comme suit :

1. Cliquez sur l'icône **Configuration système** et sélectionnez **Gestionnaire de groupes de ressources**. Créez ou éditez un groupe de ressources.
2. Sélectionnez un seuil dans la table **Affectation de seuil** et cliquez sur **Sauvegarder**. Puis, associez votre groupe de ressources à une ressource Synthetic Playback ou une ressource d'agent Synthetic Events dans la table **Affectation de ressource**. Cliquez sur **Sauvegarder**. Dans le gestionnaire de groupes de ressources, sélectionnez à nouveau votre groupe de ressources et cliquez sur l'icône **Editer** .
3. Pour démarrer Alert Notification dans un nouvel onglet, cliquez sur **Configurer la notification par courrier électronique** dans le gestionnaire de groupes de ressources. Dans Alert Notification, cliquez sur **Utilisateurs** dans la barre de navigation pour créer ou éditer des destinataires des notifications par courrier électronique. Pour plus d'informations, voir Alert Notification dans l'IBM Knowledge Center.
4. Dans Alert Notification, cliquez sur **Notification Policies** dans la barre de navigation. L'**éditeur de notifications** est automatiquement alimenté avec une nouvelle règle. Le nom et le filtre de la règle sont dérivés du groupe de ressources. Cliquez sur **Add Rule** pour définir les conditions qui déterminent l'envoi d'une notification par courrier électronique. Pour plus d'informations, voir Alert Notification dans l'IBM Knowledge Center.
5. Pour terminer la configuration de vos notifications par courrier électronique, cliquez sur **Sauvegarder**. Votre règle est répertoriée dans une table de l'onglet **Notification Policies**.

Instructions pour la maximisation des performances du serveur et des agents dans le cadre de la surveillance des fichiers journaux

Afin de maximiser les performances des agents de système d'exploitation et du serveur Performance Management, vous devez définir les expressions régulières dans le fichier de format (.fmt) et limiter le nombre d'événements de surveillance de fichier journal signalés à la console Cloud APM.

Instructions pour la définition des expressions régulières dans le fichier `.fmt`

Le fichier `.fmt` utilise des expressions régulières qui sollicitent particulièrement l'UC. Afin d'améliorer les performances du serveur et des agents, réduisez au minimum le temps consacré à comparer les enregistrements du journal des sources de surveillance avec les expressions régulières du fichier `.fmt`. Pour cela, suivez les instructions ci-dessous :

Réduisez au minimum l'utilisation des modèles multiligne.

Les modèles multiligne sont onéreux car l'agent doit identifier les enregistrements et déterminer s'ils présentent une correspondance. Lorsque vous utilisez un modèle multiligne représentant une expression régulière contenant le caractère "\n", ou un format de type TEC contenant le jeton '%n', l'agent doit d'abord scinder le fichier surveillé en plusieurs enregistrements de tailles différentes. Puis, il doit comparer les enregistrements aux expressions du fichier de format. Cette procédure implique une double vérification des expressions régulières, ce qui ralentit le traitement. Si vous utilisez un modèle d'une seule ligne, chaque ligne du fichier représente un enregistrement, ce qui accélère le traitement.

Dans certains cas, il est possible d'ignorer certaines lignes, ce qui permet d'obtenir de meilleures performances. Vous trouverez ci-après un exemple d'enregistrement unique d'un journal de trace RAS1 :

```
(4D66DACB.0001-1:RAS1,400,"CTBLD")
```

```
+4D66DACB.0001 Component: ira
```

```
+4D66DACB.0001 Driver: agent_fac:15/4114877.7
```

```
+4D66DACB.0001 Timestamp: Feb 24 2011 13:18:54
```

```
+4D66DACB.0001 Target: sos510amdx6-d
```

Ici, pour traiter la ligne :

```
+4D66DACB.0001 Driver: agent_fac:15/4114877.7
```

uniquement, vous pouvez écrire le modèle d'une seule ligne suivant :

```
^\+.*Driver: agent_fac:([0-9\.\/]+)$
```

Ce modèle d'une seule ligne traite la valeur requise sans avoir à recourir au format multiligne. Les quatre autres lignes de l'enregistrement logique sont traitées en tant qu'enregistrements d'une seule ligne qui, parce qu'ils ne présentent aucune correspondance, sont ignorés.

Triez les expressions du fichier de format selon leur fréquence d'occurrence dans le journal de surveillance.

L'agent compare chacun des enregistrements du journal qu'il lit avec les expressions du fichier de format jusqu'à trouver une correspondance. Il commence par la dernière expression du fichier, puis effectue la recherche en remontant. Lorsqu'il trouve une correspondance, il cesse la recherche. Si l'expression la plus consignée est la dernière répertoriée, alors, lorsqu'elle est consignée, elle est la seule expression pour laquelle une comparaison est effectuée.

Si le fichier de format contient 100 expressions, chaque fois qu'un enregistrement de journal correspond à la première expression répertoriée dans le fichier de format, l'agent doit d'abord comparer les 99 autres expressions, ce qui ralentit le traitement. Lorsqu'un enregistrement du journal lu par l'agent ne correspond à aucun des modèles du fichier de format, l'agent doit d'abord le comparer à tous les autres modèles pour savoir qu'il ne correspond pas. Ce processus est long et onéreux.

Incluez autant de données constantes que possible dans les expressions régulières.

Par exemple, si le journal renvoie l'erreur suivante :

```
Disk error on device: /dev/sda1 Disk error on device: /dev/sdb2 yyy
```

vous pouvez écrire cette expression :

```
^Disk.*: .*$
```

Cette expression entraîne une correspondance mais elle force le moteur d'expressions régulières à considérer plus de possibilités sur d'autres lignes qui pourraient être similaires, mais qui finalement ne correspondent pas, par exemple, si le signe : vient à manquer.

Cette expression est plus précise et force le moteur d'expressions régulières à interrompre le traitement des erreurs qui ne présentent aucune correspondance :

```
^Disk error on device: /dev/sd[a-b][0-9]$
```

N'utilisez pas les sous-expressions dont vous n'avez pas besoin.

Les sous-expressions affichées entre parenthèses dans l'exemple qui suit permettent d'informer le moteur d'expressions régulières que vous voulez utiliser une valeur renvoyée dans les données mises en correspondance. Ces sous-expressions impliquent un traitement supplémentaire et ne sont pas nécessaires si vous n'utilisez pas la valeur qui est renvoyée. Par exemple, si le journal renvoie l'erreur suivante :

```
write failure in writing to client 9.27.135.191. Error Broken pipe
```

et que vous incluez l'expression régulière suivante dans le fichier de format, le message d'erreur est capturé à la fin ; mais si vous n'utilisez pas la valeur qui est renvoyée, les performances sont affectées de manière négative :

```
REGEX
WriteFailure
```

```
^write failure in writing to client (.*)\. Error
(.*)$

ClientAddr $1
CustomSlot1

END
```

Utilisez des parenthèses dans les expressions à des fins de regroupement.

Vous pouvez utiliser l'opérateur ? afin d'indiquer au moteur d'expressions régulières de ne pas capturer la valeur renvoyée. Ainsi, l'opérateur ? permet de regrouper les valeurs renvoyées uniquement. Ce regroupement affecte les performances de manière positive. Par exemple, si les données de journal suivantes sont renvoyées :

```
Login succeeded on the first attempt for user Bob.
Login succeeded on the third attempt for user Joe.
```

Pour mettre en correspondance les deux valeurs renvoyées, vous devez prendre en compte la première ou la troisième tentative de connexion. Si la tentative de connexion ou l'utilisateur spécifique concernés vous importent peu, vous pouvez inclure cette expression afin de regrouper les valeurs renvoyées :

```
REGEX
LoginSuceeded

^login succeeded on the (?:[a-z]+) attempt for user ([A-Z][a-z]*)\.$

UserName $1
CustomSlot1
END
```

Si possible, évitez d'utiliser l'opérateur OR (|) dans les expressions.

L'opérateur | implique un traitement coûteux. L'opérateur | force le moteur d'expressions régulières à effectuer une sauvegarde et à essayer de mettre en correspondance des valeurs qui ne correspondent pas en temps normal. Une procédure bien plus efficace consiste à utiliser deux expressions distinctes. Prenons par exemple l'expression suivante :

```
REGEX DiskError
^.*disk error.*4|^.*disk failure.*4
END
```

Il est plus judicieux d'utiliser ces deux expressions :

```
REGEX DiskError
^.*disk error.*4
END

REGEX DiskError
^.*disk failure.*4
END
```

Ces expressions renvoient les mêmes résultats.

Important : L'emploi de ces expressions est contraire à l'instruction demandant d'utiliser autant de données constantes que possible, et il s'applique uniquement dans les cas où l'opérateur | est utilisé.

N'utilisez pas d'expressions ambiguës.

Les expressions ambiguës forcent le moteur d'expressions régulières à effectuer des sauvegardes et à rechercher différents moyens de mettre en correspondance une expression. Pour plus d'informations, voir Performance Tips.

Des expressions ambiguës peuvent voir le jour lorsqu'une expression est incluse afin de scinder un long enregistrement en plusieurs sous-expressions. Dans cette version dégénérée de ce problème, l'expression contient un espace entre les deux (.*):

```
(.*) (.*)
```

Dans cet exemple de la version dégénérée, le moteur regex recherche deux chaînes d'expressions (quelles qu'elles soient) séparées par un espace. Toutefois, le caractère * correspondant également à un espace, le moteur d'expressions régulières peut affecter le premier espace qu'il trouve au premier (.*). S'il atteint la fin de l'enregistrement d'entrée sans trouver d'autre espace, il effectue une sauvegarde et lance une nouvelle recherche en utilisant l'espace comme espace littéral appelé dans l'expression.

Pour améliorer les performances, utilisez uniquement des expressions spécifiques. Vous pouvez utiliser l'outil Regex Pal pour vérifier si le fichier de format défini correspond au journal de surveillance. Pour plus d'informations, voir Regex Pal.

Instructions pour limiter les événements de fichier journal signalés

Les instructions suivantes limitent les événements de fichier journal susceptibles d'entraîner de mauvaises performances de la part des agents de système d'exploitation ou du serveur Cloud APM :

Ecrivez les formats spécifiques dans le fichier `.fmt`.
Dans le fichier `.fmt`, écrivez des formats spécifiques capables de renvoyer les enregistrements appropriés. Par exemple, vous pouvez générer un événement pour une erreur spécifique, par exemple les lignes commençant par `Error:`, et ignorer les lignes commençant par `Warning:`.

```
Error:  disk failure
Error: out of memory
WARNING: incorrect login
```

N'activez pas le paramètre Unmatchlog du fichier `.conf`.
Veillez à ne pas activer le paramètre **Unmatchlog** du fichier `.conf` ; ce paramètre consigne tous les fichiers sans correspondance, surchargeant de ce fait votre système de fichiers.

Indiquez la classe d'événement `*DISCARD*` dans le fichier `.fmt`.
Essayez de limiter l'utilisation de l'UC par l'agent en indiquant la classe d'événement `*DISCARD*` prédéfinie dans le fichier `.fmt` de sorte à supprimer des données intentionnellement. Lorsque vous utilisez la classe d'événement `*DISCARD*`, aucun événement n'est créé pour les enregistrements de journal qui correspondent au modèle du fichier `.fmt`. Par exemple :

```
REGEX *DISCARD*
```

Activez la détection des événements en double sur une plus longue période.
Vous pouvez activer la détection des événements en double à l'aide des clés du fichier `.conf` suivantes :

- DupDetectionKeyAttributes
- EventSummaryInterval
- EventFloodThreshold

Dans cet exemple, les lignes en double sont reconnues par les valeurs *msg* et *CustomSlot1* :

```
DupDetectionKeyAttributes=msg,CustomSlot1
EventSummaryInterval=300
EventFloodThreshold=send_first
```

S'il existe plusieurs événements en double, appliquez les valeurs de seuil *send_first* ou *send_none* aux événements. Pour plus d'informations, voir «Détection et filtrage des événements en double», à la page 1047.

Ecrivez des conditions de seuil spécifiques.
Ecrivez des conditions de seuil spécifiques qui limitent l'ensemble de lignes correspondant au seuil. Par exemple, la formule de seuil suivante entraîne le déclenchement du seuil uniquement lorsqu'un événement de la classe d'événement FileSystemUsage possède une valeur supérieure ou égale à 95 dans CustomInteger1 :

```
( Class == 'FileSystemUsage' AND CustomInteger1 >= 95)
```

Fournissez l'ensemble de fichiers `.conf` et `.fmt` appropriés pour l'agent.
Veillez à fournir l'ensemble de fichiers `.conf` et `.fmt` appropriés pour l'agent. Par exemple, si vous configurez la surveillance du fichier journal pour l'agent de système d'exploitation Windows, veillez à configurer les fichiers `.conf` et `.fmt` spécialement créés pour cet agent.

Interrogez la base de données d'alarmes MongoDB pour déterminer le nombre d'événements ouverts ou le débit d'événements.

- Pour interroger la base de données d'alarmes MongoDB afin de déterminer le nombre d'événements ouverts ou le débit d'événements, procédez comme suit :
  1. Créez un fichier `event-query.js` comportant une requête MongoDB pour la base de données d'alarmes.
     - Cette requête compte tous les événements ouverts et fermés à l'aide du nom de seuil suivant :

       ```
       UDB_DB_Pool_Hit_Rat_Pct_Crit_2 db.alarms.count
       ```

       ```
       ({"threshold_name" : "UDB_DB_Pool_Hit_Rat_Pct_Crit_2"})
       ```

     - Cette requête compte les événements ouverts et fermés dans MongoDB :

       ```
       db.alarms.count()
       ```

  2. Exécutez cette commande afin d'obtenir les résultats de la requête dans le fichier `event-query.js` : **`/opt/ibm/mongodb/bin/mongo 127.0.0.1:27000/alarm -u user -p mongoUsrpasswd@08 <event-count.js`**.
- Limitez la quantité d'UC utilisée pour la surveillance du journal. Pour plus d'informations, voir «Variables d'environnement de la surveillance des fichiers journaux», à la page 654.

Availability Monitoring

Avec IBM Cloud Availability Monitoring, vous pouvez créer, éditer, afficher et supprimer des tests synthétiques qui miment le comportement de l'utilisateur final dans vos applications Web.

Le tableau de bord Availability Monitoring affiche les informations sur la disponibilité et les temps de réponse des applications surveillées, des URL et des API REST. Utilisez le tableau de bord pour surveiller les alertes et les activités associées à votre application, URL ou API REST dans différents emplacements, à l'aide de graphiques, tables de répartition et vues de carte.

Availability Monitoring est disponible pour les utilisateurs de l'offre IBM Cloud Application Performance Management, Advanced on Cloud avec le module complémentaire Availability Monitoring.

A propos d'Availability Monitoring

Utilisez Availability Monitoring pour créer des tests synthétiques qui surveillent la disponibilité et les performances de vos applications Web 24 heures sur 24 à partir d'emplacements publics et privés différents.

Créez des tests avec Availability Monitoring. Configurez vos tests de sorte qu'il soient exécutés aux intervalles définis et aux emplacements choisis. Téléchargez et déployez vos propres points de présence personnalisés (PoP) sur les serveurs locaux ou privés. Exécutez des tests à partir de 15 points de présence personnalisés publics, aux emplacements suivants :

Asie
Madras, Hong Kong, Singapour et Tokyo

Australie
Melbourne

Europe
Amsterdam, Francfort, Londres et Paris.

Amérique centrale
Mexico

Amérique du Nord
Dallas, San Jose, Toronto et Washington D.C.

Amérique du Sud
Sao Paolo

Une fois que vous avez créé et configuré vos tests, vous pouvez afficher les données de disponibilité et de performances de vos applications sur le tableau de bord Availability Monitoring.

Availability Monitoring inclut les principales fonctions suivantes :

Soyez opérationnel en moins de 5 minutes
Créez facilement des tests d'action uniques pour surveiller les performances et la disponibilité de votre application Web, en quelques minutes.

Maximisez le temps d'activité et augmentez la satisfaction de vos utilisateurs
Surveillez fréquemment la disponibilité et le temps de réponse de vos applications à partir de plusieurs lieux géographiques. Exécutez des tests synthétiques afin de mesurer les performances de chargement des sites Web et des appels d'API. Surveillez les scripts Selenium que vous utilisez pour imiter les flux utilisateur en provenance de différents emplacements.

Soyez proactif
Recevez des notifications pour vous alerter des problèmes avant qu'ils n'affectent les utilisateurs. Vous pouvez utiliser le service intégré Alert Notification pour créer des règles d'alerte réduisant leurs interférences.

Identifiez les raisons des échecs précisément et rapidement
Une analyse en cascade vous permet de repérer l'étape précise au cours de laquelle le problème s'est produit et les raisons de ce dernier (liens rompus, images trop volumineuses, recherches lentes, ou demandes externes. Des captures d'écran sont automatiquement créées pour vous aider à diagnostiquer les échecs de navigateur et les problèmes de performances historiques. Vous pouvez télécharger des rapports sur la disponibilité et les temps de réponse moyens de vos tests sur une base mensuelle, hebdomadaire ou quotidienne.

Pour travailler dans Availability Monitoring, vous devez être membre d'un rôle qui dispose du droit d'affichage pour l'application à surveiller. Pour plus d'informations, voir «Rôles et droits», à la page 1031.

Accès à Availability Monitoring

L'onglet **Présentation des statuts** d'Availability Monitoring pour votre application affiche les informations récapitulatives sur la disponibilité et le statut de vos tests. Vous pouvez accéder au tableau de bord Availability Monitoring à partir de l'onglet **Présentation des statuts** d'Availability Monitoring.

Pourquoi et quand exécuter cette tâche

Accédez à la page Récapitulatif d'Availability Monitoring en cliquant sur une application éligible dans le panneau **Toutes mes applications** du Tableau de bord d'Application Performance. A partir de la page Récapitulatif, vous pouvez ajouter des tests pour votre application, afficher les tests existants de votre application et afficher le tableau de bord Availability Monitoring.

Procédure

Pour accéder à Availability Monitoring, procédez comme suit :

1. Cliquez sur l'icône **Performance** puis sur **Tableau de bord d'Application Performance**.
2. Dans le panneau **Toutes mes applications**, cliquez sur une application à surveiller, puis sur **Availability Monitoring** dans le panneau **Groupes**.

   Si aucune application n'est répertoriée, vous devez en créer une. Sélectionnez bien **Application personnalisée** comme **Modèle**. Pour plus d'informations, voir «Gestion des applications», à la page 1129.

L'onglet **Présentation des statuts** d'Availability Monitoring affiche trois jauges qui indiquent la disponibilité moyenne des tests au cours des 24 dernières heures, le statut en cours de tous vos tests et l'utilisation du service de votre allocation pour votre plan en cours.

Vous pouvez configurer la manière selon laquelle Availability Monitoring calcule la disponibilité moyenne des tests en sélectionnant des tests à inclure dans la section **Calcul de la disponibilité**.

Cliquez sur l'icône en forme de flèche sur la jauge Disponibilité moyenne des tests afin d'afficher vos cartes de test, puis cliquez sur **Calcul de la disponibilité**. Cliquez sur une carte pour l'ajouter ou la retirer du calcul. Les cartes de test exclues sont estompées. Lorsque vous avez fini, cliquez sur **J'ai terminé**. La jauge Disponibilité moyenne des tests est actualisée en conséquence.

Vous pouvez afficher le statut de tous vos tests en cliquant sur l'icône en forme de flèche sur la jauge Statut actuel des tests. Les cartes de test de vos tests sont affichées. Cliquez sur une carte pour accéder au tableau de bord **Répartition** de ce test particulier.

3. Cliquez sur **Visualiser les détails de la surveillance** pour accéder au tableau de bord Availability Monitoring et afficher les données de tous les tests de votre application. Cliquez sur **Visualiser tous les tests** pour afficher et éditer vos tests dans le panneau **Tests synthétiques**. Cliquez sur **Ajouter un nouveau test** pour créer un test.

   Remarque : La première fois que vous exécutez Availability Monitoring, vous devez ajouter un test pour pouvoir afficher des données dans le tableau de bord Availability Monitoring.

Création et configuration des tests

Créez et configurez les tests qui indiquent la disponibilité et les performances de vos applications Web.

Créez et configurez des tests pour surveiller fréquemment la disponibilité et le temps de réponse de vos applications depuis plusieurs emplacements géographiques. Exécutez des tests synthétiques afin de mesurer les performances de chargement des sites Web et des appels d'API REST. Créez des tests de comportement incluant des scripts pour exécuter et surveiller les scripts Selenium imitant les flux utilisateur provenant de divers emplacements.

Création d'un test d'API REST

Créez un test d'API REST pour tester les temps de réponse et la disponibilité de votre application Web à l'aide des méthodes HTTP suivantes : GET, POST, PUT et DELETE.

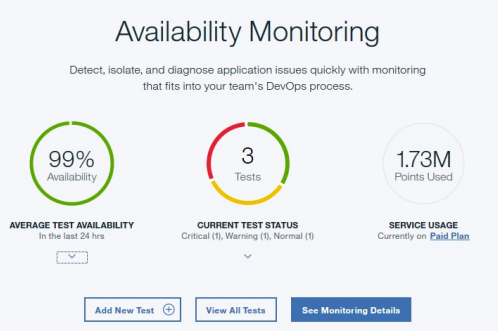
Pourquoi et quand exécuter cette tâche

Utilisez les tests d'API REST pour surveiller la disponibilité et les performances de votre application Web et des autres URL en réponse aux appels REST.

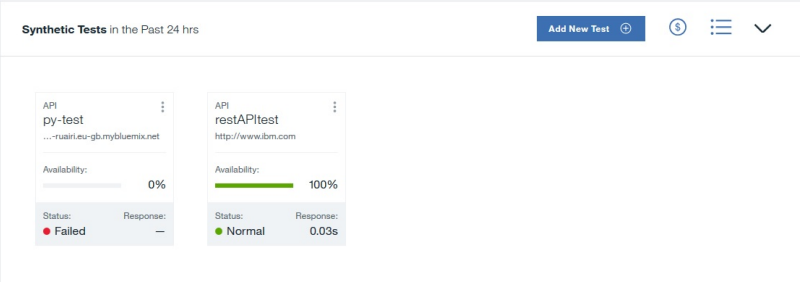
Procédure

Pour créer une API REST, procédez comme suit :

1. Si vous affichez la page Récapitulatif d'Availability Monitoring pour votre application, cliquez sur **Ajouter un nouveau test**.



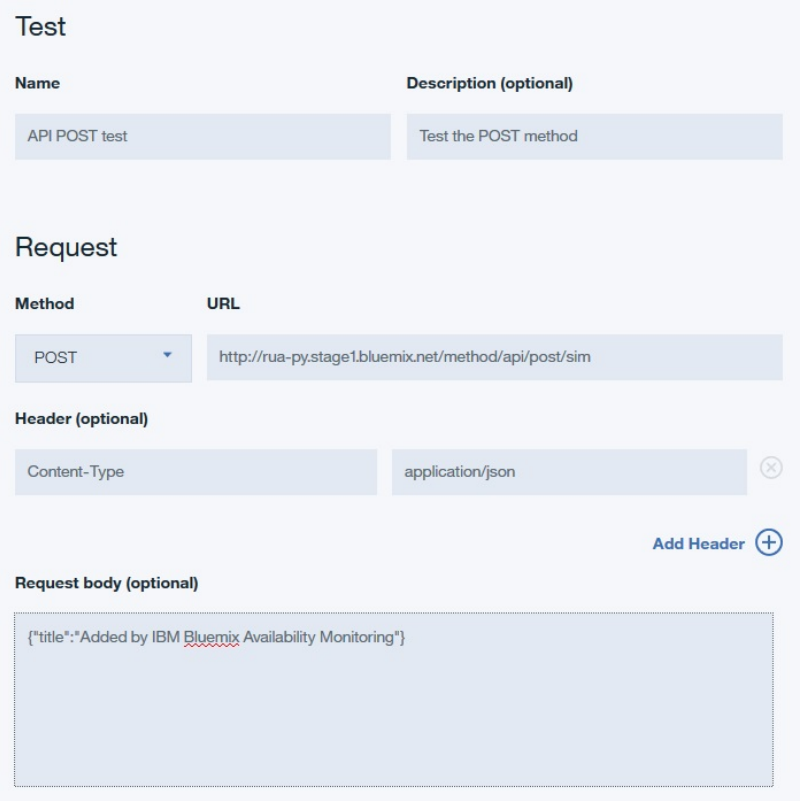
   Si le tableau de bord d'Availability Monitoring est affiché, cliquez sur **Ajouter un nouveau test** dans le panneau **Tests synthétiques**.



2. Cliquez sur **Action unique** sur la page **Configuration de la surveillance** puis sur **API REST** sur la page **Action unique**.
3. Entrez un nom significatif pour votre test dans la zone **Nom**. Ajoutez une description de l'objectif du test dans la zone **Description**.
4. Dans la section relative à la demande, sélectionnez le type de méthode dans la liste **Méthode** et entrez une valeur dans la zone **URL** correspondant à l'URL que vous voulez tester avec cette méthode.

   Vous pouvez choisir **GET**, **PUT**, **POST** ou **DELETE**. Si vous choisissez la méthode **PUT** ou **POST**, vous pouvez entrer le contenu du corps à tester dans la zone **Corps de demande (facultatif)**.

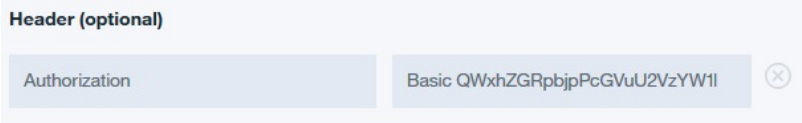
   Par exemple, le test d'API REST suivant utilise la méthode POST pour demander que votre application Web accepte des données en plus de tester la disponibilité et les performances de cette application Web.



5. Facultatif : Configurez votre test pour y inclure un en-tête particulier et une valeur. Entrez un nom d'en-tête et une valeur d'en-tête dans les zones **En-tête**.

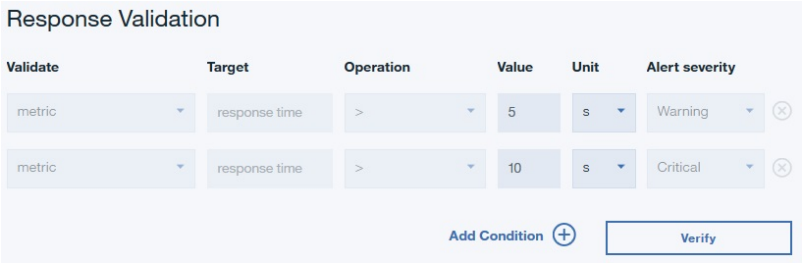
   Si l'application Web à tester requiert un nom de connexion et un mot de passe d'utilisateur, entrez `"Authorization"` dans la zone relative au nom d'en-tête. Entrez le mot "Basic", un espace et la valeur codée en base64 de *username:password* dans la zone relative à la valeur d'en-tête.

   Par exemple, si votre nom d'utilisateur est *Aladdin* et que votre mot de passe est *OpenSesame*, entrez le mot "Basic", un espace et la valeur codée en base64 de *Aladdin:OpenSesame* dans la zone relative à la valeur d'en-tête.



6. Configurez les seuils d'alerte (Avertissement et Critique) pour votre test dans la section **Validation de réponse**. Editez le contenu des zones **Valeur** et **Unité** pour chaque ligne.

   Les temps de réponse qui dépassent les seuils Avertissement et Critique que vous avez définis déclenchent des alertes.



7. Facultatif : Cliquez sur **Ajouter une condition** pour définir et ajouter des conditions de validation de réponses personnalisées.

   Les conditions de validation de réponses personnalisées sont évaluées globalement pour générer une alerte. Vous pouvez définir et ajouter jusqu'à six conditions personnalisées pour votre test.

   Important :

   Dans Availability Monitoring, chaque test peut générer un total de trois alertes au maximum. Votre test signale l'alerte de plus haute gravité jusqu'à ce que toutes les conditions causant les alertes soient résolues. Pour plus d'informations, voir «Génération d'alertes dans Availability Monitoring», à la page 1090.

   Vous pouvez valider les données suivantes :

   Header response code
   Sélectionnez **Header response code** pour effectuer un test pour un code de réponse HTTP ou pour une plage de codes de réponses HTTP.

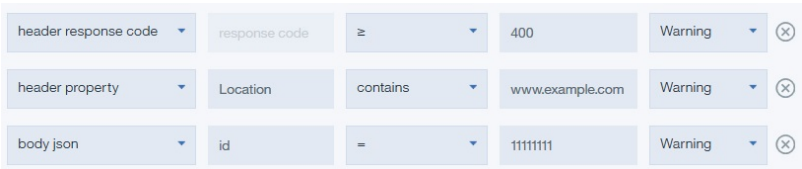
   Header property
   Sélectionnez **Header property** pour effectuer un test pour une valeur et une propriété particulière de zone d'en-tête HTTP.

   Body JSON
   Sélectionnez **Body JSON** pour tester une propriété particulière d'un corps JSON.

   Pour chaque condition, entrez une propriété à tester dans la zone **Cible**, et une valeur à tester dans la zone **Valeur**. Sélectionnez un opérateur dans le menu déroulant **Opération**. Finalement, choisissez une valeur **Gravité de l'alerte**, Avertissement ou Critique, pour votre condition.

   Important :

   Les valeurs numériques que vous entrez dans la zone **Valeur** sont traitées en tant que nombres, par défaut, et non comme des chaînes. Pour entrer une **Valeur** pour une condition de validation de réponse, utilisez des guillemets ""afin de faire la distinction entre une chaîne et un nombre. Pour effectuer un test pour la chaîne 123, par exemple, entrez `"123"` dans la zone **Valeur**. Pour procédez à une vérification pour le nombre 400, entrez `400` sans les guillemets.



8. Cliquez sur **Vérifier** pour créer votre test d'API REST et déterminer si votre demande de test est valide.

Availability Monitoring détermine la validité du test à l'aide de la méthode HTTP sélectionnée et des en-têtes de demande que vous avez définis pour le test. La validation de la réponse n'a pas lieu pendant la vérification du test.

Votre test validé est affiché dans la table **Eléments vérifiés**. Vous pouvez ajouter d'autres URL en répétant les étapes 3 à 8.

9. Pour configurer vos paramètres de test, cliquez sur **Suivant**.

   Un récapitulatif de la configuration de test est affiché. Le message suivant est affiché pour les paramètres par défaut :

   ```
   Test will occur: Every 15 minutes from 3 public locations and no private
   locations simultaneously to determine if test exceeds the specified
   threshold.
   ```

10. Dans le panneau **Paramètres**, cliquez sur **Editer** pour afficher les paramètres actuels de votre test.

    Vous pouvez mettre à jour les paramètres suivants :

    - **Intervalle** définit la fréquence d'exécution du test.
    - **Testing frequency** détermine si votre test s'exécute à partir de tous les emplacements simultanément ou d'un emplacement différent pour chaque intervalle. Sélectionnez **Simultanée** pour exécuter votre test depuis tous les emplacements simultanément, ou **Echelonnée** pour l'exécuter depuis un emplacement différent à chaque intervalle.
    - **Locations** détermine les emplacements où le test s'exécute.

11. Sélectionnez vos emplacements dans la liste des **emplacements publics**. Pour sélectionner un emplacement privé à partir duquel vous exécuterez votre test, vous devez au préalable installer et configurer un point de présence privé sur la machine à partir de laquelle vous souhaitez exécuter votre test. Pour plus d'informations, voir «Installation et configuration d'emplacements de points de présence privés», à la page 1086.
12. Cliquez sur **Sauvegarder** pour terminer la configuration de votre test, puis cliquez sur **Terminer**.

    Le tableau de bord d'Availability Monitoring s'affiche. Après une minute, le tableau de bord affiche les informations et les données de votre nouveau test.

Création d'un test de page Web

Créez un test de page Web pour tester la disponibilité de votre application Web et surveiller la durée d'ouverture de cette page.

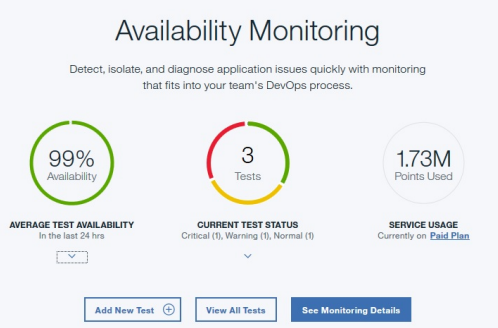
Pourquoi et quand exécuter cette tâche

Les tests de page Web indiquent le temps de réponse de chargement de l'URL de votre application Web. Créez un test de page Web pour surveiller la disponibilité et le temps de réponse de votre application Web.

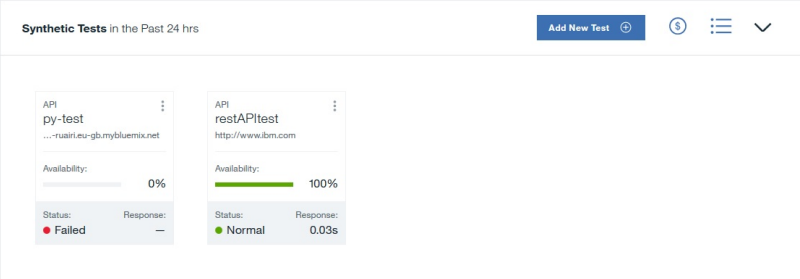
Procédure

Pour créer un test de page Web, procédez comme suit :

1. Si vous affichez la page Récapitulatif d'Availability Monitoring, cliquez sur **Ajouter un nouveau test**.

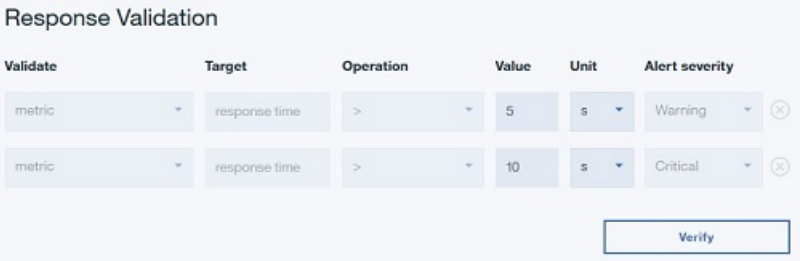


Si le tableau de bord d'Availability Monitoring est affiché, cliquez sur **Ajouter un nouveau test** dans le panneau **Tests synthétiques**.



2. Cliquez sur **Action unique** sur la page **Configuration de la surveillance** puis sur **Page Web** sur la page **Action unique**.
3. Entrez un nom significatif pour votre test dans la zone **Nom**. Ajoutez une description de l'objectif du test dans la zone **Description**.
4. Entrez l'**URL** de l'application Web à tester.
5. Configurez les seuils d'alerte (Avertissement et Critique) pour votre test dans la section **Validation de réponse**. Editez le contenu des zones **Valeur** et **Unité** pour chaque ligne.

   Les temps de réponse qui dépassent les seuils Avertissement et Critique que vous avez définis déclenchent des alertes.



6. Utilisez **Blacklist** et **Whitelist** pour spécifier à quels domaines et URL envoyer les demandes et quels domaines et URL contribuent à la mesure et au statut des tests de votre application. Ajoutez les URL et domaines que vous souhaitez inclure ou bloquer dans **Whitelist** ou **Blacklist**.

   Pour plus d'informations, voir «Blocage et filtrage à l'aide de la liste blanche et de la liste noire», à la page 1085.
7. Cliquez sur la commande **Vérifier** pour créer votre test de page Web et déterminer si votre demande de test est valide.

   Availability Monitoring détermine la validité du test en envoyant une demande GET à votre URL de test. La validation de la réponse n'a pas lieu pendant la vérification du test.

   Votre test validé est affiché dans la table **Eléments vérifiés**. Vous pouvez ajouter d'autres URL en répétant les étapes 3 à 7.
8. Pour configurer vos paramètres de test, cliquez sur **Suivant**.

   Un récapitulatif de la configuration de test est affiché. Le message suivant est affiché pour les paramètres par défaut :

   ```
   Test will occur: Every 15 minutes from 3 public locations and no private
   locations simultaneously to determine if test exceeds the specified
   threshold.
   ```

   Une estimation de l'utilisation et du nombre de tests par mois est affichée compte tenu de votre configuration actuelle.
9. Dans le panneau **Paramètres**, cliquez sur **Editer** pour afficher les paramètres actuels de votre test.

   Vous pouvez mettre à jour les paramètres suivants :

   - **Intervalle** définit la fréquence d'exécution du test.

- **Testing frequency** détermine si votre test s'exécute à partir de tous les emplacements simultanément ou d'un emplacement différent pour chaque intervalle. Sélectionnez **Simultanée** pour exécuter votre test depuis tous les emplacements simultanément, ou **Echelonnée** pour l'exécuter depuis un emplacement différent à chaque intervalle.
- **Locations** détermine les emplacements où le test s'exécute.

  Sélectionnez vos emplacements dans la liste des **emplacements publics**. Pour sélectionner un emplacement privé à partir duquel vous exécuterez votre test, vous devez au préalable installer et configurer un point de présence privé sur la machine à partir de laquelle vous souhaitez exécuter votre test. Pour plus d'informations, voir «Installation et configuration d'emplacements de points de présence privés», à la page 1086.

  Cliquez sur **Sauvegarder** pour finir de configurer votre test.

10. Cliquez sur **Terminer**.

    Le tableau de bord d'Availability Monitoring s'affiche. Après une minute, le tableau de bord affiche les informations et les données de votre nouveau test.

Création d'un test de script depuis un script téléchargé

Téléchargez un script Selenium pour créer un test de script qui teste la disponibilité et les performances de votre application Web en réponse au comportement simulé de l'utilisateur.

Avant de commencer

Pour créer un test de script, vous devez d'abord créer un script Selenium. Pour plus d'informations sur la création de scripts Selenium, voir Enregistrement de scripts synthétiques.

Pourquoi et quand exécuter cette tâche

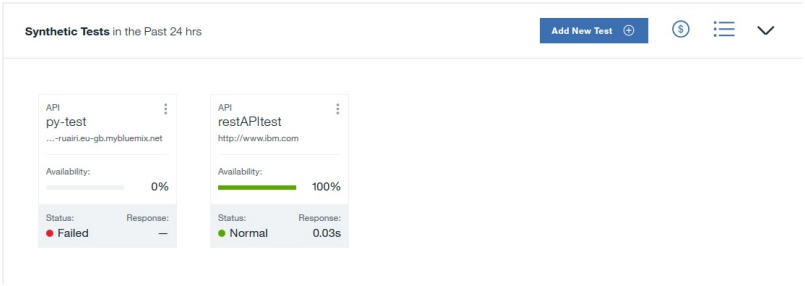
Créez un test de script permettant de surveiller un script Selenium qui simule les interactions de vos utilisateurs avec votre application Web. Si vous créez un script Selenium imitant un utilisateur qui se connecte à votre application, vous pouvez alors exécuter périodiquement un test de script pour tester les performances de votre application en réponse aux actions utilisateurs simulées.

Procédure

Pour créer un test de script, procédez comme suit :

1. Si vous affichez la page Récapitulatif d'Availability Monitoring, cliquez sur **Ajouter un nouveau test**.

   Si le tableau de bord d'Availability Monitoring est affiché, cliquez sur **Ajouter un nouveau test** dans le panneau **Tests synthétiques**.



2. Cliquez sur **Comportement contrôlé par scripts** sur la page **Configuration de la surveillance**. La page **Configuration du comportement contrôlé par scripts** s'affiche. Cliquez sur **Télécharger le fichier**.

   Pour éditer à nouveau ce test ultérieurement, vous pouvez télécharger le fichier script que vous aviez transféré. Cliquez sur l'icône **Télécharger** pour télécharger votre script.
3. Entrez un nom significatif pour votre test dans la zone **Nom**. Ajoutez une description de l'objectif du test dans la zone **Description**.
4. Cliquez sur **Parcourir** pour localiser et télécharger un fichier de script.
5. Utilisez **Blacklist** et **Whitelist** pour spécifier à quels domaines et URL envoyer les demandes et quels domaines et URL contribuent à la mesure et au statut des tests de votre application. Ajoutez les URL et domaines que vous souhaitez inclure ou bloquer dans **Whitelist** ou **Blacklist**.

   Pour plus d'informations, voir «Blocage et filtrage à l'aide de la liste blanche et de la liste noire», à la page 1085.
6. Pour configurer vos paramètres de test, cliquez sur **Suivant**.

   Un récapitulatif de la configuration de test est affiché. Le message suivant, par exemple, est affiché pour les paramètres par défaut :

   ```
   Test will occur: Every 15 minutes from 3 public locations and no private
   locations simultaneously to determine if test exceeds the specified
   threshold.
   ```

   Une estimation de l'utilisation et du nombre de tests par mois est affichée compte tenu de votre configuration actuelle.
7. Dans le panneau **Paramètres**, cliquez sur **Editer** pour afficher les paramètres actuels de votre test.

   Vous pouvez mettre à jour les paramètres suivants :

   - **Intervalle** définit la fréquence d'exécution du test.
   - **Testing frequency** détermine si votre test s'exécute à partir de tous les emplacements simultanément ou d'un emplacement différent pour chaque intervalle. Sélectionnez **Simultanée** pour exécuter votre test depuis tous les emplacements simultanément, ou **Echelonnée** pour l'exécuter depuis un emplacement différent à chaque intervalle.
   - **Seuil critique** définit le temps de réponse pour les alertes critiques du test.
   - **Warning Threshold** définit le temps de réponse pour les alertes d'avertissement du test.
   - **Locations** détermine les emplacements où le test s'exécute.

   Sélectionnez vos emplacements dans la liste des **emplacements publics** affichés par défaut. Pour sélectionner un emplacement privé à partir duquel vous exécuterez votre test, vous devez au préalable installer et configurer un point de présence privé sur la machine à partir de laquelle vous souhaitez exécuter votre test. Pour plus d'informations, voir «Installation et configuration d'emplacements de points de présence privés», à la page 1086.

   Si nécessaire, vous pouvez entrer les valeurs des variables qui sont définies dans votre script de test. Ainsi, si votre script requiert un nom et un mot de passe pour se connecter à un site Web, vous pouvez entrer les valeurs pour ces variables. Vous pouvez définir différentes valeurs pour vos variables dans divers emplacements de la table **Variables de script**.

   Cliquez sur **Sauvegarder** pour finir de configurer votre test.

8. Cliquez sur **Terminer**.

   Le tableau de bord d'Availability Monitoring s'affiche. Après une minute, le tableau de bord affiche les informations et les données de votre nouveau test.

Blocage et filtrage à l'aide de la liste blanche et de la liste noire

Utilisez la liste blanche et la liste noire pour déterminer vers quelles ressources les demandes doivent être envoyées et quelles ressources contribuent aux métriques et au statut de vos tests d'applications. Les listes blanches et les listes noires sont uniquement disponibles pour les tests de page Web et les tests de comportement contrôlés par script.

Les zones **Liste blanche** et **Liste noire** définissent les ressources auxquelles votre test peut ou ne peut pas accéder et les ressources qui contribuent aux métriques et au statut de vos tests. La liste blanche et la liste noire contrôlent les dépendances et ressources qui contribuent aux temps de réponse de vos applications Web testées, par exemple, des mesures tierces. Vous pouvez configurer votre liste blanche et votre liste noire lorsque vous créez un test de page Web ou un test de comportement contrôlé par script.

Vous pouvez utiliser la **liste blanche** pour définir les domaines et les URL autorisés puis utiliser la **liste noire** pour bloquer des éléments spécifiques de vos emplacements autorisés.

Syntaxe

Utilisez des virgules (,) pour séparer les éléments de la liste blanche et de la liste noire. Utilisez le symbole de caractère générique (*) pour filtrer les éléments de chaque URL ou domaine.

Liste blanche

Ajoutez les URL, les schémas ou les domaines que vous souhaitez inclure dans les calculs des métriques et des demandes dans la zone Liste blanche. Vous pouvez répertorier jusqu'à 10 éléments dans votre liste blanche. La longueur de chaque élément ne peut pas être supérieure à 200 caractères. L'ensemble des domaines, schémas et URL qui ne correspondent pas aux éléments de votre liste blanche sont bloqués.

Par exemple : `ibm.com, *developerworks*, *.s81c.com/*, https://www.ibm.com*, https://*`

Remarque : Si le filtre d'URL de la liste blanche inclut `http://` ou `https://`, vous devez inclure le caractère générique (*) directement après l'URL, par exemple : `https://www.ibm.com*`.

Liste noire

Ajoutez les URL, les schémas ou les domaines que vous ne souhaitez pas inclure dans les calculs des métriques et des demandes dans la zone Liste noire. Vous pouvez répertorier jusqu'à 20 éléments dans votre liste noire. La longueur de chaque élément ne peut pas être supérieure à 200 caractères.

Par exemple : `*.profile.*.cloudfront.net/*.png, http://*`

Remarque : Si le filtre d'URL de la liste noire inclut `http://` ou `https://`, vous devez inclure le caractère générique (*) directement après l'URL, par exemple : `https://www.ibm.com*`.

Comportements de filtrage et de blocage

Les tests peuvent comporter à la fois une liste blanche et une liste noire. Lorsque vous déterminez quels emplacements sont autorisés ou bloqués, la liste noire a toujours priorité sur la liste blanche. Le tableau suivant affiche les comportements de filtrage et de blocage de tous les scénarios impliquant la liste blanche et la liste noire.

Tableau 253. Comportement de filtrage et de blocage pour la liste blanche et la liste noire

Liste noire	Liste blanche	Comportement	Raison
Vide	Vide	Autoriser l'accès	Aucune règle de filtrage entrée.

Tableau 253. Comportement de filtrage et de blocage pour la liste blanche et la liste noire (suite)

Liste noire	Liste blanche	Comportement	Raison
Vide	L'URL ne correspond pas à l'entrée de la liste	Bloquer l'accès	L'URL ne figure pas dans la liste blanche.
Vide	L'URL correspond à l'entrée de la liste	Autoriser l'accès	L'URL figure dans la liste blanche. Aucune entrée de liste noire pour bloquer l'accès.
L'URL ne correspond pas à l'entrée de la liste	Vide	Autoriser l'accès	L'URL ne figure pas dans la liste noire. Pas d'entrée de liste de blanche pour empêcher l'accès à des URL qui ne figurent pas dans la liste blanche.
L'URL correspond à l'entrée de la liste	Vide	Bloquer l'accès	L'URL figure dans la liste noire.
L'URL ne correspond pas à l'entrée de la liste	L'URL ne correspond pas à l'entrée de la liste	Bloquer l'accès	L'URL ne figure pas dans la liste blanche.
L'URL ne correspond pas à l'entrée de la liste	L'URL correspond à l'entrée de la liste	Autoriser l'accès	L'URL figure dans la liste blanche. L'URL ne figure pas dans la liste noire.
L'URL correspond à l'entrée de la liste	L'URL ne correspond pas à l'entrée de la liste	Bloquer l'accès	L'URL ne figure pas dans la liste blanche. L'URL figure dans la liste noire.
L'URL correspond à l'entrée de la liste	L'URL correspond à l'entrée de la liste	Bloquer l'accès	L'URL figure dans la liste noire. L'entrée de la liste noire a priorité sur l'entrée de la liste blanche.

Installation et configuration d'emplacements de points de présence privés
Téléchargez et installez un point de présence privé sur une machine locale, puis configurez-le comme emplacement pour vos tests dans Availability Monitoring.

Avant de commencer

Pour installer un point de présence privé, l'emplacement d'installation de votre point de présence privé doit remplir les conditions suivantes :

- Linux est installé avec une version de noyau supérieure ou égale à 3.1.0.
- Le service Docker version 1.7.1 ou ultérieure est installé et démarré.
- L'espace disque disponible est de 4 Go ou plus.
- La mémoire disponible est de 2 Go ou plus.
- Coeurs d'UC :
  - Si vous n'avez besoin que de lire des API REST dans votre point de présence privé, veuillez disposer d'au moins 2 coeurs d'UC disponibles.
  - Si vous souhaitez exécuter des lectures de page Web et des lectures de script dans votre point de présence privé, veuillez disposer d'1 coeur d'UC pour tous les 1 ou 2 tests à exécuter toutes les minutes.

- Vérifiez l'utilisation de votre processeur et de votre mémoire de point de présence privé avant et après avoir ajouté de nouveaux tests, et après avoir appliqué des mises à jour logicielles au point de présence privé qui incluent des versions mises à jour de Firefox ou de l'environnement de développement intégré Selenium car les versions ultérieures pourraient nécessiter des exigences plus élevées en termes de configuration système requise.

La meilleure pratique pour déterminer quand ajouter des coeurs d'UC consiste à exécuter votre processus le plus exigeant sur votre hôte de point de présence privé pour obtenir l'utilisation de l'UC et de la mémoire : si l'utilisation totale de l'UC est supérieure à 70 % et que le processus d'utilisation de l'UC de haut niveau est Firefox, ajoutez des coeurs d'UC jusqu'à ce que l'utilisation totale de l'UC soit inférieure à 50 % ; si la mémoire disponible sur votre hôte de point de présence privé est inférieure à 500 Mo, augmentez la mémoire.

Si vous n'avez pas plus de ressources matérielles, mais que vous voulez que votre point de vente privé s'exécute sans exception, procédez comme suit pour réduire le nombre d'instances d'exécution Firefox en parallèle (vos tests sont exécutés avec des intervalles plus longs que ce qui est configuré dans l'interface utilisateur car vos ressources matérielles ne peuvent exécuter plusieurs tests) :

1. Editez le script `start-pop.sh` pour ajouter la variable d'environnement **`MAX_TASKPOOL_SIZE`**, entrez les coeurs d'UC disponibles comme valeur pour l'hôte de point de présence privé, puis exécutez la commande **`stop-pop.sh`** suivie de **`start-pop.sh`**.
2. Définissez les tests sur un intervalle plus long dans l'interface utilisateur.

Vous devez avoir accès à l'interface de ligne de commande de la machine sur laquelle vous souhaitez installer votre point de présence privé. Vous devez également disposer des droits utilisateur nécessaires pour ajouter des packages à Docker.

Important :

- vérifiez que l'heure système de la machine sur laquelle vous souhaitez exécuter un point de présence privé est synchronisée avec l'heure standard et qu'elle le reste. Sinon, vos instances de test affichent des horodatages incorrects dans le tableau de bord Availability Monitoring.
- Le point de présence privé d'Availability Monitoring est intégralement pris en charge sur les plateformes suivantes : Red Hat Enterprise Linux 7.4 et CentOS Linux 7.4.

Pourquoi et quand exécuter cette tâche

En plus des emplacements publics, vous pouvez déployer des points de présence privés lorsque vous créez ou éditez un test dans Availability Monitoring. Utilisez des points de présence privés pour tester les applications qui se trouvent derrière le pare-feu de votre société, telles que les applications qui exigent une confidentialité ou un niveau de sécurité plus élevé. Vous pouvez enregistrer jusqu'à 50 emplacements privés dans Availability Monitoring. Téléchargez le script de prévérification et le package du point de présence privé, puis enregistrez le script et le package sur la machine sur laquelle vous souhaitez exécuter le point de présence privé.

Procédure

1. Créez un test ou éditez un test existant.

   Pour créer un test, cliquez sur **Ajouter un nouveau test** dans le panneau **Tests synthétiques**. Pour éditer un test, cliquez sur **Actions** , puis sur **Editer**. Si vous créez un test, configurez-le et testez-le. Dans la section **Paramètres**, cliquez sur **Editer**.

   Pour plus d'informations, voir «Création d'un test d'API REST», à la page 1078, «Création d'un test de page Web», à la page 1081 et «Création d'un test de script depuis un script téléchargé », à la page 1083.
2. Cliquez sur **Editer** dans la section **Paramètres** pour afficher la section **Emplacements**, puis cliquez sur **Emplacements privés**. Si vous éditez un test précédent, cliquez sur **Emplacements privés** dans la section **Emplacements**.

Si vous avez déjà installé un ou plusieurs points de présence privés, une liste de tous les points de présence privés installés est affichée. Si aucun point de présence privé n'est installé et configuré, Availability Monitoring peut vous aider à en configurer un.

3. Cliquez sur **Télécharger la prévérification** et enregistrez le script de prévérification sur une machine à partir de laquelle vous souhaitez exécutez des tests.

   Important : Vous devez extraire et exécuter des scripts de l'interface de ligne de commande (CLI) pour installer un point de présence privé. Les scripts et le package du point de présence peuvent être installés sur une machine différente et sont accessibles par l'intermédiaire de l'interface de ligne de commande de cette machine. Ne fermez pas Availability Monitoring et le l'actualisez pas dans votre navigateur lorsque vous utilisez des scripts de point de présence privé ; vous perdriez les paramètres de test non enregistrés.

   Ouvrez une interface de ligne de commande pour la machine dont vous souhaitez rechercher le point de présence privé. A partir de l'interface de ligne de commande, accédez à l'emplacement dans lequel vous avez sauvegardé le script de prévérification ; exécutez ensuite ce script comme suit :

   ```
   ./precheck.sh
   ```

   Assurez-vous de disposer des droits nécessaires pour exécuter les scripts shell sur votre machine.

   Le script de prévérification affiche le résultat de la vérification. Si la vérification échoue pour votre environnement, mettez à jour votre machine afin qu'elle possède la configuration requise affichée.

4. Retournez à Availability Monitoring, cliquez sur **Télécharger le package** et enregistrez le package. Déplacez le package sur la machine à partir de laquelle vous souhaitez exécutez des tests. A partir de l'interface de ligne de commande, accédez à l'emplacement dans lequel vous avez enregistré le package téléchargé, puis exécutez la commande suivante pour extraire le package :

   ```
   tar -xvf Availability_Monitoring_PoP.tar
   ```

   Où *Availability_Monitoring_PoP.tar* est le nom du fichier `.tar` contenant le module de point de présence privé que vous avez téléchargé.

5. Configurez votre point de présence privé. A partir de l'interface de ligne de commande, exécutez le script suivant :

   ```
   ./config-pop.sh
   ```

   Lorsque vous y êtes invité, entrez les informations suivantes pour votre point de présence privé :

   - Nom de point de présence
   - Pays
   - Ville
   - Latitude du point de présence
   - Longitude du point de présence
   - Description du point de présence

6. Si l'un de vos tests d'API REST se connecte à un serveur qui utilise un certificat autosigné ou n'est pas signé par un fournisseur de certificat de l'autorité de certification connu, placez tous les certificats de l'autorité de certification dignes de confiance dont le format de fichier est `.pem` dans le répertoire `keyfiles`.

   Remarque :

   - Toute modification des fichiers de certificat `.pem` requiert le redémarrage du point de présence privé.
   - Le serveur testé doit envoyer tout sauf le certificat de l'autorité de certification racine pendant l'établissement de liaison TLS ; dans le cas contraire, corrigez la configuration du serveur, le cas échéant. Sinon, vous pouvez ajouter tout certificat manquant dans le répertoire `keyfiles` comme indiqué dans cette étape. Cependant, le(s) test(s) de point de présence risque(nt) de ne pas refléter l'expérience d'autres clients.

7. Pour configurer votre point de présence privé de sorte qu'il utilise un serveur proxy lorsque vous exécutez des tests de page Web ou des tests de comportement préétablis, entrez l'une des options suivantes :

   Important : les tests d'API REST exécutés à partir de l'emplacement de votre point de présence privé avec une configuration de proxy manuelle ou automatique n'utilisent pas ce proxy. Seuls les tests de page Web et de comportement préétablis peuvent utiliser un serveur proxy pour être exécutés à partir d'emplacements de point de présence privé.

   no
   Entrez no pour configurer votre point de présence privé de sorte qu'il n'utilise pas de proxy lorsque vous exécutez des tests.

   manual
   Entrez `manual` pour configurer manuellement une adresse IP et un numéro de port de proxy à utiliser par votre proxy de point de présence privé lorsque vous exécutez des tests. Le script demande l'adresse IP et le numéro de port du serveur proxy au format suivant : *`adresse IP`*`:`*`numéro de port`*. Vous pouvez également créer une liste "aucun proxy" pour bloquer des éléments de domaine, des noms d'hôte ou des éléments d'adresse IPv4. Lorsque vous y êtes invité, entrez un ou plusieurs éléments de domaine ou éléments d'adresse IPv4. Séparez chaque élément de liste par un espace ou une virgule (","). Le caractère générique (*) n'est pas pris en charge.

   - Pour bloquer un domaine et ses éventuels sous-domaines, entrez un suffixe de domaine, en commençant par un point. Par exemple : `.example.org, example.org`.
   - Pour bloquer un réseau, entrez une adresse IP avec un suffixe CIDR pour identifier une plage d'adresses IP à bloquer. Par exemple : `10.0.0.0/8`.

   pac
   Entrez `pac` pour configurer votre point de présence privé de sorte qu'il utilise une URL de configuration de proxy automatique. Lorsque le script vous y invite, entrez l'URL de configuration automatique du proxy.

   Vos paramètres de point de présence privé sont enregistrés dans le fichier `pop.properties`.
8. Démarrez votre point de présence privé. A partir de l'interface de ligne de commande, exécutez le script suivant :

   ```
   ./start-pop.sh
   ```

   Lorsque votre point de présence privé est en cours d'exécution, il est détectable par Availability Monitoring.
9. Retournez à Availability Monitoring et cliquez sur  **Refresh Locations** pour rechercher et afficher votre nouveau point de présence privé.

   Votre point de présence privé est répertorié dans un tableau.
10. Pour choisir votre point de présence privé comme emplacement de votre test, cochez la case de la ligne du tableau qui contient un point de présence privé. Pour supprimer un point de présence privé, procédez comme suit :
    a) A partir de l'interface de ligne de commande, exécutez le script **`./stop-pop.sh`** sur la machine sur laquelle se trouve votre point de présence privé.
    b) Retournez à Availability Monitoring et cliquez sur  **Supprimer** sur la ligne du tableau qui contient le point de présence privé à supprimer.
11. Répétez les étapes 3 à 10 pour ajouter d'autres points de présence privés sur différentes machines qui pourront être sélectionnées comme emplacements dans Availability Monitoring. Cliquez sur **Terminer** pour enregistrer et démarrer votre test.

    Le tableau de bord d'Availability Monitoring s'affiche. Après une minute environ, le tableau de bord affiche les informations et les données de votre nouveau test.

12. Facultatif : Pour mettre à niveau un point de présence privé existant, procédez comme suit :
    a) Téléchargez le nouveau package du point de présence privé dans un nouveau dossier, puis utilisez la commande **`tar -xvf`** pour décompresser le nouveau point de présence dans ce dossier.
    b) A partir de l'interface de ligne de commande, accédez au dossier dans lequel se trouve votre ancien point de présence privé. Exécutez le script suivant pour arrêter l'ancien point de présence privé :

       `./stop-pop.sh`
    c) Dans le répertoire où se trouve votre ancien point de présence privé, sauvegardez vos fichiers `system.properties` et `pop.properties` existants.

       Important : Le fichier `system.properties` contient des informations importantes qui permettent à votre point de présence privé de se connecter au serveur Cloud APM. Le fichier `pop.properties` contient les données de configuration de votre point de présence privé. Pour conserver cette configuration, assurez-vous de conserver les fichiers `pop.properties` et `system.properties` de votre ancien point de présence privé avant de mettre à niveau votre point de présence privé.
    d) Copiez tous les fichiers de votre nouveau dossier de point de présence privé, à l'exception des fichiers `pop.properties` et `system.properties`, puis remplacez les fichiers à l'emplacement de votre ancien point de présence privé.
    e) Si vous devez reconfigurer votre point de présence privé mis à niveau, exécutez le script suivant à partir de l'interface de ligne de commande :

       `./config-pop.sh`
    f) Exécutez **`./start-pop.sh`** à partir de l'interface de ligne de commande pour démarrer votre point de présence privé mis à niveau.
    g) Retournez à Availability Monitoring et cliquez sur  **Refresh Locations** pour rechercher et afficher votre point de présence privé mis à niveau.

Génération d'alertes dans Availability Monitoring
Dans Availability Monitoring, chaque test peut générer un total de trois alertes. Votre test signale l'alerte de plus haute gravité jusqu'à ce que la condition causant l'alerte soit résolue.

Une alerte séparée est émise pour trois situations différentes :

- Quand le temps de réponse de votre application Web ou URL dépasse les seuils d'avertissement ou critiques définis pour votre test. Chaque test mesure le temps de réponse par défaut et émet une alerte reposant sur les seuils Avertissement et Critique pour ce test.
- Quand votre test renvoie un code réponse HTTP qui indique que votre application Web ou URL n'est pas disponible en raison d'une erreur du client ou du serveur. Chaque test vérifie le code de réponse par défaut pour déterminer si le test a abouti ou échoué.
- Quand votre test détermine qu'une ou plusieurs conditions personnalisées sont satisfaites, une alarme est émise avec le niveau de gravité le plus élevé, comme défini dans ces conditions. Availability Monitoring considère toutes les conditions personnalisées globalement quand il détermine si une alarme est émise. Cette alarme subsiste jusqu'à ce que votre test détermine qu'aucune des conditions personnalisées ne génère plus aucune alerte Avertissement ou Critique.

Quand plus d'une alerte est déclenchée, Availability Monitoring signale l'alerte de plus haute gravité tant qu'une alerte persiste.

Par exemple, si vous ajoutez une condition personnalisée qui déclenche une alerte critique et une autre condition personnalisée qui génère une alerte d'avertissement, une alerte critique est générée par votre test. Cette alerte est visible sur le tableau de bord d'Availability Monitoring. Si la condition qui a provoqué l'alerte critique n'est plus vérifiée, la gravité de votre alerte de test passe à "Avertissement". L'alerte persiste tant qu'il existe encore une ou plusieurs conditions, sur l'ensemble des conditions, qui génèrent une alerte.

Examen des informations de disponibilité et de performance de l'application sur le tableau de bord Surveillance

Vous pouvez visualiser les détails de la disponibilité et des performances de votre application, avec les alertes et éventuels tests associés sur le tableau de bord Availability Monitoring.

Le tableau de bord Availability Monitoring est composé des panneaux suivants :

- Récapitulatif de l'application
- Fréquence des alertes
- Tests synthétiques
- Temps de réponse et disponibilité

Utilisez le menu déroulant **Accéder à** 

pour accéder rapidement à tout panneau.

Utilisez les guides pour découvrir les fonctionnalités d'Availability Monitoring. Pour ouvrir un guide, cliquez sur l'icône **Aide**  , puis sur le guide de votre choix.

Bibliothèque de tutoriels vidéo
La bibliothèque de tutoriels vidéo contient des vidéos sur la manière de créer des tests Availability Monitoring, de créer des scripts de test avec Selenium IDE et d'envoyer des alertes.

Bienvenue dans la rubrique Surveillance !
Le guide Bienvenue dans la rubrique Surveillance met en évidence des zones du tableau de bord et explique chaque fonction d'Availability Monitoring.

Vous pouvez accéder au tableau de bord **Répartition** depuis le panneau Récapitulatif de l'application, le panneau Fréquence des alertes, le panneau Tests synthétiques ou le panneau Temps de réponse et disponibilité. Le tableau de bord **Répartition** affiche des statistiques clés sur vos instances de test.

Vous pouvez changer l'ordre des panneaux selon vos besoins. Pour déplacer un panneau, cliquez sur son titre et faites-le glisser à l'emplacement voulu. Pour conserver ces modifications après votre déconnexion, cliquez sur **Sauvegarder la disposition**.

Vous pouvez définir le tableau de bord de sorte qu'il soit régénéré toutes les minutes. Cliquez sur l'icône **Configurer**  puis sur la barre coulissante **Régénérer** pour sélectionner **1 min**. Pour régénérer votre page à tout moment, cliquez **Régénérer**.

Récapitulatif de l'application
Le panneau Récapitulatif de l'application affiche une présentation du statut alerte au cours des 24 dernières heures et les informations actuelles sur le statut des tests.

Le panneau Récapitulatif de l'application affiche les informations suivantes :

- **Statut actuel** affiche le niveau de gravité le plus élevé de tous vos tests. La gravité peut correspondre au niveau Normal, Avertissement ou Critique.
- **Alertes** affiche le nombre d'alertes ouvertes et les divise en alertes d'avertissement et alertes critiques.
- **Rapport sur la disponibilité** permet de télécharger un rapport sous forme de fichier `.csv` sur la disponibilité mensuelle, hebdomadaire et quotidienne et les temps de réponse moyens de l'application.

  Cliquez sur l'icône **Rapport**  pour télécharger le rapport.

Fréquence des alertes
Le panneau **Fréquence des alertes** contient une carte qui affiche les alertes les plus récentes. Les alertes sont regroupées par emplacement et répertoriées sur la table **Alertes**.

Carte Fréquence des alertes

La carte **Fréquence des alertes** affiche des informations instantanées pour tous les points de présence publics et privés de vos tests.

Utilisez la fonction zoom pour agrandir une zone quelconque de la carte ou restaurer sa taille d'origine. Survolez chaque emplacement pour visualiser le nom de cet emplacement et le nombre d'alertes de niveau avertissement ou critique à cet emplacement. Vous pouvez filtrer les alertes affichées sur la carte en sélectionnant **Toutes**, **Ouvertes** ou **Fermées** dans la liste déroulante **Alertes**.

Emplacements des points de présence

Les icônes d'**emplacement de point de présence** 

indiquent les emplacements des points de présence pour vos tests. La couleur de chaque icône d'**emplacement de point de présence** représente la gravité de l'alerte la plus récente à chaque emplacement : Normal 

, Avertissement 

ou Critique 

. Une icône d'**emplacement de point de présence** indique que cet emplacement est celui avec les plus nombreuses alertes de la plus haute gravité entre tous les emplacements pour vos instances de test.

Ajoutez les emplacements de point de présence à votre test sélectionné en survolant une icône d'**emplacement de point de présence inactif**  et en cliquant sur **Tester ici**. La page relative au mode test s'affiche pour votre test sélectionné. Vous pouvez sélectionner un test depuis le menu déroulant **Test** du panneau **Temps de réponse** et **Disponibilité**.

Les emplacements de point de présence privé sont représentés par des icônes d'**emplacement de point de présence privé** 

Nombre d'alertes

Les icônes d'**emplacement de point de présence** affichent le nombre d'alertes ouvertes, fermées ou de toutes les alertes générées à chaque emplacement. Les icônes **Critique**, **Avertissement** et **Normal** 

affichent le nombre d'alertes de chaque gravité pour vos emplacements.

Tests ayant échoué

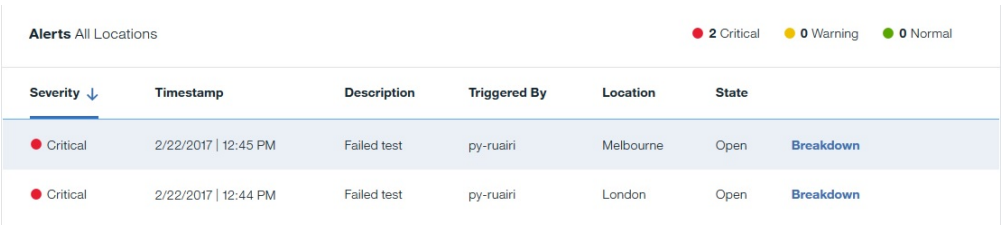
Les emplacements où des tests ont échoué sont indiqués par une icône d'**emplacement de point de présence** avec une bordure en pointillés 

.

Utilisez la fonction zoom pour agrandir une zone quelconque de la carte ou restaurer sa taille d'origine. Survolez chaque emplacement pour visualiser le nom de cet emplacement et le nombre d'alertes de niveau avertissement ou critique à cet emplacement. Vous pouvez filtrer les alertes affichées sur la carte en sélectionnant **Toutes**, **Ouvertes** ou **Fermées** dans la liste déroulante **Alertes**.

table Alertes

Les alertes pour tous les emplacements sont affichées dans une table.



Cette table contient les informations suivantes sur vos alertes :

- **Gravité** indique si l'alerte est de niveau critique ou avertissement.
- **Horodatage** indique l'heure de création de l'alerte.
- **Description** récapitule les performances de votre instance de test.
- **Déclenchée par** indique le nom du test qui a déclenché l'alerte.

- **Emplacement** signale où s'est produit le problème.
- **Etat** indique si l'alerte est ouverte ou fermée.

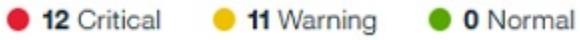
Affichage des détails d'alerte

Chaque alerte dans le tableau comporte un lien vers le tableau de bord **Répartition**. Utilisez le tableau de bord Répartition pour vous aider à identifier et résoudre le problème à l'origine de l'alerte.

Filtrage des alertes

Pour filtrer les alertes d'un emplacement particulier, cliquez sur une icône d'**emplacement de point de présence** sur la carte. Pour afficher les alertes de tous les emplacements, cliquez sur un endroit de la carte qui ne correspond pas à une icône d'**emplacement de point de présence**.

Pour filtrer les alertes par gravité dans le tableau, cliquez sur l'icône **Critique**, **Avertissement** ou **Normal**



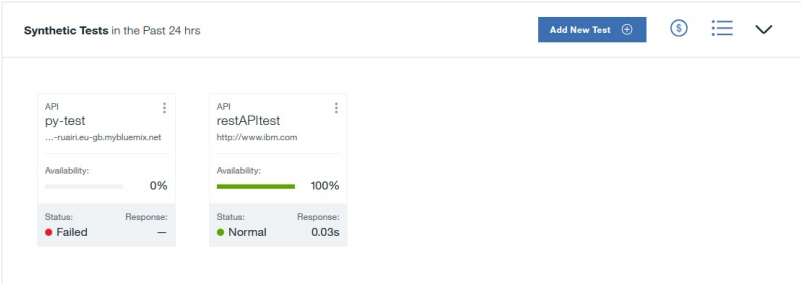
. Pour supprimer le filtre et inclure les alertes de tous les niveaux de gravité dans le tableau, cliquez à nouveau sur l'icône que vous aviez sélectionnée.

Modification des seuils d'alerte

Les alertes sont déclenchées par les seuils que vous spécifiez lorsque vous créez un test. Dans la plupart des cas, ils sont générés suite à des problèmes de disponibilité ou de lenteur des temps de réponse. Pour modifier les paramètres de seuil, cliquez sur l'icône **Actions** du test ayant généré l'alerte sur le panneau **Tests synthétiques** puis cliquez sur **Editer**.

Tests synthétiques

Dans le panneau **Tests synthétiques**, vous pouvez créer, éditer, supprimer et afficher des *tests synthétiques* qui surveillent les performances et la disponibilité de vos applications. Les tests sont affichés dans une vue liste ou carte dans le panneau **Tests synthétiques**.



Chaque carte de test affiche des informations sur le test :

Disponibilité
: Affiche la disponibilité en pourcentage du test pendant les dernières 24 heures.

Statut
: Affiche le statut en cours du test. Le statut peut être Critique, Avertissement, Normal, Echec, Inactif ou Inconnu.

Avg. Response
: Affiche le temps de réponse moyen du test pendant les dernières 24 heures.

Vous pouvez surveiller trois types de test différents :

API REST
: Indique les temps de réponse d'une API REST. Tous les formats de demandes HTTP, comme GET, POST, PUT et DELETE, sont pris en charge.

Page Web
: Indique les temps de réponse pour le chargement du site Web sur l'URL que vous entrez.

Scripted behavior
Surveille des scripts Selenium que vous créez pour imiter les interactions d'un utilisateur avec un site Web. Ainsi, vous pouvez créer un script Selenium imitant un utilisateur qui se connecte à votre application. Exécutez ce script périodiquement pour tester les performances de votre application en réponse aux actions utilisateur qui sont automatisées par le script. Pour plus d'informations sur la création de scripts Selenium, voir «Enregistrement de scripts synthétiques», à la page 1058.

Pour ajouter un autre test, cliquez sur **Ajouter un nouveau test**.

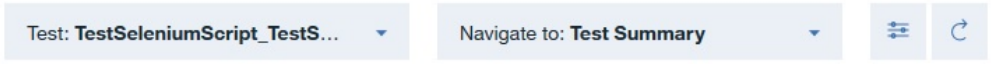
Pour arrêter, démarrer, supprimer ou éditer un test synthétique, cliquez sur l'icône **Actions** , puis cliquez sur l'action voulue. Pour afficher la **répartition** détaillée du test, cliquez sur ce dernier.

Pour visualiser l'utilisation spécifique de chaque test synthétique, cliquez sur l'icône **Coût** . Si vous avez souscrit au forfait payant, votre utilisation est affichée en points de données.

Répartition
Le tableau de bord **Répartition** affiche les statistiques clés sur vos tests. Il récapitule également les informations de disponibilité et de temps de réponse, les tendances dégagées de l'historique, et les données de performance des tests sur les 24 heures précédentes.

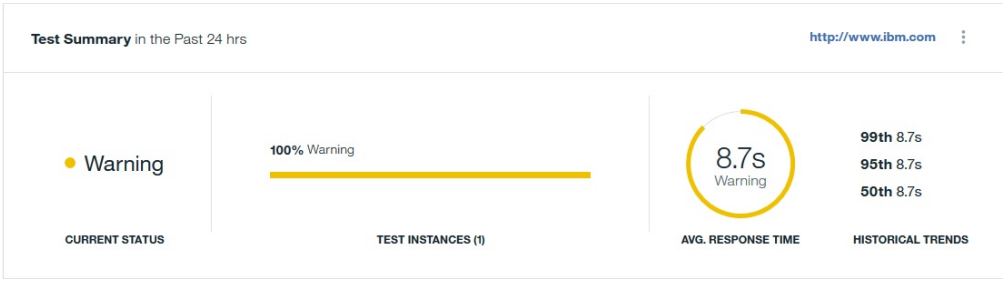
Pour afficher la répartition détaillée d'un test, cliquez sur celui-ci dans le panneau **Tests synthétiques**. Vous pouvez également ouvrir le tableau de bord **Répartition** en cliquant sur **Répartition** dans le tableau **Alertes** sur le panneau Fréquence des alertes.

Utilisez le menu déroulant **Test** pour afficher les répartitions des différents tests. Utilisez le menu déroulant **Accéder à** pour accéder rapidement à tout panneau.



Le tableau de bord Répartition affiche quatre panneaux.

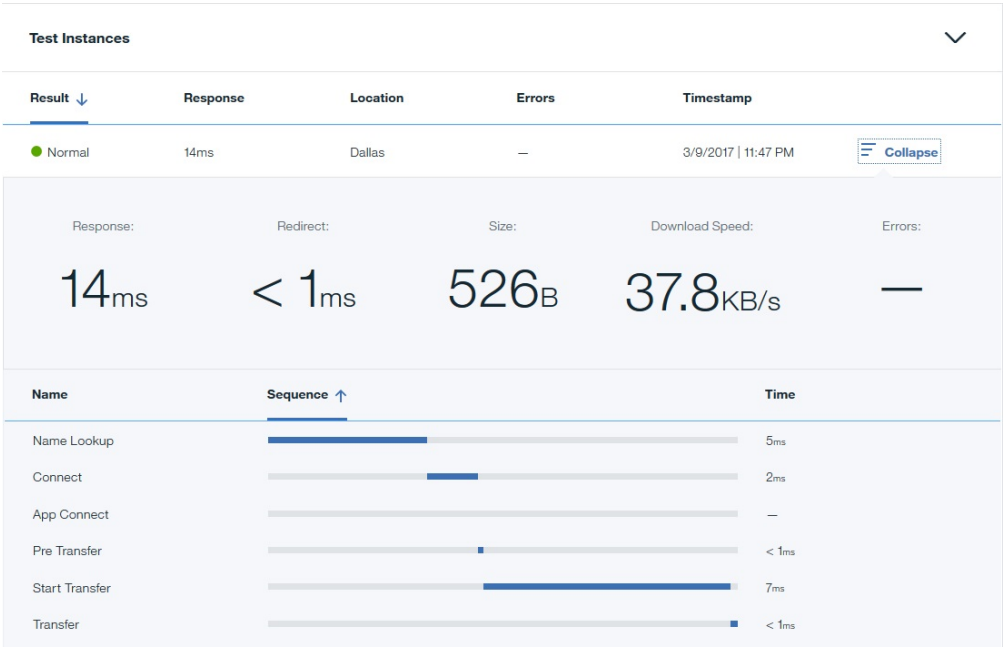
Récapitulatif du test



Le panneau **Récapitulatif du test** affiche les informations de test suivantes pour les dernières 24 heures :

- **Statut actuel** affiche le statut du test.
- **Instances de test** affiche la répartition en pourcentage d'instances de test de type normal, avertissement et critique.
- **Temps de réponse moyen** affiche le temps de réponse moyen du test.
- **Tendances de l'historique** affiche les tendances de l'historique de votre test de performances pour les 50e, 95e et 99e percentiles, en millisecondes.

Instances de test



La table **Instances de test** affiche des informations détaillées sur chaque instance de test, dont le statut, le temps de réponse, l'emplacement où s'exécute le test, le nombre d'erreurs et la date et l'heure de son exécution. Pour explorer en détail une instance de test, cliquez sur **Extension**. Des informations de réponse détaillée sont répertoriées pour chaque étape de l'instance de test. Vous pouvez trier les colonnes pour vous aider à identifier rapidement l'étape précise durant laquelle un ralentissement ou un échec s'est produit. L'affichage des erreurs, de la séquence de test et des temps de réponse vous permet d'identifier facilement les problèmes.

Les informations affichées dépendent du type de test synthétique qui fait l'objet de la surveillance.

API

Lorsque vous cliquez sur **Développer** pour une instance de test d'API, un récapitulatif de haut niveau affiche les informations suivantes :

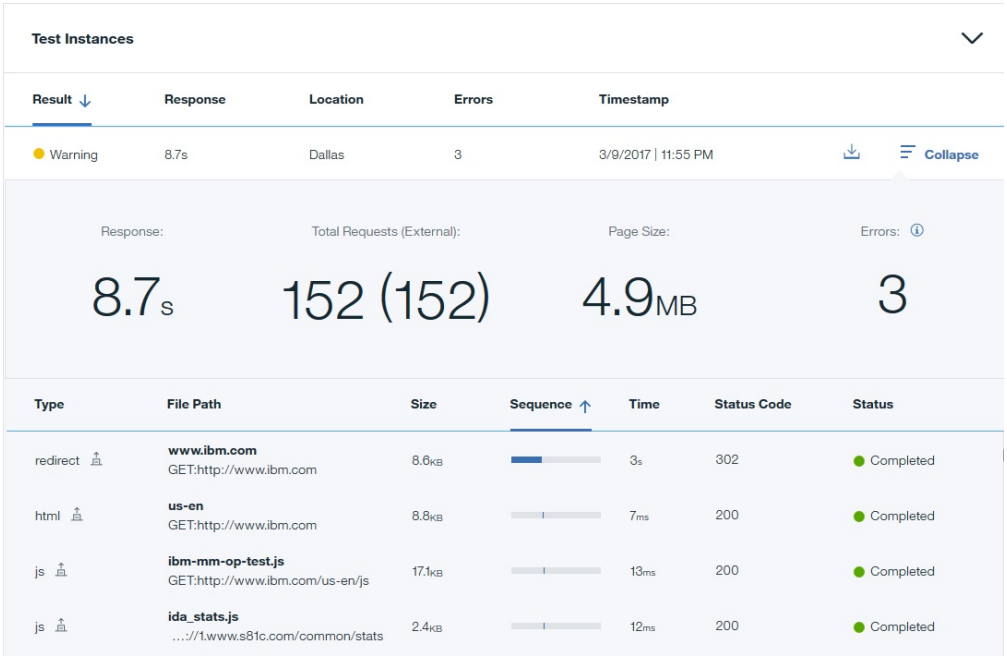
- **Réponse** affiche le temps de réponse total pour l'instance de test, y-compris le temps occupé par la redirection.
- **Redirection** affiche le temps total de redirection pour l'instance de test.
- **Taille** indique la taille de l'objet.
- **Vitesse de téléchargement** indique à quelle vitesse chaque objet a été téléchargé.
- **Erreurs** indique le nombre d'erreurs qui se sont produites au cours de l'instance de test. Pour consulter les détails des erreurs, cliquez sur l'icône **Information**.

Un tableau décrit chaque étape de l'appel d'API, en indiquant le nom de l'étape, la séquence des étapes et le temps de réponse pour chaque étape. Les noms d'étapes suivants s'affichent :

- **Recherche de nom** indique combien de temps l'instance de test a pris pour résoudre le nom de l'objet.
- **Connexion** indique combien de temps l'instance de test a pris depuis le début de l'étape jusqu'à l'établissement d'une connexion à l'hôte distant ou au proxy.
- **Connexion d'application** indique combien de temps l'instance de test a pris depuis le début de l'étape jusqu'à l'établissement de la connexion SSL avec l'hôte distant.
- **Pré-transfert** indique combien de temps s'est écoulé dans l'instance de test depuis le début de l'étape jusqu'au démarrage de la commande de transfert.
- **Démarrage du transfert** indique combien de temps s'est écoulé dans l'instance de test depuis le début de l'étape jusqu'à la réception du premier octet.

- **Transfert** indique combien de temps l'instance de test a pris pour transférer le fichier.

Page Web



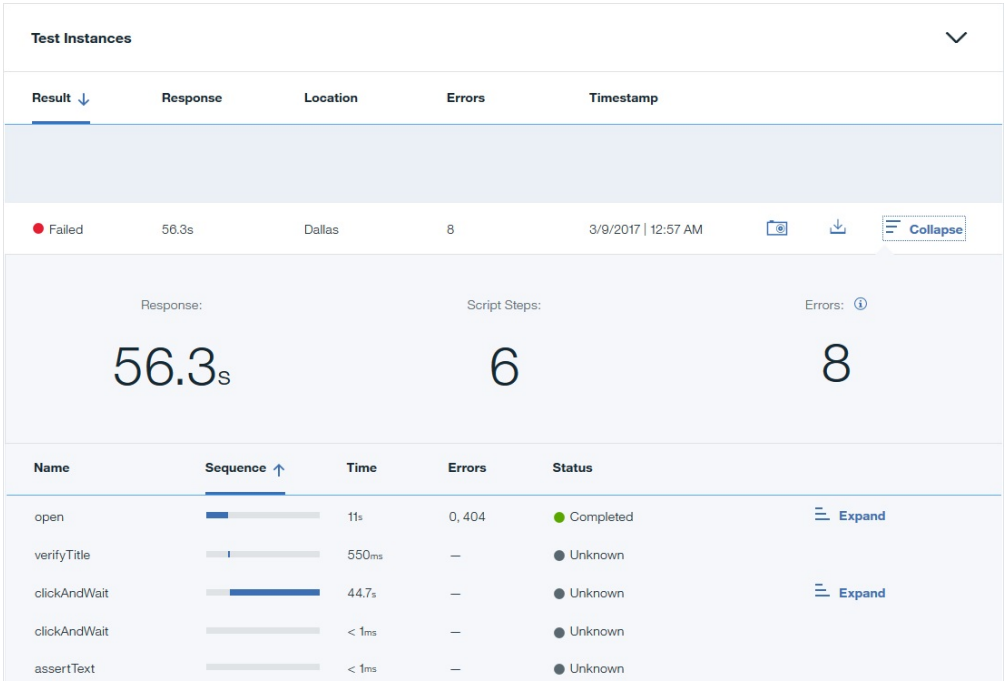
Lorsque vous cliquez sur **Développer** pour une instance de test de page Web, un récapitulatif de haut niveau affiche les informations suivantes :

- **Réponse** indique le temps de réponse de l'instance de test.
- **Nombre total de demandes (externes)** indique le nombre total de demandes pour l'instance de test. Le nombre de demandes externes est affiché entre parenthèses.
- **Taille de la page** indique la taille de la page Web.
- **Erreurs** indique le nombre d'erreurs qui se sont produites au cours de l'instance de test. Pour consulter les détails des erreurs, cliquez sur l'icône **Information**.

Une table répertoriant les informations suivantes pour chaque demande soumise par le test est également affichée :

- **Type** indique le type de la demande. Par exemple, HTML, CSS, JavaScript ou image. Les demandes externes et internes sont représentées par des icônes.
- **Chemin de fichier** indique l'emplacement de l'objet demandé.
- **Taille** indique la taille de l'objet demandé.
- **Séquence** indique la séquence des demandes soumises par le test.
- **Durée** indique la durée de réalisation de chaque demande.
- **Code de statut** indique le code de statut de la demande HTTP.
- **Statut** décrit le résultat de la demande (Terminé, Inconnu ou Echec, par exemple).

Script

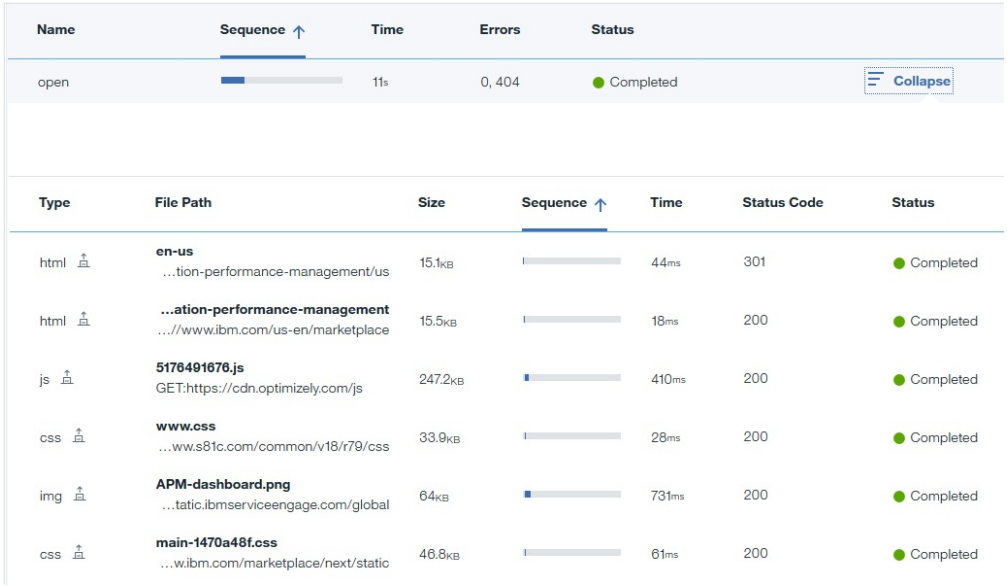


Lorsque vous cliquez sur **Développer** pour une instance de test de script, le temps de réponse, le nombre d'étapes du script et le nombre d'erreurs sont affichés. Pour consulter les détails des erreurs, cliquez sur l'icône **Information**.

Les informations suivantes sur chaque étape du script sont affichées dans un tableau :

- **Nom** affiche chaque commande Selenium appelée par votre instance de test. Par exemple, `Open`, `ClickAt` ou `VerifyBodyText`.
- **Séquence** affiche la séquence des étapes de script du début à la fin de l'instance de test.
- **Durée** indique la durée de réalisation de chaque étape du script.
- **Erreurs** indique le nombre d'erreurs qui se sont produites au cours de chaque étape du script.
- **Statut** décrit le résultat de l'étape de script (Terminé, Inconnu ou Echec, par exemple).

Vous pouvez explorer en aval et visualiser les informations sur les demandes générées par chaque étape du script.



Cliquez sur **Développer** pour afficher un tableau contenant les informations suivantes :

- **Type** indique le type de la demande. Par exemple, HTML, CSS, JavaScript ou image. Les demandes externes et internes sont représentées par des icônes.
- **Chemin de fichier** indique l'emplacement de l'objet demandé.
- **Taille** indique la taille de l'objet demandé.
- **Séquence** indique la séquence des demandes soumises par le test.
- **Durée** indique la durée de réalisation de chaque demande.
- **Code de statut** indique le code de statut de la demande HTTP.
- **Statut** décrit le résultat de la demande (Terminé, Inconnu ou Echec, par exemple).

Availability Monitoring peut automatiquement effectuer une capture d'écran si le chargement de la page Web ou une étape du script échouent. Ainsi, si l'une des étapes de votre script ouvre une page Web mais que celle-ci ne se charge pas, Availability Monitoring crée automatiquement une capture d'écran. Pour visualiser une capture d'écran de la page Web ou du script, cliquez sur l'icône **Capture d'écran de l'erreur**  . Cette fonction n'est disponible que pour la page Web et les tests préétablis. Elle ne fonctionne pas avec les tests d'API REST.

Vous pouvez aussi télécharger un enregistrement du trafic réseau pour une instance de test spécifique sous forme de fichier `.har` en cliquant sur l'icône **Télécharger**  . Cette fonction est disponible pour la page Web et les tests de comportement préétablis.

Temps de réponse et disponibilité

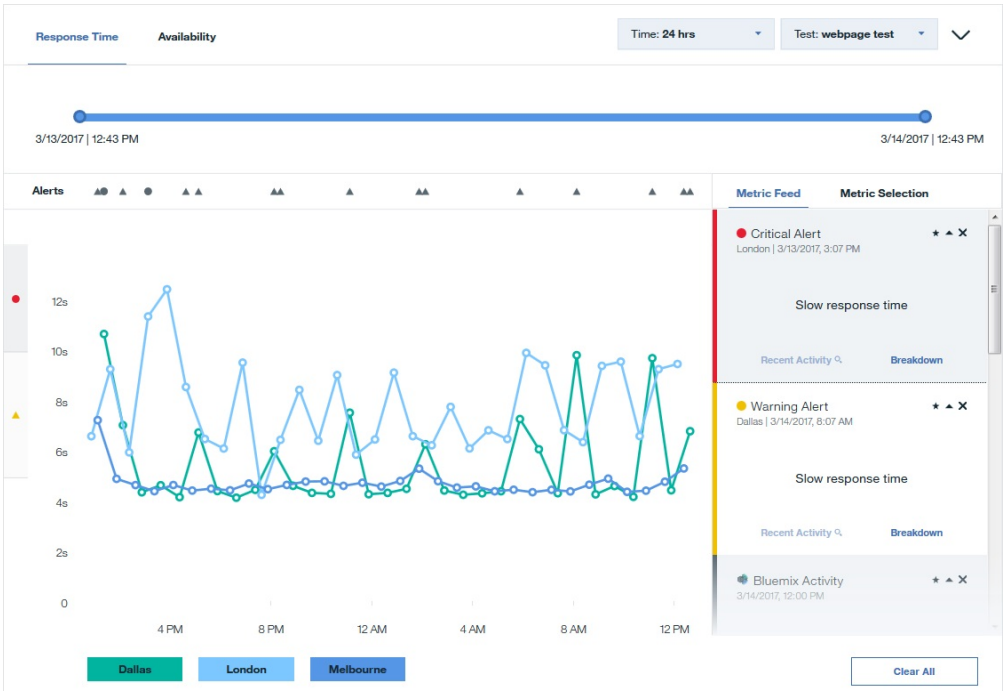
Le panneau **Temps de réponse et disponibilité** affiche un graphique des temps de réponse mesurés et de la disponibilité des instances de votre test sur la période définie. Pour plus d'informations, voir «Temps de réponse et disponibilité», à la page 1098.

Temps de réponse et disponibilité

Utilisez les panneaux **Temps de réponse** et **Disponibilité** pour vous aider à visualiser le temps de réponse, les tendances de disponibilité et les alertes dans le temps.

Graphique Temps de réponse

Les informations de temps de réponse s'affichent sur un diagramme linéaire. Pour le visualiser, cliquez sur l'onglet **Temps de réponse**.



Important : Les temps de réponse mesurés par Availability Monitoring sont légèrement supérieurs aux temps de réponse perçus par les utilisateurs. Availability Monitoring simule le comportement réel de l'utilisateur, ce qui augmente les temps de réponse. Le temps de réponse augmente avec les facteurs suivants :

- Availability Monitoring crée une instance Firefox pour chaque test afin d'empêcher les instances de test précédentes d'influencer le test en cours. Les utilisateurs réels peuvent constater des temps de réponses plus courts en raison de la mise en cache du navigateur.
- Availability Monitoring installe le plug-in de pilote Web de Firefox avant chaque test.

Les différents temps de réponse des tests sont représentés par une icône **Point de réponse** sur le diagramme linéaire. Des couleurs différentes indiquent les divers emplacements géographiques dans lesquels l'application s'exécute. L'axe des Y du graphique utilise des icônes d'alerte pour identifier les plages de seuils Avertissement et Critique. L'icône d'avertissement jaune représente la plage de seuil d'avertissement, et l'icône critique rouge représente la plage de seuil critique. Cliquez sur l'icône d'avertissement jaune ou l'icône critique rouge pour identifier aisément les instances de test signalées sur les plages de seuil d'avertissement ou critique. Pour visualiser les détails d'une instance de test spécifique, cliquez sur **Point de réponse** sur le graphique.

Filtres

Choisissez un test dans le menu déroulant **Test**. Vous pouvez filtrer les données sur 3 heures, 24 heures, 7 jours, 30 jours et 12 mois. Quand vous procédez à un filtrage pour une plage de temps supérieure à 24 heures, une moyenne des valeurs s'affichant dans le graphique est effectuée. Pour afficher des informations plus spécifiques, cliquez sur le graphique pour explorer en détail les alertes et avertissements individuels. Vous pouvez aussi utiliser le curseur pour restreindre ou étendre la plage de temps.

Le graphique Temps de réponse permet de mettre en évidence et de masquer les données d'emplacements POP particuliers. Pour mettre en évidence les données de temps de réponse d'un emplacement POP particulier, survolez son nom, puis cliquez sur l'icône **Mettre en évidence l'emplacement** . Pour masquer les données de temps de réponse d'un emplacement POP,

survolez son nom puis, cliquez sur l'icône **Masquer l'emplacement** . Pour restaurer les données de l'emplacement POP dans le graphique, cliquez sur **Ajouter plus d'emplacements** ou sur l'onglet **Sélection de métrique**, puis cliquez sur l'emplacement de point de présence que vous aviez retiré.

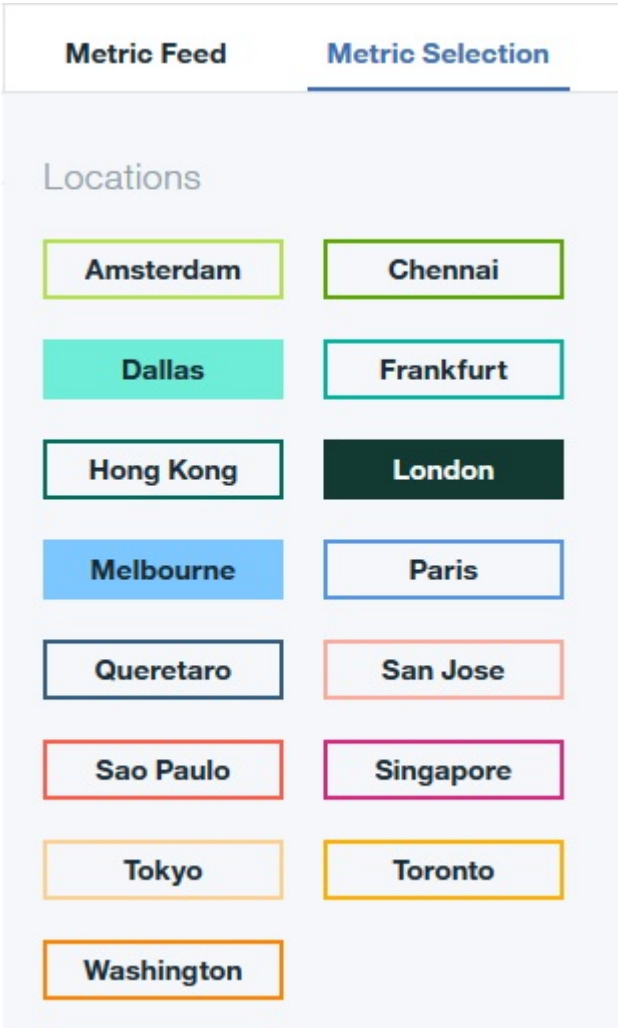
Alertes

Vous pouvez facilement identifier les alertes Critique et Avertissement dans la ligne Alertes. Survolez une **icône d'alerte** pour identifier la gravité et l'horodatage de l'alerte. Cliquez sur une **icône d'alerte** pour afficher les détails pour cette alerte dans **Flux métrique**.

Si plusieurs icônes sont juxtaposées sur la ligne Alertes, une **icône de nombre** affiche le nombre d'alertes à cet instant donné. Survolez l'**icône de nombre** pour afficher les différentes alertes et cliquez sur une alerte pour afficher les informations dans le **Flux métrique**

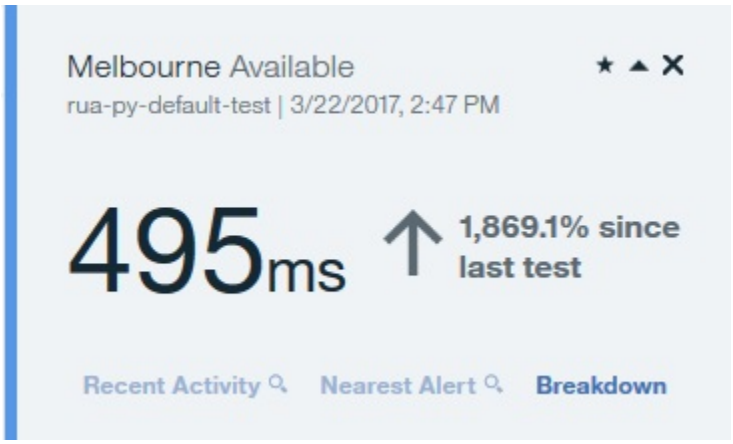
Sélection de métrique et Flux métrique

Pour filtrer d'après des métriques définies par région géographique, cliquez sur **Sélection de métrique**. Cliquez sur un emplacement pour ajouter ou retirer des métriques qui sont mesurées à cet emplacement depuis le graphique. Cliquez sur **Ajouter plus d'emplacements** pour ouvrir la page Tester le mode édition et ajouter un emplacement POP au test sélectionné.

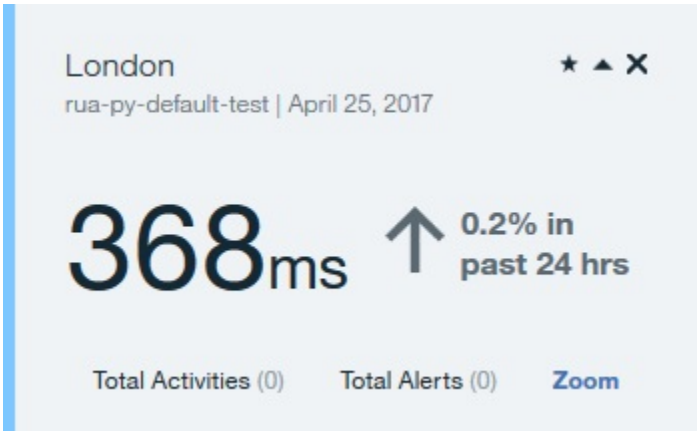


Pour afficher une liste des détails relatifs aux métriques, cliquez sur **Flux métrique**. **Flux métrique** affiche une liste des instances dans lesquelles une métrique est satisfaite.

Cliquez sur une **icône d'alerte** ou de **point de réponse** sur le graphique pour ajouter les détails de cette métrique dans **Flux métrique**.



Si vous filtrez le graphique Temps de réponse sur une plage de temps supérieure à 24 heures et si vous cliquez sur un **point de réponse**, le **flux métrique** montre les informations cumulées correspondant à cette journée.

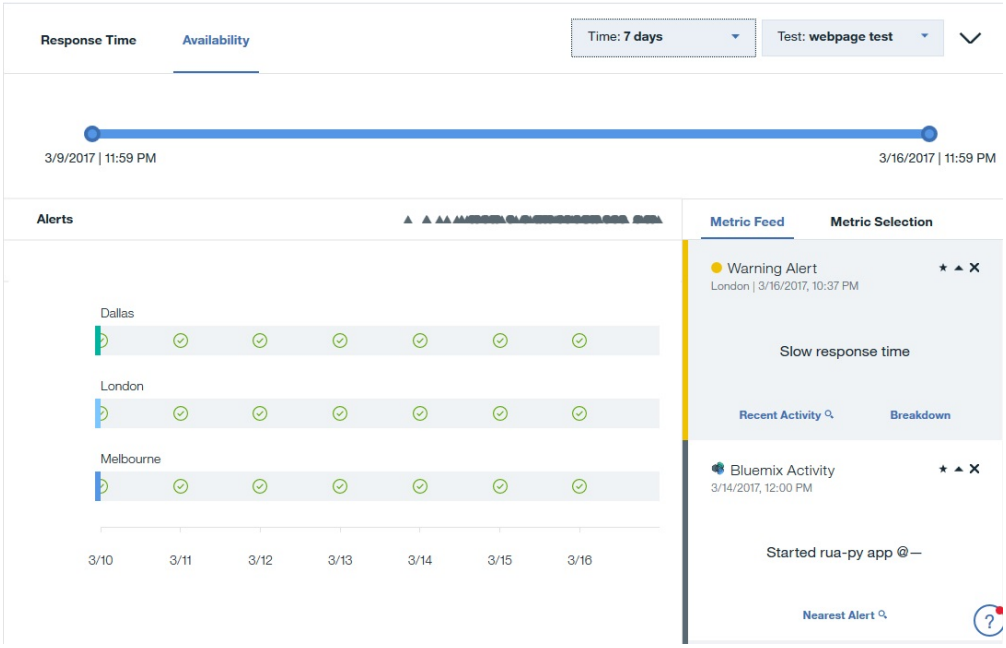


Cliquez sur **Zoom** pour afficher tous les temps de réponse et les alertes générés par le test pour ce jour dans le graphique Temps de réponse.

Pour afficher les informations détaillées sur une alerte ou un temps de réponse de test, cliquez sur **Répartition** dans **Flux métrique**. Cliquez sur **Alerte la plus proche** pour afficher l'alerte la plus proche de cette instance de test dans **Flux métrique**, si une alerte s'est produite.

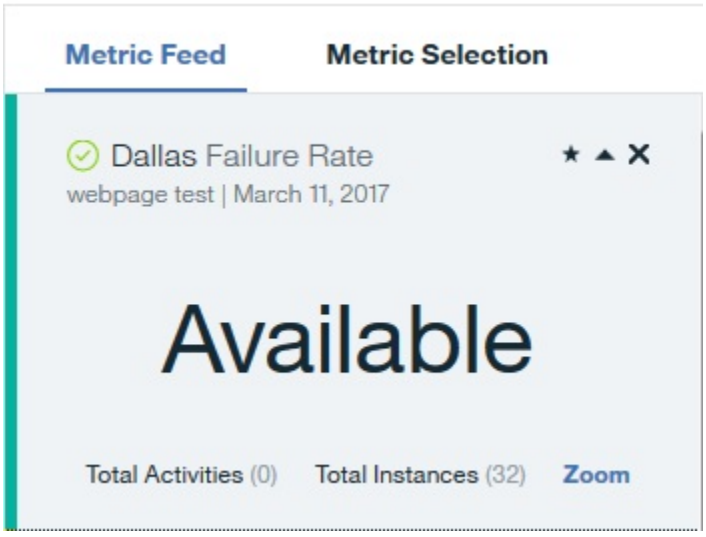
Disponibilité

Pour afficher les informations de disponibilité pour vos applications, cliquez sur **Disponibilité**. Le graphique Disponibilité affiche la disponibilité quotidienne de chaque point de présence (ou point POP, pour Point of Presence) pour le test sélectionné.



Le graphique Disponibilité permet de mettre en évidence et de masquer les données d'emplacements POP particuliers. Pour mettre en évidence les données de disponibilité d'un emplacement POP particulier, survolez son nom, puis cliquez sur l'icône **Mettre en évidence l'emplacement**  . Pour masquer les données de disponibilité d'un emplacement POP, survolez son nom puis, cliquez sur l'icône **Masquer l'emplacement**  . Pour restaurer les données de l'emplacement POP dans le graphique, cliquez sur l'onglet **Sélection de métrique**, puis sur l'emplacement POP que vous aviez retiré.

Survolez un point du graphique pour afficher le taux d'échec et le nombre d'instances de test pour un jour et un emplacement particulier. Cliquez sur un point du graphique pour afficher ces informations dans **Flux métrique**.



Cliquez sur **Zoom** pour filtrer le graphique **Disponibilité** et le graphique **Temps de réponse** afin d'afficher les informations pour le jour sélectionné.

Utilisation d'Availability Monitoring

Vous pouvez visualiser des détails sur l'utilisation d'Availability Monitoring sur l'onglet **Monitoring** de la sous-fenêtre d'application et sur le tableau de bord principal d'Availability Monitoring.

Pour afficher une présentation de votre utilisation depuis le tableau de bord principal d'Availability

Monitoring, cliquez sur l'icône **Configurer** . Si vous utilisez la version d'essai d'Availability Monitoring, votre utilisation est affichée sous forme d'un graphique à barres, ainsi que le nombre de tests en cours. Si vous utilisez le plan Paid, votre utilisation est affichée sous forme de points de données. Vous pouvez consulter des informations d'utilisation détaillées pour chaque test individuel dans le panneau **Tests synthétiques**.

Votre utilisation est mesurée en points de données. Le nombre de points de données estimé est calculé à partir de la formule suivante :

Nombre de points de données estimé = T * L * (60/M * 24 * 30) par mois

Où T = nombre de tests synthétiques qui sont exécutés, L = nombre d'emplacements, et M = intervalle entre les tests (minutes).

Les tests simples tels que les tests de page Web et d'API REST utilisent 1 point de données pour chaque test. Les tests avancés tels que les tests de scripts Selenium et de scripts d'API REST utilisent 100 points de données pour chaque test.

Exploration des API

Utilisez les API IBM Cloud Application Performance Management pour créer des scripts afin d'automatiser l'intégration de votre environnement Cloud APM .A partir de l'offre de service gérée par API Cloud APM de l'Explorateur d'API sous IBM developerWorks, vous pouvez accéder aux API Resource Group Management Service, Threshold Management Service et Role-Based access control Service disponibles.

Avant de commencer

Vous devez avoir un abonnement actif à Cloud APM pour obtenir une clé d'ID client et exécuter des opérations API.

Procédure

1. Ouvrez l'Explorateur d'API dans votre navigateur : https://developer.ibm.com/api.
2. Connectez-vous avec votre ID IBMid.
3. Dans la zone **Search All APIs**, entrez `gestion des performances` et cliquez sur .
4. Sélectionnez la mosaïque de l'API IBM Cloud Application Performance Management.
5. Cliquez sur **Documentation** à gauche de la fenêtre Explorateur d'API.
6. Sélectionnez l'API spécifique.
7. Sélectionnez la sous-section pour développer la liste des opérations API.
8. Pour poursuivre, vous avez besoin d'un abonnement Cloud APM actif. Effectuez l'une des étapes suivantes :
   a) Si vous ne possédez pas d'abonnement Cloud APM, inscrivez-vous pour bénéficier d'un abonnement à l'essai gratuit de 30 jours.
   b) Si vous possédez déjà un abonnement, connectez-vous en cliquant sur **Mes API** pour tester certaines des opérations d'API dans l'Explorateur d'API.

   Lorsque votre abonnement est actif et que vous êtes connecté à la page de l'Explorateur d'API, vous pouvez voir une liste de vos abonnements d'API.
9. Sélectionnez une opération API pour plus de détails.
10. Sélectionnez l'un des langages (tels que shell ou curl) en haut de la page de l'API Explorer pour afficher un exemple de demande.

11. Récupérez votre clé d'identificateur client et votre clé secrète client et stockez-les dans un endroit sûr pour une utilisation externe.

    Envoyez votre clé d'identificateur client et votre clé secrète client avec chaque demande d'API. Vous devez posséder un abonnement Cloud APM pour pouvoir effectuer cette action.

Que faire ensuite

Pour plus d'informations sur la manière d'exécuter des opérations API, voir les rubriques suivantes :

«Accès et utilisation de l'API Role-Based Access Control Service», à la page 1041
«Utilisation de l'API Resource Group Management Service», à la page 1026
«Utilisation de l'API Threshold Management Service», à la page 1028

Configuration avancée

Utilisez la page **Configuration avancée** pour contrôler les paramètres de communications et les fonctions avancées, par exemple l'acheminement d'événement.

Une fois que vous avez cliqué sur **Configuration système** > **Configuration avancée**, les catégories de configuration ci-dessous s'affichent sur la page Configuration avancée.

Intégration de l'interface utilisateur

Pour les produits qui s'intègrent à la console Cloud APM, vous pouvez ajouter ou éditer l'URL permettant de lancer l'application intégrée. Les zones sont alimentées avec les URL définies lors de la procédure de configuration de l'intégration.

- L'**URL de Log Analysis** permet de lancer IBM Operations Analytics - Log Analysis pour effectuer des recherches dans les journaux d'application du Tableau de bord d'Application Performance. Pour plus d'informations, voir «Recherche dans les fichiers journaux», à la page 1111.
- **Activer les événements sous-noeud**, pour les agents avec sous-noeuds, contrôle si les sous-noeuds apparaissent dans l'onglet Evénements. Lorsque les événements de sous-noeud sont activés, le noeud et le sous-noeud pour lesquels un événement a été ouvert s'affichent. En particulier, si vous voulez afficher les situations de surveillance des fichiers journaux dans l'onglet Evénements, vous devez vérifier que les événements de sous-noeud sont activés. Valeur par défaut : `False`.
- **Dashboard Refresh Rate** contrôle la fréquence d'actualisation automatique du Tableau de bord d'Application Performance. Vous pouvez ajuster le paramètre sur une valeur comprise entre 1 et 60 minutes. Le paramètre affecte le statut des ressources qui s'affiche dans le navigateur et dans l'onglet Présentation des statuts. Il n'a aucun impact sur les entrées de l'onglet Evénements. Valeur par défaut : 1 minute.

Gestionnaire d'événements

Le gestionnaire d'événements contrôle l'acheminement des événements à l'aide du Protocole SMTP (Simple Mail Transfer Protocol), ainsi que les notifications par e-mail. Si vous entrez une valeur pour Adresses e-mail cible, un e-mail est envoyé pour chaque événement d'ouverture, de fermeture et d'arrêt. Vous pouvez utiliser les zones **Gestionnaire d'événements** pour configurer des événements à partir de Cloud APM pour ouvrir automatiquement des tickets dans IBM Control Desk. Pour connaître les tâches de configuration supplémentaires, voir Intégration à Control Desk «Intégration à Control Desk», à la page 999.

Si vous configurez le réexpéditeur SMTP afin qu'il utilise SSL, vous devez ajouter le certificat de l'autorité de certification signataire du serveur SMTP au fichier de clés du serveur Cloud APM. Ajoutez le certificat de l'autorité de certification au fichier de clés par défaut en utilisant la commande keytool de la machine JVM :

```
rép_install/java/jre/bin/keytool -importcert\
-noprompt \
-alias votre_alias_cert_AC \
```

```
-file chemin_vers_votre_fichier_cert_AC (*.cer)
 -keystore /rép_install/wlp/usr/servers/min/resources/security/key.jks \
-storepass ccmR0cKs! \
-storetype jks \
-trustcacerts
```

Pour visualiser un exemple de courrier électronique, voir «E-mail d'événement», à la page 1106.

- **Adresses e-mail cibles** indique les adresses électroniques vers lesquelles sont acheminés les événements. Séparez chaque adresse par une virgule (,), comme `annette@ibm.com,jim@ibm.com,owen@ibm.com`.
- **Alert Notification for ITMv6** est l'option qui permet d'activer les événements Alert Notification for ITMv6 en définissant la valeur `True`. Valeur par défaut : `False`
- **Webhook de gestion des événements Cloud** correspond à l'URL de webhook générée dans Cloud Event Management lorsque vous configurez l'intégration entre IBM Cloud Application Performance Management et Cloud Event Management. Vous devez coller l'URL de webhook générée ici pour que les événements soient transmis depuis Cloud APM.

Vous pouvez utiliser Alert Notification au lieu de la fonction de messagerie du gestionnaire d'événements pour contrôler les personnes notifiées pour des événements différents et leur mode de notification. Pour plus d'informations, voir «Intégration à Alert Notification», à la page 998.

Si vous transmettez des événements à un récepteur EIF (Event Integration Facility), vous pouvez personnaliser les emplacements EIF de sorte à ajouter un attribut à l'événement EIF. Pour plus d'informations, voir «Personnalisation d'un événement à transmettre à un récepteur EIF», à la page 1019. Pour plus d'informations sur la transmission de vos événements au gestionnaire d'événements IBM Netcool/OMNIbus, voir Intégration à Netcool/OMNIbus (cloud) ou Intégration à Netcool/OMNIbus (sur site) dans le «Intégration à Netcool/OMNIbus», à la page 992.

Service d'analyse de suivi

Paramètres utilisés pour le service d'analyse de suivi. Les paramètres s'appliquent uniquement à l'offre Cloud APM, Advanced et si vous configurez le suivi des transactions dans votre environnement.

- La **Taille du pool de connexions** correspond au nombre de connexions Db2 simultanées que le service d'analyse du suivi maintient dans le pool de connexions pour la demande des "*N* premiers". Augmentez cette valeur si vous êtes confronté à des périodes pour lesquelles le délai est lent en raison d'un nombre important d'utilisateurs simultanés de la console Cloud APM. Valeur par défaut : `10`.
- Les **Pseudo-noeuds** activent la visualisation des services qui ne sont pas instrumentés. Valeur par défaut : `True`.
- Le **Délai d'attente de requête en secondes** est le nombre de secondes nécessaires à chaque demande des "*N* premiers" (où *N* est un nombre comme dans "5 premiers" ou "10 premiers") avant que le délai d'attente soit dépassé. La valeur du délai d'attente peut être augmentée pour les applications dont la charge de travail est plus élevée et dont les périodes de délai attendues sont plus importantes. Valeur par défaut : `120` secondes.
- En général, le paramètre **Réoptimisation des requêtes DB2 activée** n'a pas à être modifié. Ce paramètre affecte l'optimiseur de requêtes Db2. Dans certains environnements, la désactivation de l'optimiseur peut améliorer les performances pour certains ensembles de transactions. Valeur par défaut : `False`.

Fonction d'abonnement d'agent

Agent Subscription Facility inclut l'interface REST (Representative State Transfer) de l'agent et le serveur HTTP de Central Configuration Services. L'interface REST est utilisée par les agents et les collecteurs de données pour envoyer les données de surveillance conservées sur le serveur Db2 et les événements de seuil. Le serveur HTTP de Central Configuration Services gère les demandes des agents pour les fichiers de configuration, tels que les définitions de seuil. Utilisez ces paramètres pour configurer les communications entre la fonction d'abonnement d'agent et le serveur Cloud APM.

- **Limite du nombre d'interrogations manquées (signal de présence rapide)** désigne le nombre maximal de fois où un agent de surveillance, avec un intervalle entre les signaux de présence

inférieur ou égal à 60 secondes, ne parvient pas à se connecter avant d'être marqué comme étant hors ligne. Valeur par défaut : 30 intervalles.

- **Limite du nombre d'interrogations manquées (signal de présence lent)** désigne le nombre maximal de fois où un agent de surveillance, avec un intervalle entre les signaux de présence supérieur à 60 secondes, ne parvient pas à se connecter avant d'être marqué comme étant hors ligne. Valeur par défaut : 3 intervalles.
- **Délai d'expiration de la transaction** désigne la durée, en secondes, pendant laquelle le serveur attend une réponse à une demande. Valeur par défaut : 120 secondes.
- **Délai avant suppression d'un système hors ligne** détermine le nombre de minutes d'attente avant le retrait de l'affichage d'un système géré hors ligne. Dans le Tableau de bord d'Application Performance, les systèmes gérés hors ligne sont identifiés par l'indicateur de statut inconnu . Le système géré reste affiché, même si vous désinstallez l'agent, jusqu'à ce que le délai soit terminé. Pour plus d'informations, voir «Affichage et suppression des agents en ligne», à la page 1135. Valeur par défaut : 5760 minutes (4 jours).

Activation des seuils

Vos agents de surveillance contiennent tous un ensemble de seuils prédéfinis qui sont activés et démarrés avec l'agent. Ces seuils prédéfinis sont affectés au groupe de ressources système par défaut pour l'agent.

- L'option **Sélectionnez une action afin de définir la règle des seuils de meilleure pratique prédéfinis** contrôle si les seuils prédéfinis pour vos ressources gérées sont activés ou désactivés par défaut. Définissez la zone sur **Désactiver tout** si vous ne voulez pas exécuter les seuils prédéfinis. Le paramètre **Désactiver tout** supprime l'affectation du groupe de systèmes de tous les seuils prédéfinis. Un seuil auquel aucun groupe n'est affecté n'est distribué à aucun système surveillé et reste arrêté jusqu'à ce qu'il soit distribué à un groupe de ressources. Si vous décidez par la suite d'activer les seuils prédéfinis, définissez la zone sur **Activer tout**.

Pour plus d'informations sur les seuils prédéfinis et les seuils personnalisés, voir «Informations de référence», à la page 1004 et «Exemples de seuils désactivés», à la page 1006.

E-mail d'événement

Utilisez les zones du Gestionnaire d'événements de la page Configuration avancée pour configurer la notification d'événements par courrier électronique à une liste de destinataires.

Email for open event

Lorsqu'une condition de seuil est vérifiée, un événement est ouvert et le message électronique envoyé par le serveur Cloud APM contient les attributs de base qui s'appliquent à tous les événements, ainsi que les attributs de la première ligne du jeu de données correspondant à la condition de seuil. L'attribut situation_status possède la valeur Y pour les événements ouverts.

Email for close events

Lorsqu'une condition de seuil n'est plus vérifiée, un événement de fermeture est généré. Le message électronique des événements de fermeture ne contient que les attributs de base qui s'appliquent à tous les événements d'agent et la valeur de l'attribut situation_status est N. Les attributs de l'agent ne sont pas inclus dans ces messages électroniques car la condition de seuil n'est pas remplie.

Email for stop event

Lorsqu'un seuil est arrêté, un événement d'arrêt est généré. Le message électronique des événements d'arrêt ne contient que les attributs de base qui s'appliquent à tous les événements d'agent et la valeur de l'attribut situation_status est P. Les attributs de l'agent ne sont pas inclus dans ces messages électroniques car la condition de seuil n'est pas remplie.

Un seuil est arrêté pour un agent si vous supprimez la définition de seuil ou que vous modifiez l'une des définitions de seuil distribuées à l'agent.

Les exemples suivants montrent un e-mail pour un événement d'ouverture :

```
From:    noreply@apm.ibmserviceengage.com
To:         tester@us.ibm.com
Date:    10/25/2017 01:56 PM
Subject:    Linux_Disk_Space_Low on nc049048:LZ (Notification)
```

```
Le texte ci-dessous répertorie les informations reçues de l'agent qui a déclenché cet événement.
Les valeurs IP et Agent identifient l'agent qui a détecté l'événement.
Les valeurs Description et Severity indiquent le nom de la définition de seuil et sa gravité.
Sous la description se trouvent toutes les paires attribut/valeur présentes dans l'événement,
dans leur forme brute.
    Server IP  : 10.107.76.230 (SIDR26APAP1BLUE.test.ibm.com)
    Agent IP   : 9.42.49.48
    Agent      : nc049048:LZ
    Severity   : warning
    Description: Linux_Disk_Space_Low[Disk_Free_Percent <= 20  AND Disk_Free_Percent > 10
                 AND FS_Type != nfs  AND FS_Type != iso9660 ]
      ITM_KLZ_Disk
      ManagedSystemGroups='*LINUX_SYSTEM'
      TenantID=F43E-D704-DADC-6270-1ED8-543E-A388-6513
      adapter_host=nc049048.tivlab.raleigh.ibm.com
      apm_hostname=SIDR26APAP1BLUE.test.ibm.com
      appl_label=A:P:S
      date=01/25/2017
      disk_free=5843
      disk_free_percent=20
      disk_name=/dev/sda2
      disk_used=22676
      disk_used_percent=80
      file_system_status=2
      file_system_status_enum=Up
      fqhostname=nc049048.test.ibm.com
      fs_type=ext4
      hostname=nc049048.test.ibm.com
      identifier=Linux_Disk_Space_Lownc049048:LZ/ITM_KLZ_Disk
      inodes_free=1721587
      inodes_free_percent=88
      inodes_used=232477
      inodes_used_percent=12
      integration_type=U
      mount_options=rw
      mount_point=/
      msg='Linux_Disk_Space_Low[Disk_Free_Percent <= 20  AND Disk_Free_Percent > 10  AND FS_Type !
= nfs
     AND FS_Type != iso9660 ]'
      origin=9.42.49.48
      severity=WARNING
      situation_displayitem=/
      situation_eventdata='disk_name=/dev/
sda2;inodes_used_percent=12;mount_options=rw;fs_type=ext4;

system_name=nc049048:LZ;mount_point=/;disk_used_percent=80;disk_free=5843;file_system_status_enum=
Up;
     size=30040;disk_used=22676;inodes_used=232477;disk_free_percent=20;file_system_status=2;
     total_inodes=1954064;inodes_free=1721587;timestamp=1170125135553000;inodes_free_percent=88;~'
      situation_name=Linux_Disk_Space_Low
      situation_origin=nc049048:LZ
      situation_origin_uuid=09fb36afd6b3.22.02.09.2a.31.30.56.9d
      situation_status=Y
      situation_thrunode=nc049048:LZ
      situation_time='01/25/2017 13:55:55.000'
      situation_type=S
      size=30040
      source='ITM Agent: Private Situation'
      sub_origin=/
      sub_source=nc049048:LZ
      system_name=nc049048:LZ
      timestamp=1170125135553000
      tmz_diff=18000
      total_inodes=1954064
Pour vous désabonner de ces e-mails, connectez-vous à la console Cloud APM et retirez
votre adresse e-mail de
la liste des adresses e-mail cible dans la catégorie Gestionnaire
d'événements de la page Configuration avancée.
```

L'exemple suivant montre un e-mail pour un événement de fermeture.

```
From:    noreply@apm.ibmserviceengage.com
To:      tester@us.ibm.com
Date:    01/25/2017 02:01 PM
Subject:    Linux_Disk_Space_Low on nc049048:LZ (Closed)
Le texte ci-dessous répertorie les informations reçues de l'agent qui a déclenché cet événement.
Les valeurs IP et Agent identifient l'agent qui a détecté l'événement.
Les valeurs Description et Severity indiquent le nom de la définition de seuil et sa gravité.
Sous la description se trouvent toutes les paires attribut/valeur présentes dans l'événement,
dans leur forme brute.
    Server IP  : 10.107.76.230 (SIDR26APAP1BLUE-12f.test.ibm.com)
    Agent IP   : 9.42.49.48
```

```
    Agent      : nc049048:LZ
    Severity   : warning
    Description: Linux_Disk_Space_Low[Disk_Free_Percent <= 20  AND Disk_Free_Percent > 10
                 AND FS_Type != nfs  AND FS_Type != iso9660 ]
      ITM_KLZ_Disk
      ManagedSystemGroups='*LINUX_SYSTEM'
      TenantID=F43E-D704-DADC-6270-1ED8-543E-A388-6513
      adapter_host=nc049048.tivlab.raleigh.ibm.com
      apm_hostname=SIDR26APAP1BLUE-12f.test.ibm.com
      appl_label=A:P:S
      date=01/25/2017
      fqhostname=nc049048.test.ibm.com
      hostname=nc049048.test.ibm.com
      identifier=Linux_Disk_Space_Lownc049048:LZ/ITM_KLZ_Disk
      integration_type=U
      msg='Linux_Disk_Space_Low[Disk_Free_Percent <= 20  AND Disk_Free_Percent > 10  AND FS_Type !
= nfs
     AND FS_Type != iso9660 ]'
      origin=9.42.49.48
      severity=WARNING
      situation_displayitem=/
      situation_eventdata=~
      situation_name=Linux_Disk_Space_Low
      situation_origin=nc049048:LZ
      situation_origin_uuid=09fb36afd6b3.22.02.09.2a.31.30.56.9d
      situation_status=N
      situation_thrunode=nc049048:LZ
      situation_time='01/25/2017 14:00:55.000'
      situation_type=S
      source='ITM Agent: Private Situation'
      sub_origin=/
      sub_source=nc049048:LZ
      tmz_diff=18000
Pour vous désabonner de ces e-mails, connectez-vous à la console Cloud APM et
retirez votre adresse e-mail de
la liste des adresses e-mail cible dans la catégorie Gestionnaire
d'événements de la page Configuration avancée.
```

Chapitre 10. Utilisation des tableaux de bord

Sélectionnez **Performance** > **Tableau de bord d'Application Performance** pour obtenir une présentation complète du statut de vos applications. Vous pouvez effectuer une exploration en aval de la vue la plus générale à la vue détaillée des mesures, dans le même écran.

Utilisez les outils disponibles dans les tableaux de bord pour examiner les conditions ayant le statut critique ou avertissement dans votre environnement, créer des vues de mesures supplémentaires, ainsi que pour exécuter des actions telles que des recherches dans les journaux de trace et la comparaison de mesures dans le temps.

Toutes mes applications - Tableau de bord d'Application Performance

Le Tableau de bord d'Application Performance présente le récapitulatif des statuts de vos domaines surveillés dans **Toutes mes applications**. Une *zone récapitulative* est affichée pour chaque application définie par l'utilisateur, comme par exemple "Inventory Management", et pour les applications prédéfinies, "Mes composants" ou "Mes transactions" si votre environnement inclut de telles applications. A partir des zones récapitulatives ou du navigateur, explorez en aval chaque application et ses constituants afin d'en voir les mesures détaillées.

Au fur et à mesure que vous sélectionnez des éléments, le chemin correspondant s'affiche au-dessus du titre de l'élément sélectionné et vous pouvez cliquer sur l'un des liens de chemin pour revenir à cette vue.

A partir de n'importe quelle page de la console Cloud APM, vous pouvez cliquer sur **Performance** > **Tableau de bord d'Application Performance** pour ouvrir le tableau de bord **Toutes mes applications**. Visualisez les domaines qui vous intéressent en les sélectionnant dans le navigateur ou en cliquant dans une zone récapitulative pour accéder au niveau suivant.

Zones récapitulatives

Toutes mes applications comporte une zone récapitulative pour chaque application définie. Des indicateurs définissent la gravité de statut la plus élevée pour l'application dans la barre de titre et pour chaque groupe dans la zone récapitulative. Les groupes prédéfinis disponibles sont les suivants, selon les produits de surveillance inclus dans l'application définie :

L'Availability Monitoring n'a pas de sous-groupe

Composants contient un sous-groupe pour chaque type d'agent de surveillance prenant en charge votre application

Transactions peut inclure **Transactions utilisateur final** et **Transactions synthétiques** (IBM Website Monitoring on Cloud avant l'édition d'août 2017)

De plus, chaque zone récapitulative inclut la zone **Evénements**, qui affiche la gravité de l'événement dont la gravité est la plus élevée ayant été ouvert pour l'application. Vous pouvez cliquer sur le lien Evénements pour rechercher tous les événements ouverts (voir «Statut de l'événement», à la page 1140).

 . Cliquez sur la barre de titre d'une zone récapitulative pour ouvrir l'onglet Présentation des statuts de l'application. Ou cliquez sur l'une des icônes de zone récapitulative pour ouvrir l'onglet Présentation des statuts pour le groupe Composants ou le sous-groupe Utilisateurs ou Transactions, ou pour ouvrir l'onglet Evénements pour le groupe ou le sous-groupe d'applications.

Vous pouvez réduire les cases récapitulatives et les filtrer en cochant ou en décochant des cases :

- Pour afficher seulement les barres de titre récapitulatives afin de faciliter le défilement dans vos applications définies, décochez la case **Afficher les détails**.
- Pour filtrer les zones récapitulatives sur le statut de gravité à masquer, désélectionnez la case d'un compteur comme ☐ ☑ 12 . La case à cocher d'une gravité sans événements est désélectionnée. Par

exemple, dans ce graphique, les filtres pour Critique et Normal sont activés ; Avertissement et Inconnu sont désactivés car ils ont un nombre égal à 0 : .

Rechercher

Utilisez la zone Rechercher pour rechercher les entrées de journal de la dernière heure qui contiennent le texte saisi. Vous pouvez cliquer sur pour afficher les résultats d'une autre plage de temps. Le texte à rechercher est comparé aux entrées de journal associées à la sélection du navigateur et les correspondances s'affichent dans un nouvel onglet ou une nouvelle fenêtre de navigateur. Pour plus d'informations, voir «Recherche dans les fichiers journaux», à la page 1111. La fonction de recherche est fournie par IBM Operations Analytics - Log Analysis.

Actions

Le menu **Actions** comporte des options pour copier l'URL, pointant vers le journal de tableau de bord, et définir une trace pour le traitement des incidents. Pour plus d'informations, voir «Copie de l'URL du tableau de bord», à la page 1154 et «Définition d'une trace», à la page 1154.

Utilisez l'option de **journal de tableau de bord** pour passer en revue la liste des tableaux de bord d'agent mis à jour depuis le dernier redémarrage du serveur.

Lorsque le tableau de bord de base **Toutes mes applications** ou l'une des applications est sélectionné, le menu Actions inclut l'option **Rapports de lancement** pour vous aider à analyser les tendances en matière d'utilisation et de performance si les rapports Cognos sont disponibles et si votre environnement comprend Tivoli Common Reporting. Pour plus d'informations, voir «Rapports», à la page 1156.

Lorsque le groupe **Composants** est sélectionné, à partir de la section **Groupes** du navigateur ou d'une zone récapitulative, le menu **Actions** contient une option d'**édition** permettant d'éditer le tableau de bord de présentation des statuts des composants. L'option **Editer** est disponible uniquement si l'utilisateur dispose des droits de modification du tableau de bord Performance Management et des droits de création d'applications. Pour plus d'informations, voir «Edition des widgets de groupe du tableau de bord Composants», à la page 1120.

Aide

Ouvrez l'aide contextuelle pour obtenir une brève description du tableau de bord actuel, avec les liens suivants : **En savoir plus** ouvre l'intégralité de la rubrique de tableau de bord dans le système d'aide local Cloud APM ; **Visite guidée du tableau de bord** lance la visite guidée du tableau de bord d'IBM Cloud APM, qui présente une brève description des éléments du tableau de bord tout en présentant ses différentes fonctions.

Navigateur

Le navigateur affiche une hiérarchie des applications, ainsi que de leurs utilisateurs, transactions et composants, qui reflète leur organisation. Le navigateur comporte une section pour chaque niveau de la hiérarchie des applications. A chaque niveau du navigateur, les mesures du tableau de bord changent pour afficher les données du composant. Sélectionnez un élément pour basculer le contexte du tableau de bord vers la sélection. La portée de l'affichage est déterminée par vos droits utilisateur.

Chaque élément de navigateur possède un indicateur de statut critique, d'avertissement, normal ou inconnu, qui indique que l'agent n'est pas disponible. Chaque section de navigateur présente un certain nombre d'événements pour chaque gravité associée à l'élément de navigateur sélectionné. Pour en savoir plus sur le mappage des statuts aux événements de seuil, voir «Statut de l'événement», à la page 1140.

Pour libérer de l'espace pour d'autres sections, cliquez sur une barre de titre pour réduire la section et cliquez à nouveau dessus pour la restaurer. Vous pouvez également masquer entièrement le navigateur en cliquant sur sur la bordure du navigateur, le restaurer en cliquant sur , ou ajuster la largeur en faisant glisser la bordure.

Le navigateur comporte trois sections :

- La section **Applications** répertorie toutes les applications définies de vos domaines ou disposant d'une autorisation pour votre rôle utilisateur.

- Une fois que vous avez sélectionné une application, le tableau de bord affiche un récapitulatif général des statuts dans l'onglet **Présentation des statuts** et un indicateur du statut de gravité la plus élevée apparaît dans l'onglet **Evénements**. Pour plus d'informations, voir «Application - Tableau de bord d'Application Performance», à la page 1112.
- Tous les composants de votre domaine qui ont été détectés par l'infrastructure de surveillance s'affichent dans l'application prédéfinie nommée "Mes composants", qui ne peut pas être modifiée ou supprimée.
- Si vous disposez de droits administrateur, la barre d'outils **Applications** inclut des outils de gestion d'applications. Pour plus d'informations, voir «Gestion des applications», à la page 1129.

- Une fois que vous avez sélectionné une application, la section **Groupes** affiche les groupes prenant en charge l'application. Pour plus d'informations, voir «Groupe et Instance - Tableau de bord d'Application Performance», à la page 1117.
- Une fois que vous avez sélectionné un sous-groupe, la section **Instances** est renommée pour le titre de sous-groupe et renseignée avec les noms des systèmes gérés individuels. L'onglet **Présentation des statuts** change et affiche les KPI du sous-groupe sélectionné. Après que vous sélectionnez un système géré, les widgets de groupe détaillés s'affiche avec les KPI du système géré. Pour les instances de composant, vous disposez également d'un onglet **Détails de l'attribut** qui affiche un tableau des indicateurs clés de performance des attributs de l'ensemble de données de votre choix. Pour plus d'informations, voir «Affichage et gestion de graphiques et tableaux personnalisés», à la page 1123.

Si un message popup **Erreur réseau** apparaît dans le navigateur, les indicateurs de statut peuvent passer à Normal jusqu'après la restauration de la connexion. A ce moment-là, tous les événements ouverts sont traités à nouveau et le statut affiché peut être Normal jusqu'à ce que le traitement soit terminé.

Recherche dans les fichiers journaux

Pour rechercher la cause première d'un problème rencontré par des utilisateurs, tel qu'une lenteur ou une défaillance, vous pouvez effectuer une recherche dans les données de journal associées à vos applications. IBM Operations Analytics - Log Analysis fournit la fonction de recherche. Les données du journal d'application et les données de performances sont combinées pour vous aider à trouver la cause première d'un problème lié à vos applications et accélérer sa résolution.

Procédure

Effectuez les opérations suivantes pour chercher les entrées de journal qui peuvent être liées à un problème que vous examinez, par exemple, une utilisation élevée de l'unité centrale.

1. Si le Tableau de bord d'Application Performance n'est pas affiché, sélectionnez-le dans le menu **Performance**.
2. Si vous souhaitez effectuer une recherche dans une application, sélectionnez-la dans le tableau de bord "Toutes mes applications".
   Par exemple, cliquez sur "Mes composants" pour effectuer une recherche dans les journaux de toutes les ressources de composant.
3. Entrez le texte de fichier journal à rechercher dans la zone de recherche .
   Par exemple, entrez `annulé` pour rechercher les ressources Agent WebSphere Applications qui ont été restaurées au niveau précédent.
4. Si vous souhaitez rechercher des données dans une plage horaire autre que **Dernière heure**, cliquez sur et sélectionnez une période différente.
5. Cliquez sur .

Résultats
Toutes les entrées de journal contenant le texte à rechercher dans le contexte du niveau de navigateur en cours s'affichent dans un nouvel onglet ou une nouvelle fenêtre de navigateur. La fenêtre de navigateur est nommée en fonction du contexte, par exemple, application "de traitement des cartes de crédit".

Que faire ensuite
Examinez les résultats de la recherche. Vous pouvez sélectionner une autre application pour modifier les résultats de la recherche en fonction du contexte. Utilisez la zone de recherche pour affiner les résultats. Par exemple, si la zone de recherche montre `db2 AND (datasourceHostName:Pear* OR datasourceHostname:Persimmon* OR datasourceHostname:Pomegranate*)`, vous pouvez supprimer des sources de données pour limiter les résultats : `db2 AND (datasourceHostname:Persimmon*)`.

Pour plus d'informations, consultez l'ensemble de rubriques relatives à IBMOperations Analytics Log Analysis dans IBM Knowledge Center ou accédez à IBM Operations Analytics - Developers Community.

Application - Tableau de bord d'Application Performance

Après avoir sélectionné une application depuis le navigateur ou une zone récapitulative dans le tableau de bord **Toutes mes applications**, un tableau de bord à onglets présente les différentes facettes de votre application. L'onglet **Présentation des statuts** présente un récapitulatif général du statut de votre application. Les indicateurs de seuil et de statut du graphique donnent des informations générales sur la santé et les performances. Sélectionnez l'onglet **Evénements** pour identifier les seuils d'événement qui contribuent à la santé de l'application.

Pour une description du navigateur et des éléments de bannière, voir «Navigateur», à la page 1110, «Rechercher», à la page 1110, «Actions», à la page 1110 et « Aide», à la page 1110.

présentation des statuts

- Selon la composition de l'application sélectionnée, l'onglet **Présentation des statuts** présente une ou plusieurs perspectives permettant d'évaluer le statut de l'application à un niveau global :

  Disponibilité dans le temps
  IBM Website Monitoring on Cloud avant l'édition d'août 2017 : Le graphique à barres **Disponibilité dans le temps** s'affiche si l'application inclut l'Agent Synthetic Playback (dans le groupe de navigation **Transactions** et dans l'application prédéfinie, **Mes transactions**).

  Chaque point de tracé est un exemple de transaction comportant un indicateur de couleur pour un statut **Sain**, **Lent** ou **Non disponible**.

  Cliquez n'importe où sur la barre de temps pour ouvrir une fenêtre en incrustation avec les tables **Liste des transactions** et **Liste des emplacements**.

  Demandes et temps de réponse
  Le graphique à barres empilées **Demandes et temps de réponse** s'affiche si l'application inclut l'Agent de surveillance des temps de réponse (**Transactions utilisateur final** dans le groupe de navigation **Transactions**).

  Utilisez ce graphique pour examiner les motifs de tendance relatifs aux performances. Chaque barre empilée représente le pourcentage des demandes pour lesquelles le temps de réponse est correct, pour lesquelles le temps de réponse est lent, ou qui n'ont pas abouti. Le graphique à courbes représente le temps de réponse moyen au cours de la période de cinq minutes. Utilisez le sélecteur de durée pour modifier l'intervalle affiché, comme décrit dans «Ajustement et comparaison de mesures dans le temps», à la page 1121.

  Agréger une topologie de transaction
  Agréger une topologie de transaction s'affiche si le suivi de transaction est activé et si l'application comprend l'un des agents ou collecteurs de données suivants :

  – agent DataPower

- agent HTTP Server
- agent IBM Integration Bus
- collecteur de données J2SE
- agent JBoss
- collecteur de données Liberty
- agent Microsoft .NET
- agent Microsoft SQL Server
- collecteur de données Node.js
- Agent de surveillance des temps de réponse
- Agent SAP NetWeaver Java Stack
- Agent Tomcat
- Agent WebLogic (Linux et Windows uniquement)
- Agent WebSphere Applications
- agent WebSphere MQ

Vous devez activer manuellement le suivi de transaction pour tous les agents sauf pour l'Agent de surveillance des temps de réponse. Le suivi des transactions est activé automatiquement pour les collecteurs de données. Pour plus d'informations, voir «Page Configuration d'agent», à la page 187.

Le widget **Agréger une topologie de transaction** présente les ressources qui sont associées à l'application et leurs relations. Le pied de page indique le nombre des noeuds, ressources et relations sélectionnés, tous les filtres de la topologie ainsi que l'heure de la dernière régénération des données.

Si un composant d'application est ajouté à une application métier et que le composant transporte le trafic pour plusieurs applications, la topologie d'application qui s'affiche pour ces applications métier comprend les chemins vers les noeuds pour toutes les applications.

Pour la Liste d'applications Java IBM où JavaScript est automatiquement injecté, le niveau de noeud le plus élevé représente le navigateur et le noeud le plus granulaire correspond à la base de données. Concernant les autres applications, le niveau de noeud le plus élevé représente l'application, alors que le noeud le plus granulaire correspond à l'instance du système géré.

Chaque noeud comporte un indicateur de statut et une mise en évidence d'arrière-plan qui montrent la gravité de statut la plus élevée à ce niveau d'agrégation. Si vous réduisez le navigateur afin de libérer de l'espace, vous pouvez continuer de voir le même statut dans le widget **Agréger une topologie de transaction**. L'environnement source du noeud se présente comme suit **Cloud** (IBM Cloud Application Performance Management), **ITM** (IBM Tivoli Monitoring), **Sur site** (IBM Cloud Application Performance Management, Private) , **Private Cloud** (IBM Cloud Private), or **Public Cloud** (IBM Cloud). Aucune icône n'apparaît pour **Autre** (la ressource gérée provient d'un autre environnement).

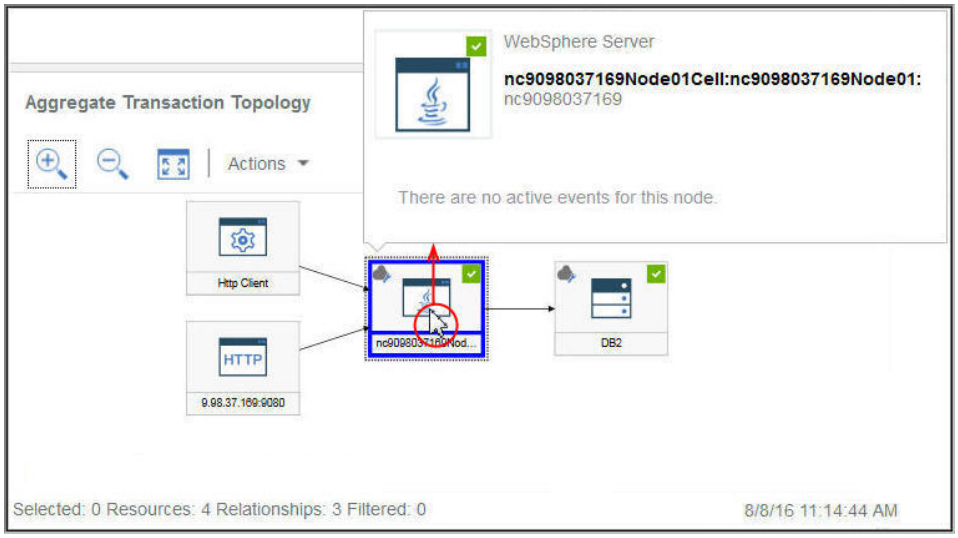
Faites passer la souris sur un noeud, ouvrez le menu de raccourci et sélectionnez des noeuds pour obtenir davantage d'informations sur le statut et ainsi identifier plus facilement la cause première d'un problème :

- Lorsque vous faites passer votre souris sur un noeud, un message en incrustation fournit une liste des événements critiques et d'avertissement.
- Cliquez deux fois sur une URL de lien dans un nœud afin d'ouvrir le tableau de bord correspondant qui présente les détails de composant ou de transaction.
- Cliquez avec le bouton droit de la souris sur un noeud et sélectionnez l'une des options d'analyse détaillée du tableau de bord : **Accéder à la page Récapitulatif des transactions** du noeud de sous-groupe sélectionné ; **Accéder à la page Instance de composant** du noeud d'instance ; ou **Propriétés** pour afficher le nom de la ressource, le statut, le nom du système géré et le domaine du fournisseur (tel que "Cloud").

Utilisez les icônes de la barre d'outils pour ajuster l'affichage et suivez la procédure décrite dans «Manipulation du widget Agréger une topologie de transaction», à la page 1116.

Cliquez sur l'outil pour basculer entre cette vue et **Statut courant des composants**, décrit ci-après.

Les agents de surveillance sans information de topologie ne s'affichent pas dans le widget Agréger une topologie de transaction.



Statut des composants en cours

Le graphique à barres empilées de **statut de composant en cours** indique le pourcentage et le nombre de statuts Critique, Avertissement, Normal et Inconnu pour chaque type de composant de l'application. Par exemple, cinq systèmes Linux prennent en charge l'application sélectionnée. Des barres empilées indiquant 40 % pour le statut Critique et 60 % pour le statut Normal signifient que deux systèmes ont le statut Critique et trois systèmes, le statut Normal.

Placez le pointeur de la souris sur une barre pour lire le statut dans une fenêtre en incrustation : le pourcentage et le nombre d'instances de composant possédant ce statut. Les domaines dans lesquels se trouvent les instances sont également affichés avec un statut pour chaque domaine : IBM Cloud, Cloud, Sur site, ITM et Autre. Par exemple, deux de vos cinq systèmes Linux se trouvent dans le domaine ITM et trois dans le domaine Cloud. Si l'un des systèmes critiques se trouve dans le domaine ITM et que l'autre se trouve dans le domaine Cloud, lorsque vous déplacez la souris sur le segment de la barre critique (40 %), la fenêtre en incrustation du statut affiche un système dans le domaine ITM et l'autre système dans le domaine Cloud.

Vous pouvez cliquer sur une barre pour ouvrir le tableau de bord récapitulatif de statut pour le type de composant, avec un widget de groupe pour chaque système surveillé.

Cliquez sur l'outil pour basculer entre cette vue et le widget **Agréger une topologie de transaction** décrite plus haut.

Availability Monitoring

Lorsque l'application définie est constituée uniquement de Availability Monitoring, le tableau de bord récapitulatif s'affiche comme indiqué dans «Accès à Availability Monitoring», à la page 1077.

- Une fois que vous avez sélectionné un sous-groupe de la section **Groupes**, la section **Instances** est renommée pour le titre de sous-groupe et elle est renseignée avec les noms des instances individuelles. Pour plus d'informations sur les tableaux de bord au niveau du groupe, du sous-groupe et de l'instance du navigateur, ainsi que sur l'onglet **Détails d'attribut** qui s'affiche après la sélection d'un système géré, voir «Groupe et Instance - Tableau de bord d'Application Performance», à la page 1117 et «Affichage et gestion de graphiques et tableaux personnalisés», à la page 1123.
- Certains widgets de tableau de bord montrent des mesures basées sur un intervalle, et d'autres montrent les mesures les plus récentes. Si une barre de sélection de durée s'affiche, vous pouvez ajuster l'intervalle pour le tableau de bord afin d'affecter tous les graphiques ou tableaux dont les

valeurs sont dérivées de données historiques. Pour plus d'informations, voir «Ajustement et comparaison de mesures dans le temps», à la page 1121.
Tout en visualisant les graphiques, vous pouvez cliquer sur un point de tracé pour ouvrir une infobulle indiquant la valeur du point de tracé et d'autres informations pertinentes. Lorsque vous avez fini d'afficher un graphique à courbes dans le navigateur Internet Explorer version 11, vous pouvez continuer de voir l'infobulle pendant que vous déplacez le curseur autour de la fenêtre. Si vous rencontrez ce comportement, vous pouvez fermer l'infobulle en cliquant plusieurs fois dans le graphique.

- Les données sont actualisées automatiquement toutes les minutes dans la console. Cette activité est essentielle et ne peut pas être interrompue, arrêtée ni masquée.
- Si aucune donnée n'est disponible pour un graphique ou une zone récapitulative de statut, un message d'information s'affiche.

Evénements

- Les indicateurs de statut qui s'affichent en regard du titre d'onglet **Evénements**, tels que **14** **3**, indiquent le nombre de gravités d'événement les plus élevées pour l'élément de navigateur sélectionné : application, groupe, sous-groupe ou instance. Les gravités des seuils sont consolidées, comme illustré dans le tableau suivant. Par exemple, **Evénements** signifie que l'événement ayant la gravité maximale est mineur ou correspond à un avertissement.

Onglet Evénements	Gravité de seuil
Critique	Fatal et Critique
Avertissement	Mineur et Avertissement
Normal	Inconnu

  Lorsque votre environnement géré inclut IBM Operations Analytics - Predictive Insights et qu'une anomalie est détectée, un événement est ouvert. Une icône en forme de diamant recouvre l'indicateur de statut, par exemple, , pour vous informer qu'au moins une anomalie a été détectée par Operations Analytics - Predictive Insights. Par exemple, **Evénements** , indique que l'événement de statut le plus élevé est Avertissement, et qu'au moins un événement d'anomalie est ouvert.
- Cliquez sur l'onglet **Evénements** pour afficher le récapitulatif du nombre total d'événements, le nombre d'événements pour chaque type de gravité et une jauge en pourcentage des gravités. Pour plus d'informations, voir «Statut de l'événement», à la page 1140.

Vues personnalisées

Les pages que vous créez et que vous enregistrez sont associées à l'application sélectionnée. Par exemple, l'application Inventory Management dans Cloud APM Démonstration guidée possède les agents de surveillance suivants : Linux OS, MySQL, Node.js, Hadoop et Ruby. Vous pouvez créer et enregistrer une page personnalisée à n'importe quel niveau du navigateur allant de l'application à l'instance, puis l'ouvrir au niveau où elle a été créée. Une page créée à un niveau particulier ne peut être ouverte qu'au même niveau. Les métriques disponibles pour les widgets peuvent être des ressources, quelles qu'elles soient, de l'application. A l'aide de l'exemple Inventory Management, vous pouvez créer une page avec une table à partir de l'Agent Ruby, un graphique à partir de l'Linux OS, etc.

- L'onglet **Vues personnalisées** est disponible à n'importe quel niveau du navigateur lorsque vous sélectionnez une application dans **Toutes mes applications**.
- Une fois que vous avez ouvert l'onglet **Vues personnalisées**, la fenêtre de **sélection d'un modèle pour votre page personnalisée** est affichée ou la page par défaut est affichée si elle est déjà définie.
  - Dans la fenêtre de **sélection d'un modèle pour votre page personnalisée**, vous pouvez sélectionner un modèle pour créer une page.
  - Dans la page par défaut, vous pouvez cliquer sur pour créer une page.

- Dans la page par défaut, cliquez sur dans la liste des pages et sélectionnez l'une des pages sauvegardées de la liste.
- Les options disponibles dans l'onglet Vues personnalisées varient selon que la page soit éditée ou consultée. Pour plus d'informations sur l'édition d'une page, voir «Création et gestion de pages personnalisées», à la page 1144. Pour plus d'informations sur l'affichage d'une page, voir «Affichage de pages personnalisées», à la page 1151.

Manipulation du widget Agréger une topologie de transaction

Utilisez le widget **Agréger une topologie de transaction** pour afficher la hiérarchie des ressources dans l'application sélectionnée. Vous pouvez ajuster et déplacer l'affichage pour voir le statut de chaque composant et sa relation avec les autres composants, et ouvrir le tableau de bord correspondant.

Avant de commencer

Une fois que vous avez sélectionné une application dans le Tableau de bord d'Application Performance, l'onglet **Présentation des statuts** s'affiche avec un ou plusieurs graphiques, en fonction des ressources surveillées incluses dans l'application.

Le widget **Agréger une topologie de transaction** s'affiche pour les agents suivants qui prennent en charge le suivi des transactions :

- agent DataPower
- agent HTTP Server
- agent IBM Integration Bus
- collecteur de données J2SE
- agent JBoss
- collecteur de données Liberty
- agent Microsoft .NET
- agent Microsoft SQL Server
- collecteur de données Node.js
- Agent de surveillance des temps de réponse
- Agent SAP NetWeaver Java Stack
- Agent Tomcat
- Agent WebLogic (Linux et Windows uniquement)
- Agent WebSphere Applications
- agent WebSphere MQ

Agréger une topologie de transaction affiche un objet de noeud pour chaque ressource surveillée qui prend en charge la fonction de topologie.

Procédure

Effectuez l'une des étapes suivantes pour manipuler le widget **Agréger une topologie de transaction** et ouvrir des tableaux de bord qui sont associés aux noeuds :

- Pour ouvrir un tableau de bord lié, cliquez deux fois sur le noeud de topologie. Vous pouvez également cliquer avec le bouton droit de la souris sur un noeud et sélectionner l'une des options d'analyse détaillée du tableau de bord, **accéder à la page Récapitulatif des transactions**, **accéder à la page Instance de composant** ou sélectionner **Propriétés** pour afficher les informations relatives au système géré.
- Pour agrandir la taille d'affichage de la topologie, cliquez sur **Zoom avant**. Vous pouvez également cliquer sur **Actions** > **Zoom avant** si aucun noeud n'est sélectionné.

- Pour réduire la taille d'affichage de la topologie, cliquez sur **Zoom arrière**. Vous pouvez également cliquer sur **Actions** > **Zoom arrière** si aucun noeud n'est sélectionné.
- Pour ajuster la taille d'affichage de la topologie afin de l'adapter à l'espace de widget en cours, cliquez sur **Ajuster au contenu**. Vous pouvez également cliquer sur **Actions** > **Ajuster au contenu** si aucun noeud n'est sélectionné.
- Pour filtrer les noeuds de la topologie, sélectionnez l'un des indicateurs dans la barre de filtre. Vous pouvez activer et désactiver les filtres et sélectionner plusieurs filtres. Tous les noeuds comportant une propriété ne correspondant pas au filtre apparaissent en grisé, tandis que ceux correspondant au filtre restent visibles.
  - Normal, Avertissement, Critique ou Inconnu pour filtrer par statut de noeud.
  - Pour filtrer en fonction de l'environnement, sélectionnez **Cloud** (IBM Cloud Application Performance Management), **ITM** (IBM Tivoli Monitoring), **Sur site** (IBM Cloud Application Performance Management, Private) , **Private Cloud** (IBM Cloud Private), or **Public Cloud** (IBM Cloud).
  - Filtrer pour ajouter un filtre personnalisé.
- Pour libérer de l'espace pour le widget de topologie, cliquez sur la **Réduire la section** du navigateur ou sur les widgets de graphique environnants ou faites glisser une bordure du widget.

Groupe et Instance - Tableau de bord d'Application Performance

Utilisez le tableau de bord du groupe, du sous-groupe ou de l'instance de l'application sélectionnée pour obtenir un statut de haut niveau de vos systèmes gérés. Vous pouvez accéder jusqu'au niveau des tableaux de bord détaillés comportant des mesures associées à l'instance sélectionnée et créer des graphiques et des tableaux personnalisés.

Une fois que vous avez sélectionné une application sous **Toutes mes applications** dans le Tableau de bord d'Application Performance, les onglets **Présentation des statuts** et **Evénements** s'affichent.

La section **Groupes** du navigateur affiche un ou plusieurs groupes possibles, selon les éléments de l'application définie.

Pour une description du navigateur et des éléments de bannière, voir «Navigateur», à la page 1110, «Rechercher», à la page 1110, «Actions», à la page 1110 et « Aide», à la page 1110.

présentation des statuts

Groupes et sous-groupes

- Sélectionnez un groupe ou développez un groupe et sélectionnez un sous-groupe pour faire apparaître un widget de groupe récapitulatif pour chaque système géré dans l'application. Lorsqu'un sous-groupe est sélectionné, les widgets de groupe récapitulatif dans l'onglet **Présentation des statuts** sont propres à ce sous-groupe.
- Les groupes prédéfinis disponibles sont les suivants, selon les produits de surveillance installés :

  Availability Monitoring
  Ce groupe est affiché pour les applications personnalisées. Le comportement de navigation d'Availability Monitoring est différent des groupes **Composants** et **Transactions**.

  Les tableaux de bord et le module complémentaire d'Availability Monitoring sont décrits dans la rubrique «Availability Monitoring», à la page 1076.

  Composants
  Ce groupe s'affiche pour toutes les applications, à l'exception de l'Agent de surveillance des temps de réponse, de l'Agent Synthetic Playback et d'Availability Monitoring.

Le groupe **Composants** comporte un sous-groupe pour chaque composant logiciel surveillé qui prend en charge l'application sélectionnée.

Transactions
Ce groupe inclut **Transactions utilisateur final**et **Transactions synthétiques** (IBM Website Monitoring on Cloud avant l'édition d'août 2017). Pour plus d'informations, voir l'aide de la surveillance des transactions et de l'Agent Synthetic Playback ou leurs PDF de référence sur l'APM Developer Center sous Agent metrics/Reference PDFs.

- Une fois que vous avez sélectionné **Composants** ou un sous-groupe de la section **Groupes**, l'onglet **Présentation des statuts** change et affiche un tableau de bord récapitulatif avec un widget de groupe pour chaque ressource gérée. L'environnement source s'affiche sous forme de **Cloud** (IBM Cloud Application Performance Management), **ITM** (IBM Tivoli Monitoring), **Sur site** (IBM Cloud Application Performance Management, Private) , **Private Cloud** (IBM Cloud Private), or **Public Cloud** (IBM Cloud). La section **Instances** est renommée pour le titre de sous-groupe et elle est renseignée avec les noms des différentes instances.

Si l'application compte de nombreuses instances de système géré, de nombreux widgets de groupe sont affichés. Vous pouvez parcourir la liste pour les afficher tous. Vous pouvez également sélectionner un type de système géré de la liste de sous-groupes de composants, tels que le système d'exploitation Windows, pour confiner l'affichage aux mêmes types de système géré. Vous pouvez également filtrer les instances de système géré.

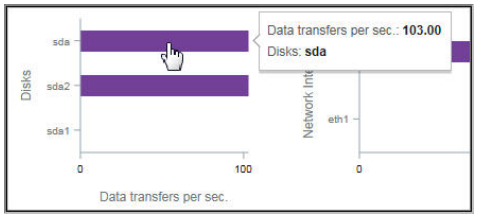
Navigateur Firefox seulement : selon le nombre d'agents et la bande passante, à mesure que vous descendez dans la page Composants, un message en incrustation vous avertira sans doute que le script de chargement de la page de ressource prend un certain temps pour se terminer. Sélectionnez l'option "Don't ask me again" pour désactiver le message et continuer à ouvrir les widgets. Vous pouvez également entrer `about:config` dans la zone d'adresse, rechercher **`dom.max_script_run_time`** et accroître la valeur de délai (en secondes). La valeur zéro (0) désactive le délai d'attente.

Instances

- Cliquez dans un widget de groupe ou sélectionnez le nom de l'instance dans le navigateur afin d'ouvrir un tableau de bord détaillé de la ressource gérée.
- Si plusieurs instances s'affichent dans le navigateur, utilisez la zone de recherche dans la barre d'outils Instances. A mesure de la frappe dans cette zone, toute instance qui ne concorde pas est supprimée de l'affichage.
- Pour mettre en pause l'actualisation automatique du Tableau de bord d'Application Performance, cliquez sur **Pause** dans la barre d'outils Instances ; pour reprendre l'actualisation automatique, cliquez sur **Reprise**.
- Les widgets et indicateurs clés de performance qui s'affichent pour un système géré peuvent dépendre de la version de l'agent. Si un agent est installé sur le système géré à un niveau de version antérieur, il se peut qu'il ne puisse pas fournir autant d'informations que la version actuelle de l'agent. Un message s'affiche à la place d'un ou plusieurs indicateurs clés de performance dans un graphique ou un tableau lorsqu'aucune donnée n'est disponible. Cela peut simplement être dû au

fait qu'aucune donnée n'a été signalée pour l'intervalle de temps. Sinon, cette situation peut être liée au fait qu'un agent de niveau antérieur qui ne prend pas en charge l'ensemble de données ou un attribut est inclus dans le graphique ou le tableau.
Pour obtenir la liste des tableaux de bord d'agent mis à jour depuis le dernier redémarrage du serveur Cloud APM, sélectionnez **Actions** > **Journal de tableau de bord**.

- Certains widgets de tableau de bord montrent des mesures basées sur un intervalle, et d'autres montrent les mesures les plus récentes. Si une barre de sélection de durée s'affiche, vous pouvez ajuster l'intervalle pour le tableau de bord afin d'affecter tous les graphiques ou tableaux dont les valeurs sont dérivées de données historiques. Pour plus d'informations, voir «Ajustement et comparaison de mesures dans le temps», à la page 1121.
  Tout en visualisant les graphiques, vous pouvez cliquer sur un point de tracé pour ouvrir une infobulle indiquant la valeur du point de tracé et d'autres informations pertinentes. Lorsque vous avez fini d'afficher un graphique à courbes dans le navigateur Internet Explorer version 11, vous pouvez continuer de voir l'infobulle pendant que vous déplacez le curseur autour de la fenêtre. Si vous rencontrez ce comportement, vous pouvez fermer l'infobulle en cliquant plusieurs fois dans le graphique.
- Si vous consultez un graphique dont certaines barres sont manquantes, cela signifie que la valeur de ce point de données correspond à 0 (zéro).



- Les utilisateurs d'IBM Cloud Application Performance Management, Advanced disposent de tableaux de bord de diagnostic supplémentaires auxquels vous pouvez accéder en cliquant sur le lien **Diagnostiquer** à partir d'un widget de groupe dans le tableau de bord Détails.

  Restriction : Le système géré pour lequel vous ouvrez les tableaux de bord de diagnostic doit résider dans le domaine IBM Cloud APM. Si le système géré réside dans le domaine source IBM Cloud ou IBM Tivoli Monitoring, les tableaux de bord de diagnostic ne sont pas disponibles. Voir aussi «Coexistence de l'agent Cloud APM et de l'agent Tivoli Monitoring», à la page 976.
- Si votre environnement inclut l'Agent Synthetic Playback, vous pouvez lancer les rapports Cloud APM pour l'instance d'agent à partir du menu **Actions**.

Evénements

- Les indicateurs de statut qui s'affichent en regard du titre d'onglet **Evénements**, tels que **14** **3**, indiquent le nombre de gravités d'événement les plus élevées pour l'élément de navigateur sélectionné : application, groupe, sous-groupe ou instance. Les gravités des seuils sont consolidées, comme illustré dans le tableau suivant. Par exemple, **Evénements** signifie que l'événement ayant la gravité maximale est mineur ou correspond à un avertissement.

Onglet Evénements	Gravité de seuil
Critique	Fatal et Critique
Avertissement	Mineur et Avertissement
Normal	Inconnu

Lorsque votre environnement géré inclut IBM Operations Analytics - Predictive Insights et qu'une anomalie est détectée, un événement est ouvert. Une icône en forme de diamant recouvre l'indicateur de statut, par exemple, , pour vous informer qu'au moins une anomalie a été détectée par Operations Analytics - Predictive Insights. Par exemple, **Evénements** , indique que l'événement de statut le plus élevé est Avertissement, et qu'au moins un événement d'anomalie est ouvert.

- Cliquez sur l'onglet **Evénements** pour afficher le récapitulatif du nombre total d'événements, le nombre d'événements pour chaque type de gravité et une jauge en pourcentage des gravités. Pour plus d'informations, voir «Statut de l'événement», à la page 1140.

Vues personnalisées

Les pages que vous créez et que vous enregistrez sont associées à l'application sélectionnée. Par exemple, l'application Inventory Management dans Cloud APM Démonstration guidée possède les agents de surveillance suivants : Linux OS, MySQL, Node.js, Hadoop et Ruby. Vous pouvez créer et enregistrer une page personnalisée à n'importe quel niveau du navigateur allant de l'application à l'instance, puis l'ouvrir au niveau où elle a été créée. Une page créée à un niveau particulier ne peut être ouverte qu'au même niveau. Les métriques disponibles pour les widgets peuvent être des ressources, quelles qu'elles soient, de l'application. A l'aide de l'exemple Inventory Management, vous pouvez créer une page avec une table à partir de l'Agent Ruby, un graphique à partir de l'Linux OS, etc.

- L'onglet **Vues personnalisées** est disponible à n'importe quel niveau du navigateur lorsque vous sélectionnez une application dans **Toutes mes applications**.
- Une fois que vous avez ouvert l'onglet **Vues personnalisées**, la fenêtre de **sélection d'un modèle pour votre page personnalisée** est affichée ou la page par défaut est affichée si elle est déjà définie.
  - Dans la fenêtre de **sélection d'un modèle pour votre page personnalisée**, vous pouvez sélectionner un modèle pour créer une page.
  - Dans la page par défaut, vous pouvez cliquer sur  pour créer une page.
- Dans la page par défaut, cliquez sur dans la liste des pages et sélectionnez l'une des pages sauvegardées de la liste.
- Les options disponibles dans l'onglet Vues personnalisées varient selon que la page soit éditée ou consultée. Pour plus d'informations sur l'édition d'une page, voir «Création et gestion de pages personnalisées», à la page 1144. Pour plus d'informations sur l'affichage d'une page, voir «Affichage de pages personnalisées», à la page 1151.

Détails d'attribut

- L'onglet **Détails d'attribut** s'affiche après que vous avez sélectionné une instance de composant dans la section **Instances** du navigateur (renommée avec le nom du sous-groupe sélectionné) ou si vous cliquez dans un widget de groupe récapitulatif.
- Si des pages de graphique ou de tableau ont été enregistrées pour l'agent, la page récemment ouverte est affichée avec des valeurs de l'instance de composant sélectionnée. Cliquez sur le titre pour sélectionner une autre page à partir de **Mes pages**  ou **Pages partagées** .
- Vous pouvez modifier le graphique ou le tableau et cliquer sur **Prévisualiser les résultats** pour afficher le graphique ou le tableau avec les attributs sélectionnés. Pour plus d'options, voir «Création d'une page de graphiques ou de tableaux personnalisés», à la page 1123.

Edition des widgets de groupe du tableau de bord Composants

Vous pouvez éditer les valeurs de seuil des widgets de groupe qui s'affichent dans le tableau de bord **Composants** (sélectionné dans la section **Groupes** du navigateur). Vous pouvez également contrôler l'affichage et la position des widgets de groupe, et décider s'il convient d'inclure un seuil de widget dans la détermination du statut de composant.

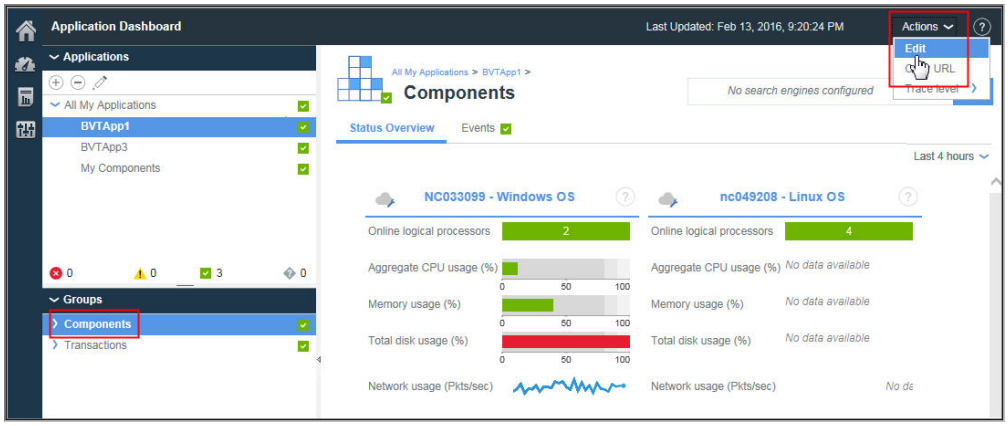
Pourquoi et quand exécuter cette tâche

Cette tâche implique l'édition du tableau de bord du groupe Composants et de son widget de groupe récapitulatif pour une application définie. L'éditeur du groupe Composants n'est pas disponible pour l'application prédéfinie **Mes composants**. Pour plus d'informations sur les applications définies, voir «Gestion des applications», à la page 1129.

Votre ID utilisateur doit également disposer de l'autorisation de modification du Tableau de bord d'Application Performance et de l'autorisation de création d'applications. Pour plus d'informations, voir «Rôles et droits», à la page 1031.

Procédure

1. Après avoir ouvert le Tableau de bord d'Application Performance à partir du menu **Performance**, sélectionnez l'application dont vous souhaitez éditer les widgets de groupe récapitulatif dans le tableau de bord **Toutes mes applications**.
2. Dans la section **Groupes** du navigateur, cliquez sur **Composants** afin d'ouvrir un tableau de bord présentant les widgets de groupe pour tous les composants de l'application.
3. Cliquez sur **Actions** > **Editer** pour ouvrir l'éditeur des widgets de groupe dans le groupe **Composants**.
   L'option **Editer** ne s'affiche que lorsque le tableau de bord **Composants** est ouvert.



4. Apportez l'une des modifications suivantes aux widgets de groupe :
   - Pour supprimer un widget de groupe de la vue, cliquez sur .
   - Pour modifier les seuils récapitulatifs d'un widget, cliquez sur **Paramètres**, sélectionnez l'onglet **Seuils** et modifiez les valeurs du niveau de gravité critique, avertissement ou normal. Après avoir modifié les seuils pour le widget de groupe, cliquez sur **Terminé**.
   - Pour ajouter un widget, cliquez sur , cliquez sur les icônes des applications jusqu'à ce que celle de votre choix s'affiche, cliquez dans le widget de groupe pour le sélectionner, puis cliquez sur **Ajouter**.
   - Pour redimensionner un widget, faites glisser l'icône de poignée . Le redimensionnement d'un widget ne modifie pas la taille du texte qu'il contient, ni sa hauteur.
   - Pour déplacer un widget, faites-le glisser vers sa nouvelle position.
5. Pour enregistrer vos modifications et fermer l'éditeur, cliquez sur **Sauvegarder**, ou cliquez sur **Annuler** pour supprimer vos modifications.

Résultats

Le tableau de bord **Composants** de l'application sélectionnée s'affiche avec les nouveaux paramètres.

Que faire ensuite

Pour plus d'informations sur le tableau de bord lorsqu'un groupe ou sous-groupe est sélectionné dans le navigateur, voir «Groupe et Instance - Tableau de bord d'Application Performance», à la page 1117 ; pour plus d'informations sur le tableau de bord de composant surveillé, cliquez sur le bouton dans la bannière **Tableau de bord des applications**.

Ajustement et comparaison de mesures dans le temps

Certains graphiques de tableau de bord montrent des mesures basées sur un intervalle et d'autres montrent uniquement les mesures les plus récentes. Si une barre de sélection de durée est affichée dans

l'onglet **Présentation des statuts** d'une instance de système géré, vous pouvez ajuster la période des graphiques dont les valeurs sont dérivées des échantillons de données historiques. Pour les attributs dont les données ont été collectées pour plusieurs jours et présentées dans un graphique à courbes, vous pouvez comparer les valeurs du jour à celles d'un jour précédent.

Avant de commencer

Si vous effectuez une comparaison avec un intervalle horaire d'un jour précédent, la date jusqu'à laquelle vous pouvez remonter dépend du nombre de jours que le serveur Cloud APM a sauvegardés et du type de données affichées sur la page. . Pour les abonnés ayant acheté une licence Cloud APM, les échantillons de données sont stockés pendant 8 jours pour la plupart des jeux de données de surveillance des ressources. Le nombre exact est publié dans l'aide sur les attributs de l'agent ou du collecteur de données, ainsi que dans le PDF de référence (voir Chapitre 2, «Documentation au format PDF», à la page 43). Pour les abonnés ayant téléchargé une version d'essai de Cloud APM, les échantillons de données de surveillance des ressources sont stockés pendant 2 jours. Les données de suivi des transactions de l'Agent de surveillance des temps de réponse ou des agents middleware concernent uniquement les dernières 24 heures (ou dans certains cas les 4 dernières heures) et leur durée de conservation ne peut pas être modifiée.

Procédure

Pour ajuster l'intervalle horaire affiché dans le graphique à courbes pour une instance de ressource gérée ou comparer les valeurs au même intervalle horaire d'un jour précédent, procédez comme suit :

1. Si le Tableau de bord d'Application Performance n'est pas affiché, sélectionnez-le dans le menu **Performance**.
2. Accédez à la page de tableau de bord d'une instance qui présente les graphiques à courbes historiques et cliquez sur le sélecteur de durée **4 dernières heures**.
3. Sélectionnez une ou plusieurs des options suivantes :
   - Pour modifier l'intervalle affiché, sélectionnez **4 dernières heures**, **12 dernières heures** ou **Dernier jour**.
   - Pour comparer l'intervalle affiché dans un graphique à courbes avec les mesures d'un autre jour, sélectionnez **Comparer à** et sélectionnez un jour antérieur, jusqu' au nombre de jours indiqués comme disponibles dans le calendrier en incrustation (les dates non disponibles sont barrées).
   - Pour que l'intervalle s'applique à tous les tableaux de bord de toutes les applications définies dans votre environnement surveillé, sélectionnez **Toutes les applications**. Sinon, laissez le paramètre défini sur **Uniquement cette application** pour appliquer l'intervalle uniquement à l'application en cours (par exemple "Mes composants"). La sélection **Comparer à** n'est effective que pour la page en cours.

Résultats

- Si vous visualisez des données historiques sans comparaison, tous les tableaux de bord de l'application en cours (ou de toutes les applications) sont affectés par la modification.
- Si vous visualisez une comparaison, seuls les graphiques à courbes de la page en cours sont affectés. Une ligne est tracée pour chaque indicateur clé de performance afin de présenter les mesures du jour choisi. Certains graphiques à courbes sont indisponibles pour la comparaison, comme indiqué par une cote d'alerte sur le graphique : "Aucune comparaison disponible". Cela peut se produire avec les ressources gérées les plus récentes n'ayant pas encore collectées de données pour la date spécifiée. Essayez de sélectionner une date plus récente pour la comparaison.
- Les widgets pour lesquels les données d'historique ne sont pas collectées continuent d'afficher les valeurs les plus récentes.
- Les points de données sont répartis sur toute la longueur du graphique pour l'intervalle sélectionné. Les horodatages sont affichés sur l'étiquette d'axe, des plus anciens aux plus récents. Vérifiez l'échantillon de données le plus ancien pour confirmer si les données d'historique sont affichées partiellement ou en totalité.

- Les données envoyées aux graphiques et aux tableaux sont normalisées au temps moyen de Greenwich. L'axe **Horodatage** imprime les horodatages en fonction du fuseau horaire de votre navigateur. Si votre horodatage utilise l'heure d'été, l'horodatage affiché pendant l'heure de transition est décalé d'une heure. Imaginez par exemple que vous affichez un graphique à courbes en Espagne et qu'à 2h00, il est désormais 3h00 suite au passage à l'heure d'été. En raison de la différence entre l'heure des données au temps moyen de Greenwich et l'heure locale de l'horodatage, celui-ci comporte un écart d'une heure entre 2h00 et 3h00. Si vous affichez le même graphique en Nouvelle-Zélande lors du passage de l'heure d'été (3h00) à l'heure d'hiver (2h00), les horodatages de 2h00 à 3h00 sont répétés.

Affichage et gestion de graphiques et tableaux personnalisés

Le Tableau de bord d'Application Performance fournit des tableaux de bord prédéfinis des indicateurs clés de performance de votre système géré. Lorsque vous visualisez le tableau de bord d'une instance de composant, utilisez l'onglet **Détails d'attribut** pour afficher des pages de graphiques ou de tableaux sauvegardées et créer et gérer d'autres pages.

Par exemple, vous observez un indicateur critique dans le tableau de bord récapitulatif. Vous accédez alors au niveau de l'instance dans laquelle cette condition a été constatée. A cet emplacement, vous ajoutez un graphique illustrant le débit de l'unité centrale occupée pour observer les événements sur une période donnée. Vous pouvez afficher des détails sur tout attribut disponible de l'instance de composant sélectionnée et sauvegarder le graphique ou le tableau personnalisé avec l'agent et l'afficher chaque fois que vous ouvrez une instance de système géré.

Un sous-ensemble des attributs et des ensembles de données de l'agent est disponible pour l'utilisation dans les tables et les graphiques personnalisés. Ces attributs sont les plus utiles pour l'affichage dans les tableaux de bord. L'ensemble complet des attributs peut être utilisé dans les seuils personnalisés (voir «Gestionnaire de seuils», à la page 1014).

Pour améliorer les performances et réduire la redondance, les agents restreignent le nombre de lignes affichées pour certains ensembles de données dans les détails d'attribut. Les descriptions des ensembles de données dans l'aide et le fichier PDF de l'agent indiquent si l'échantillon de données par défaut limite le nombre de lignes envoyées au serveur Cloud APM.

Pour les utilisateurs malvoyants, la possibilité de créer des tables historiques fournit une alternative aux graphiques à courbes que les technologies d'assistance aux personnes handicapées, telles les logiciels de lecteur d'écran, ne peuvent pas interpréter. L'onglet **Détails d'attribut**, disponible pour les instances de transaction de l'Agent de surveillance des temps de réponse et de l'Agent Synthetic Playback, vous permet ainsi de créer des tables historiques. Pour plus d'informations, voir «Exemple de création d'une table personnalisée avec les commandes du clavier», à la page 1126.

Création d'une page de graphiques ou de tableaux personnalisés

Lorsque vous visualisez le Tableau de bord d'Application Performance d'une instance de composant, vous pouvez sélectionner l'onglet **Détails d'attribut** pour afficher des pages de graphiques ou de tableaux enregistrées, ainsi que pour créer et gérer d'autres pages.

Pourquoi et quand exécuter cette tâche

Lorsque vous êtes dans la page d'accueil du Tableau de bord d'Application Performance et que vous descendez dans la hiérarchie jusqu'à une instance de votre ressource gérée, l'onglet **Détails d'attribut** est ajouté aux onglets **Présentation des statuts** et **Evénements** sur la page du tableau de bord.

Ces instructions concernent la création de graphiques et de tableaux personnalisés pour les instances de composant. Vous pouvez suivre les étapes relatives aux instances de transaction de l'Agent de surveillance des temps de réponse et de l'Agent Synthetic Playback, avec les limitations suivantes : tables historiques uniquement (pas de graphiques) ; impossibilité de filtrer la liste des **fichiers** ou des **attributs** ; sélection de tous les attributs (vous ne pouvez ni sélectionner, ni désélectionner des attributs individuels) ; impossibilité de sauvegarder la page ; indisponibilité de l'option **Précédent** dans le sélecteur de temps pour l'Agent Synthetic Playback.

Procédure

Pour créer un graphique ou un tableau à partir d'un fichier disponible pour l'instance de composant surveillée, procédez comme suit :

1. Après avoir ouvert le Tableau de bord d'Application Performance à partir du menu **Performance**, accédez au niveau d'une instance de la ressource gérée.

   Le système sélectionné est mis en évidence dans la section **Instances** du navigateur, avec un nom basé sur le type de composant, par exemple **Ruby App**.
2. Cliquez sur l'onglet **Détails d'attribut**.

   Si aucune page de graphiques ou de tableaux n'a été enregistrée pour ce type d'agent de surveillance, le **tableau** **Temps réel** est sélectionné. Temps réel est approprié pour les ensembles de données qui renvoient plusieurs lignes et n'est disponible que pour les tableaux.
3. Si une page de graphiques ou de tableaux enregistrée est affichée, cliquez sur **Nouveau**.
4. Entrez un nom pour la page de graphiques ou de tableaux dans la zone de titre.

   N'utilisez aucun des caractères suivants dans le titre : ! " % & ' * ? < > } { \.
5. Si vous préférez afficher des échantillons de données au fil du temps, modifiez le type pour **Historique**.

   L'option **Graphique** est activée.
6. Si vous avez sélectionné **Historique** et que vous préférez obtenir un graphique plutôt qu'un tableau, cliquez sur **Graphique**.
7. Depuis la liste **Ensemble de données**, sélectionnez le bouton d'option du type d'attributs que vous voulez afficher. Si la liste est longue, utilisez la zone de filtre pour réduire la liste en entrant le texte qui doit figurer dans l'ensemble de données.
   Par exemple, l'attribut "config" pour l'agent de système d'exploitation Linux, filtre les ensembles de données pour n'afficher que les ensembles de données **Linux_CPU_Config** et **Linux_OS_Config**.
8. Pour inclure un attribut dans le graphique ou le tableau, cochez la case à côté du nom concerné dans la liste **Attributs** ou cochez la case située en début de liste pour sélectionner tous les attributs.
   Entrez le texte dans la zone de filtre pour localiser des attributs spécifiques comme "percent".
   Par exemple, l'attribut "percent" dans l'ensemble de données KLZ_VM_Stats, filtre la liste pour n'afficher que l'attribut **Espace de stockage virtuel disponible (pourcentage)** et 5 autres attributs "Pourcentage".

   Les graphiques peuvent tracer uniquement des valeurs numériques. Tous les attributs de texte ou de date/heure sont désactivés.
9. Cliquez sur **Prévisualiser les résultats** pour générer la page avec les ensembles de données choisis, un regroupement par colonne de tableau ou ligne du graphique pour chaque attribut, et une ligne ou un point pour chaque échantillon de données.

   Vous obtenez également une ligne ou une ligne de tracé pour l'agrégat de toutes les valeurs.
10. Pour masquer des lignes de graphique ou de tableau, effectuez l'une des étapes suivantes :

Option	Description
Graphique	Masquez une mesure (une ligne du graphique) en désélectionnant la case située en regard du nom dans la légende. Cochez une case pour afficher une mesure.
Tableau	Réduisez le nombre de lignes affichées en entrant la valeur à utiliser pour le filtrage dans la zone de filtre. Vous pouvez également créer un filtre avancé, comme décrit dans «Définition d'un filtre de tableau», à la page 1127.

11. Pour modifier l'intervalle, utilisez le sélecteur de temps :

Option	Description
Temps réel	Pour les tableaux seulement, actualise et affiche uniquement les derniers échantillonnages de données.

Option	Description
2 heures	Représente un point ou ajoute une ligne pour chaque échantillon de données recueilli au cours des deux dernières heures, à intervalles réguliers.
4 heures	Représente un point ou ajoute une ligne pour chaque échantillon de données recueilli au cours des quatre dernières heures, à intervalles réguliers.
12 heures	Représente un point ou ajoute une ligne pour chaque échantillon de données recueilli au cours des douze dernières heures, à intervalles réguliers.
24 heures	Représente un point ou ajoute une ligne pour chaque échantillon de données recueilli au cours des dernières vingt-quatre heures, à intervalles réguliers.
Précédent	Sous-menu d'options permettant d'inclure des données depuis la même période **Hier**, **Il y a deux jours** ou depuis n'importe quel jour jusqu'à **Il y a une semaine**. Par exemple, nous sommes le 22 août à 14h10 et vous définissez le graphique ou le tableau de sorte qu'il affiche les 4 dernières heures. Si vous sélectionnez **Précédent** > **Il y a 1 semaine**, vous voyez des points de données allant de 10h10 à 14h10, au jour d'aujourd'hui, et de 10h10 à 14h10 le 15 août. Si vous sélectionnez un jour précédent, le sélecteur de temps affiche un astérisque (*) tel que Last 4 hours* et les données du jour sélectionné sont réactualisées :

- Vous pouvez uniquement visualiser les données dont la date est comprise entre la date du jour et une semaine auparavant (même si vous avez redéfini la durée maximale de conservation des données historiques sur une valeur supérieure à 8 jours).
- Les graphiques historiques sont représentés de l'échantillon de données le plus ancien au plus récent pour l'intervalle sélectionné ; par exemple, ces 4 dernières heures. Lorsqu'un jour précédent est sélectionné, vous visualisez les données dont la date est comprise entre l'intervalle sélectionné la veille et l'intervalle du jour. Tous les jours compris entre la date la plus ancienne et aujourd'hui montrent un point de tracé avec un horodatage et sans échantillon de données.
- Les tables historiques sont représentées dans l'ordre chronologique décroissant. Lorsqu'un jour précédent est sélectionné pour l'Agent de surveillance des temps de réponse, chaque colonne est répliquée pour le jour précédent avec la mention"Précédent" dans l'en-tête de colonne.
- Quel que soit l'intervalle sélectionné, 11 000 lignes au maximum peuvent être affichées. Par exemple, si vous choisissez d'afficher 12 heures d'un ensemble de données qui envoie 7000 lignes en 2 heures, moins de 3 heures de données d'historique sont renvoyées et les échantillons de données les plus anciens s'affichent.

12. Pour enregistrer ou apporter des modifications au graphique ou au tableau, sélectionnez l'une des options suivantes :

Option	Description
Editer	Renvoie à l'éditeur pour apporter les modifications suivantes : • Editer le titre • Accéder aux échantillons de données **Temps réel** ou **Historique** • Accéder à **Graphique** ou **Tableau** • Sélectionner un **Ensemble de données** et/ou des **Attributs** différents.
Nouveau	Annule toutes les modifications non enregistrées apportées à la vue en cours et vous renvoie à la page de sélection pour créer un nouveau graphique ou tableau.
Annuler	Annule la session d'édition pour la page de graphiques ou de tableaux en cours.

Option	Description
Supprimer	Supprime la page. **Supprimer** est uniquement disponible lorsqu'une page est enregistrée et qu'une édition en cours est annulée.
Sauvegarder pour moi	Enregistre la page de graphiques ou de tableaux pour l'affichage par votre ID utilisateur uniquement. Aucun autre utilisateur ne peut afficher la page enregistrée.
Sauvegarder pour partager	Enregistre la page de graphiques ou de tableaux pour l'affichage par n'importe quel ID utilisateur connecté à la console Cloud APM.

Les vues que vous sauvegardez ont un verrou ouvert à côté du titre. Les vues qu'un autre utilisateur a sauvegardées et que vous n'avez pas le droit d'éditer ont une icône de verrou fermé.

Résultats

Une fois le graphique ou le tableau personnalisé enregistré, il est ajouté à la liste des pages enregistrées. Lorsque vous sélectionnez à nouveau une instance du même type de source de données, par exemple WebSphere Applications, et que vous sélectionnez l'onglet **Détails d'attribut**, la page enregistrée récemment ouverte est affichée. Cliquez sur le titre pour sélectionner une autre page à partir de **Mes pages** ou **Pages partagées**.

Que faire ensuite

Répétez cette procédure pour créer et gérer d'autres pages de graphiques ou de tableaux.

Pour des instructions sur la création d'une table à l'aide des commandes de clavier au lieu des clics de souris, voir «Exemple de création d'une table personnalisée avec les commandes du clavier», à la page 1126.

Exemple de création d'une table personnalisée avec les commandes du clavier

Les utilisateurs malvoyants peuvent utiliser l'onglet de tableau de bord **Détails d'attribut** pour créer des tables historiques comme alternative aux graphiques en courbes historiques, que les technologies d'assistance aux personnes handicapées, telles le logiciel de lecteur d'écran, ne peuvent pas interpréter.

Pourquoi et quand exécuter cette tâche

L'exemple suivant illustre l'utilisation des commandes du clavier pour créer une table historique des transactions qui sont signalées par l'Agent Synthetic Playback. Pour plus d'informations sur l'agent, voir «Gestion des transactions et des événements synthétiques avec Website Monitoring», à la page 1057.

A mesure que vous appuyez sur la touche de tabulation, le focus se déplace en direction de la zone ou de la section suivante de la fenêtre d'application, de gauche à droite ou de haut en bas. Vous pouvez suivre ces étapes pour générer une table de transactions pour l'Agent de surveillance des temps de réponse en remplaçant **My transactions** par une application qui inclut l'agent, ou pour générer une table pour une instance de composant en remplaçant **My transactions** par une autre application et en sélectionnant le groupe **Composants**.

Procédure

Pour créer une table des transactions de l'Agent Synthetic Playback sous l'onglet **Détails d'attribut** à l'aide des raccourcis-claviers, procédez comme suit :

1. Connectez-vous à IBM Cloud Application Performance Management.

   Le focus se trouve sur la barre de navigation.
2. Pour ouvrir le Tableau de bord d'Application Performance, appuyez sur la flèche vers le bas pour déplacer le focus vers le menu **Performance**, appuyez sur la touche Entrée pour le sélectionner, appuyez sur la flèche vers le bas jusqu'à l'option **Tableau de bord d'Application Performance**, puis appuyez de nouveau sur la touche Entrée.

3. Pour ouvrir la page du tableau de bord **Transactions synthétiques**, appuyez plusieurs fois sur la touche de tabulation (environ 7 fois) jusqu'à ce que le focus se déplace vers le navigateur, puis appuyez sur la flèche vers le bas pour activer l'application prédéfinie **My transactions** et appuyez sur la touche Entrée.
4. Pour ouvrir la page du tableau de bord **Détails des transactions**, appuyez plusieurs fois sur la touche de tabulation (environ 10 fois) jusqu'à ce que le focus se déplace vers la section **Instances** de navigateur sur une instance de transaction de l'application **Transactions Synthétiques**, puis appuyez sur la touche Entrée.

   L'onglet **Détails d'attribut** apparaît sur le tableau de bord.
5. Pour ouvrir l'onglet **Détails d'attribut**, appuyez plusieurs fois sur la touche de tabulation (environ 6 fois) jusqu'à le focus se trouve sur l'onglet **Présentation des statuts**, puis appuyez sur la flèche vers la droite jusqu'à ce que le focus se trouve sur l'onglet **Détails d'attribut**.

   Le **tableau** **Historique** ainsi que tous les attributs de l'ensemble de données **Disponibilité des transactions dans le temps** sont sélectionnés.
6. Pour générer la table, appuyez plusieurs fois sur la touche de tabulation (environ 18 fois) jusqu'à ce que le focus se trouve sur le bouton **Prévisualiser les résultats**, puis appuyez sur la touche Entrée.

Résultats

Les attributs **Disponibilité des transactions dans le temps** sont affichés dans une table, avec une colonne pour chaque attribut et une ligne pour chaque échantillon de données recueilli au cours des dernières 4 heures.

Que faire ensuite

- Pour diminuer le nombre de lignes affichées, vous pouvez appuyer sur la touche de tabulation pour activer la zone de texte **Filtrer** et saisir un texte partiel ou entier ou une valeur d'horodatage sur laquelle appliquer le filtre.
- Pour modifier l'intervalle, déplacez le focus vers le menu déroulant **Dernières 4 heures** du sélecteur de temps et sélectionnez une autre option. Pour plus d'informations, voir l'étape «11», à la page 1124 dans «Création d'une page de graphiques ou de tableaux personnalisés», à la page 1123.
- Pour générer une table avec l'ensemble de données **Temps de réponse de transaction**, appuyez plusieurs fois sur la touche de tabulation (environ 2 fois) pour déplacer le focus vers l'outil **Nouveau**, puis appuyez sur la touche Entrée. Le panneau de sélection est affiché. Sélectionnez l'ensemble de données **Temps de réponse de transaction** et le bouton **Prévisualiser les résultats**.

Définition d'un filtre de tableau

Vous pouvez limiter les lignes d'un tableau que vous visualisez dans l'onglet **Détails d'attribut** du tableau de bord pour n'afficher que les lignes d'un certain type, ou ayant des valeurs d'attribut spécifiques par texte ou par horodatage. Bien que les valeurs numériques soient indisponibles pour le filtrage, telles que les pourcentages, certaines valeurs d'attribut numérique sont converties en valeur d'affichage pour le tableau et traitées comme du texte.Vous pouvez appliquer un filtre rapide ou ouvrir un éditeur pour composer un filtre avancé.

Procédure

Procédez comme suit pour filtrer un tableau personnalisé selon les valeurs d'attribut de texte ou d'horodatage. Bien que les valeurs numériques soient indisponibles pour le filtrage, telles que les pourcentages, certaines valeurs d'attribut numérique sont converties en valeur d'affichage pour le tableau et traitées comme du texte.

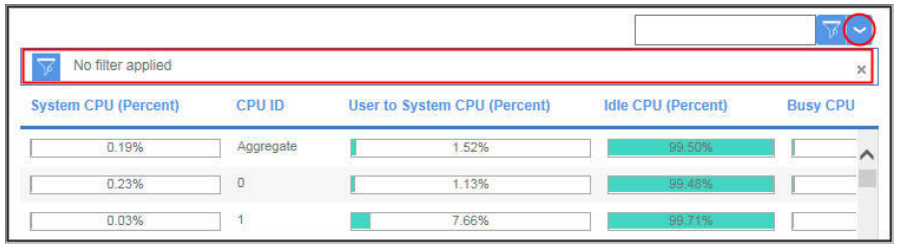
1. Après avoir ouvert le Tableau de bord d'Application Performance à partir du menu **Performance**, accédez au niveau d'une instance de la ressource gérée.
2. Cliquez sur l'onglet **Détails d'attribut**.

   La page enregistrée la plus récente est affichée ou, si aucune page n'a été enregistrée, les listes de sélection d'**Ensemble de données** et d'**Attributs** sont affichées.

3. Si une page de table enregistrée est affichée, passez à l'étape «5», à la page 1128, sélectionnez une autre page de table enregistrée dans le menu déroulant ou cliquez sur **Ajouter** pour créer une table.
4. Si vous créez un nouveau tableau ou que vous éditez un tableau enregistré, sélectionnez l'**Ensemble de données** et les **Attributs** à utiliser, puis cliquez sur **Prévisualiser les résultats**.
5. Pour appliquer un filtre rapide, cliquez dans la zone de texte **Filtre** et entrez le texte partiel ou complet qui servira de filtre.

   A mesure que vous entrez des caractères, toutes les lignes ne contenant pas les caractères saisis sont supprimées du tableau. Pour supprimer le filtre rapide, supprimez la valeur ou cliquez sur "x".
6. Pour appliquer un filtre avancé, cliquez sur le menu déroulant et sélectionnez **Définir le filtre** ou cliquez dans la barre de filtre.

   La fenêtre de **génération de filtre** s'ouvre avec les règles qui ont été définies.



7. Pour définir une règle, renseignez les zones :
   a) Laissez le paramètre de colonne défini sur "Any Column" (Toute colonne) ou sélectionnez l'attribut selon lequel filtrer dans la liste.
   b) Laissez la condition définie sur "contains" (contient) ou sélectionnez un autre opérateur dans la liste et entrez la valeur de texte ou d'horodatage selon laquelle filtrer dans la zone de texte :

Condition	Ligne incluse dans le tableau lorsque...
contains	La valeur de filtre est trouvée quelque part dans la cellule.
equals	La valeur de cellule correspond exactement à la valeur de filtre, y compris la casse.
starts with	La valeur de cellule commence par les mêmes caractères que la valeur de filtre.
ends with	La valeur de cellule comporte les mêmes caractères que la fin de la valeur de filtre.
does not equal	La valeur de cellule n'est pas une correspondance exacte de la valeur de filtre.
does not contain	La valeur de cellule ne contient pas le même texte ou nombre que la valeur de filtre.
does not start with	La valeur de cellule ne commence pas par les mêmes caractères que la valeur de filtre.
does not end with	La valeur de cellule ne se termine pas par les mêmes caractères que la valeur de filtre.
is empty	La cellule ne contient pas de données.

   c) Une fois que vous avez terminé la règle, cliquez sur **Filtre** pour voir les résultats, puis sur **Ajouter une règle de filtrage** pour ajouter une autre règle, ou passez à l'étape suivante.
8. Si le filtre comporte plusieurs règles, opérez votre sélection parmi les options suivantes :

   - **Match** (Correspondance) est défini initialement sur **All rules** (toutes les règles), ce qui signifie qu'une ligne s'affiche uniquement si ses données suivent toutes les règles du filtre. La ligne est exclue si aucune valeur de texte ou d'horodatage ne suit une règle. S'il existe plusieurs règles et

que vous voulez inclure une ligne si elle suit l'une des règles au moins, remplacez le paramètre par **Any rule**.

- Pour éditer une règle, modifiez une ou plusieurs valeurs de zone.
- Pour supprimer une règle, sélectionnez-la et cliquez sur **Supprimer la règle**.

9. Lorsque vous avez terminé de définir une ou plusieurs règles, cliquez sur **Filtre** pour fermer la boîte de dialogue et appliquer le filtre.

Résultats

Les groupes qui ne répondent pas aux critères de filtrage ne s'affichent plus et la barre de filtre signale le nombre d'éléments, par exemple, "480 of 1200 items shown".

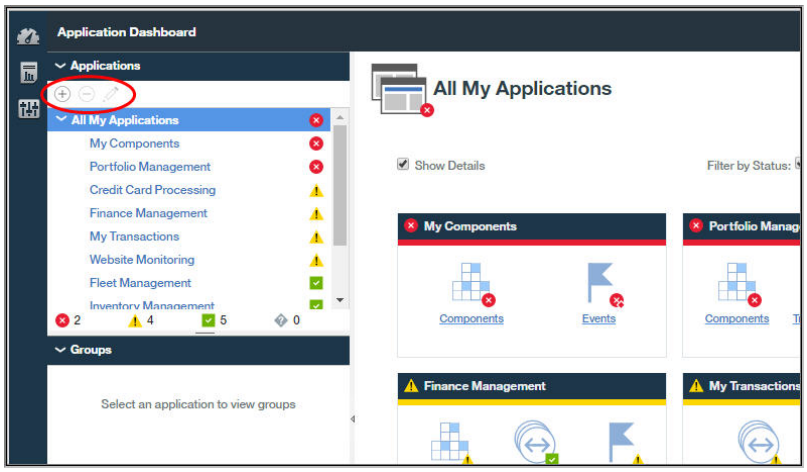
Que faire ensuite

- Survolez la barre de filtre avec le pointeur de la souris pour ouvrir une fenêtre en incrustation avec les critères de filtrage. Vous pouvez supprimer une règle (cliquez sur ×) ou cliquer à l'intérieur de la fenêtre pour éditer les critères de filtrage.
- Cliquez sur **Effacer le filtre** dans la barre de filtre ou sur **Effacer** dans la fenêtre **Générer le filtre** pour supprimer le filtre et afficher toutes les lignes.

Gestion des applications

Utilisez les outils disponibles dans le Tableau de bord d'Application Performance pour organiser vos ressources gérées dans les applications.

Les outils **Applications** du navigateur ouvrent l'éditeur d'application en vue de la création ou de l'édition d'applications et de l'application des ressources gérées disponibles.



L'application **Mes composants** est une application prédéfinie qui inclut les systèmes gérés reconnus par le serveur serveur Cloud APM. Elle ne peut pas être éditée ni supprimée.

Pour une démonstration vidéo sur l'ajout d'une application, visionnez Application Performance Management - Define Application.

Pour un scénario sur la création d'une application de surveillance de la liste d'applications IBM Java, voir «Ajout d'applications Web au Tableau de bord d'Application Performance », à la page 92 et «Association d'une Liste d'applications Java IBM à l'application Web », à la page 93.

Restriction : Vous devez disposer des droits de modification pour les Applications afin de pouvoir utiliser l'outil Ajouter une application. Vous devez disposer des droits de modifications pour Applications ou pour l'application spécifique afin de pouvoir utiliser les outils Supprimer et Editer. Pour plus d'informations, voir «Utilisation des rôles, des utilisateurs et des droits», à la page 1039.

Ajout d'une application

Utilisez l'éditeur d'application pour créer une application et appliquer les ressources gérées qui sont disponibles, ou sélectionner une application parmi les applications reconnues.

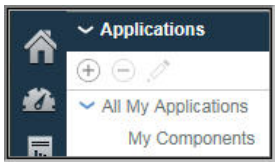
Avant de commencer

Vous devez disposer des droits de modification pour les Applications afin de pouvoir utiliser l'outil Ajouter une application. Pour plus d'informations, voir «Utilisation des rôles, des utilisateurs et des droits», à la page 1039.

Procédure

Effectuez les étapes suivantes dans la console Cloud APM pour ajouter une application au Tableau de bord d'Application Performance.

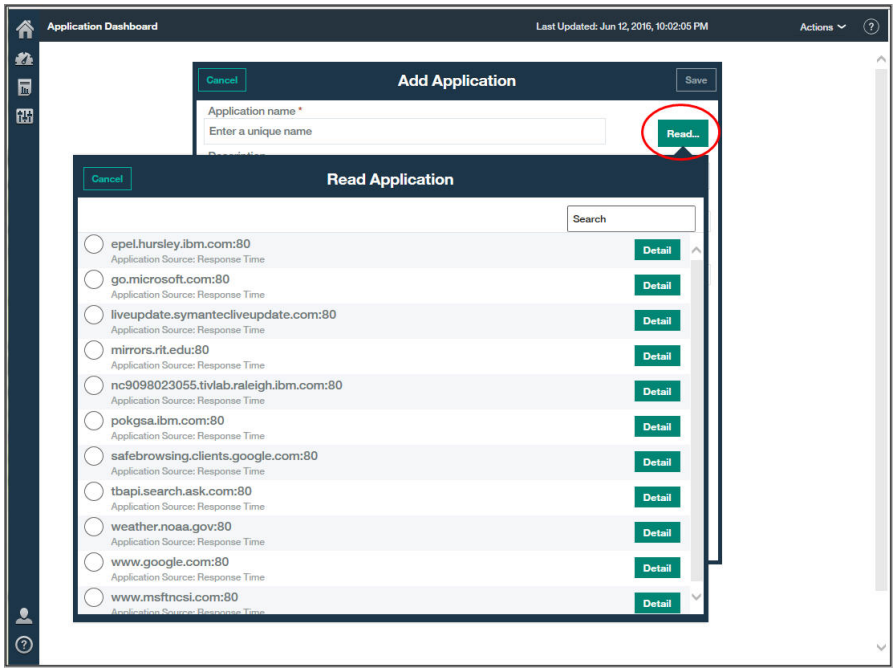
1. Si le Tableau de bord d'Application Performance n'est pas affiché, sélectionnez-le dans le menu **Performance**, ou, à partir d'une autre page de la console, cliquez sur le lien **Accueil**.
2. Dans la section **Applications** du navigateur, cliquez sur . La fenêtre **Ajouter une application** s'ouvre.

3. Entrez un nom pour votre application dans la zone **Nom de l'application** ainsi qu'une description (facultatif) dans la zone **Description**.

   N'utilisez pas les symboles ! " % & ' * ? < > } { \ dans le nom ou la description.

   Des exemples de nom d'application tels que "Finance Management" et "Credit Card Processing" sont disponibles dans la Démonstration guidée.
4. Cliquez sur **Lire** pour ouvrir la fenêtre **Lire l'application** affichant la liste des applications reconnues et effectuez une ou plusieurs des étapes ci-après :
   - Cliquez sur **Détail** pour afficher les composants d'une application.
   - Sélectionnez l'application que vous voulez utiliser, puis cliquez sur **Sauvegarder**. La fenêtre **Lire l'application** se ferme, le référentiel source apparaît dans la zone **Application lue dans**, et les composants sont répertoriés dans **Composants d'application**.
   - Cliquez sur **Annuler** pour fermer la fenêtre sans effectuer de choix.



5. Dans la zone **Modèle**, conservez le modèle **Application personnalisée** ou sélectionnez un modèle différent avec le bouton , puis cliquez sur **Sauvegarder**.

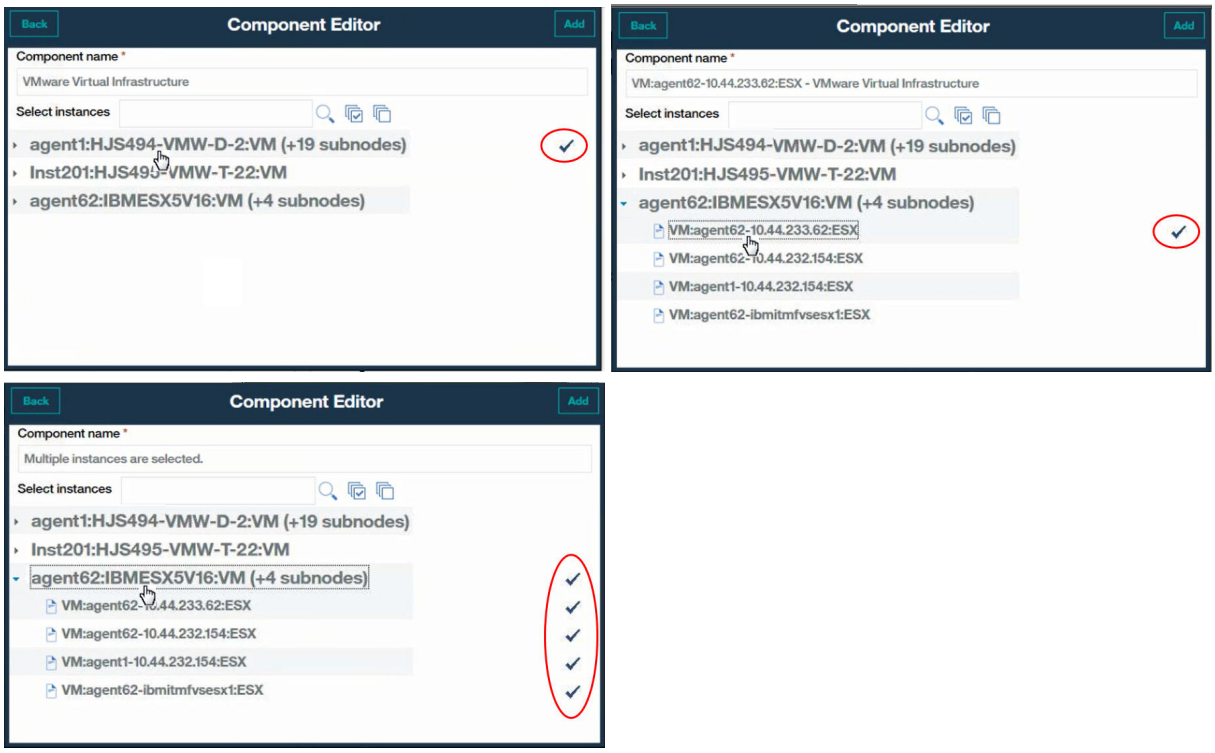
   Les instances et les types de composant associés sont répertoriés dans la liste **Composants d'application**.

6. Cliquez sur **Ajouter des composants** et, dans la fenêtre **Sélectionner le composant** qui s'ouvre, sélectionnez un composant dans la liste.

   L'**éditeur de composant** s'ouvre.

7. Pour rechercher et sélectionner des instances de noeud et/ou de sous-noeud agent pour l'application, effectuez une ou plusieurs des étapes ci-après :

   - Cliquez sur une instance pour la sélectionner.
   - Pour les noeuds agent comportant des sous-noeuds, sélectionnez le noeud seul en cliquant sur son nom dans l'arborescence alors que celle-ci est réduite, sélectionnez le noeud et tous les sous-noeuds en développant l'arborescence de noeud (cliquez sur), puis cliquez sur le noeud, ou sélectionnez des sous-noeuds individuels en développant l'arborescence de noeud et en cliquant sur l'instance.
   - Utilisez la barre d'outils pour rechercher des instances contenant le texte dans la zone de texte à rechercher, sélectionner toutes les instances, ou désélectionner toutes les instances.
   - Pour changer le nom d'affichage dans le navigateur, éditez le nom du composant.



V6-V7 Si vous ajoutez une instance d'agent Tivoli Monitoring et ne le voyez pas dans la liste des instances disponibles, vérifiez que Tivoli Enterprise Portal Server qui est associé à la Passerelle hybride est dans une version prise en charge (visitez le Hybrid Gateway supported agents (APM Developer Center)).

8. Cliquez sur **Ajouter** pour ajouter les noeuds et sous-noeuds agent sélectionnés à l'application, puis cliquez sur **Précédent**.

   La liste Composants d'application est mise à jour avec les nouveaux noms de composant.

9. Sélectionnez un autre composant auquel ajouter des instances, puis répétez les étapes «6», à la page 1131, «7», à la page 1131 et «8», à la page 1132, ou cliquez sur **Fermer**.
10. Si d'autres instances sont liées aux composants dans la liste **Composants d'application**, un bouton qui indique le nombre d'instances liées est affiché, et vous pouvez effectuer les opérations suivantes :

    a) Cliquez sur le bouton pour afficher les instances associées dans la fenêtre **Détails mis à jour**. Une barre s'affiche pour chaque type de mise à jour, y compris le nom d'instance. Par exemple, si l'un des composants a été supprimé, il apparaît sous la barre des composants **Supprimé**.

    b) Sélectionnez une ou plusieurs instances et cliquez sur **Sauvegarder** pour mettre à jour la liste des ressources d'application.

11. Une fois que vous avez terminé de définir l'application, fermez l'éditeur d'application en cliquant sur **Sauvegarder** pour sauvegarder vos modifications, ou cliquez sur **Annuler** pour annuler les modifications.

Résultats

Vos mises à jour d'application sont effectuées par le serveur Cloud APM une fois que vous avez sauvegardé vos modifications. L'affichage des modifications dans le tableau de bord peut prendre quelques minutes. (Essayez de nettoyer le cache du navigateur si l'affichage de vos modifications prend trop de temps.) La nouvelle application s'affiche dans le Tableau de bord d'Application Performance et dans la section **Applications** du navigateur. Lorsque l'application est sélectionnée, les composants s'affichent dans la section **Groupes**.

Edition d'une application

Utilisez l'éditeur d'application pour modifier une application définie et ajouter ou supprimer des ressources gérées en tant que composants de l'application.

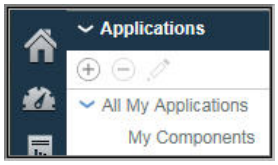
Avant de commencer

Vous devez disposer d'une autorisation de modification des applications ou de l'application spécifique pour utiliser l'outil d'édition. Pour plus d'informations, voir «Rôles et droits», à la page 1031.

Procédure

Effectuez les étapes suivantes dans la console Cloud APM pour éditer une application.

1. Si le Tableau de bord d'Application Performance n'est pas affiché, sélectionnez-le dans le menu **Performance**, ou, à partir d'une autre page de la console, cliquez sur le lien **Accueil**.
2. Sélectionnez l'application à éditer dans la liste **Toutes mes applications** du navigateur, puis cliquez sur .

   La fenêtre **Modification d'application** s'ouvre.
3. Facultatif : Editez le **Nom d'application** ou la **Description**.

   N'utilisez pas les symboles ! " % & ' * ? < > } { \ dans le nom ou la description.
   Si vos autorisations d'affichage ou de modification des applications concernent certaines applications mais pas toutes, vous ne pourrez peut-être pas visualiser l'application dans le tableau de bord ni la modifier après son changement de nom. Cette limitation se produit car l'application renommée est traitée comme une nouvelle application. Demandez à l'administrateur de rôle ou de surveillance de vous donner l'autorisation d'affichage ou de modification de l'application renommée.
4. Pour ajouter des composants et des instances à l'application procédez comme suit.
   a) Cliquez sur et, dans la fenêtre qui s'ouvre, sélectionnez un composant dans la liste.

      L'**éditeur de composant** s'ouvre.
   b) Sélectionnez les instances de noeud et/ou de sous-noeud agent pour l'application :
      - Cliquez sur une instance pour la sélectionner.
      - Pour les noeuds comportant des sous-noeuds, sélectionnez le noeud en cliquant sur son nom dans l'arborescence alors que celle-ci est réduite, sélectionnez le noeud et tous les sous-noeuds en développant l'arborescence de noeud (cliquez sur), puis cliquez sur le noeud, ou sélectionnez des sous-noeuds individuels en développant l'arborescence de noeud et en cliquant sur l'instance.
      - Utilisez la barre d'outils pour rechercher des instances contenant le texte dans la zone de texte à rechercher, sélectionner toutes les instances, ou désélectionner toutes les instances.
      - Pour changer le nom d'affichage dans le navigateur, éditez le nom du composant.
   c) Cliquez sur **Ajouter** pour ajouter l'instance ou les instances, puis cliquez sur **Précédent**.

      La liste Composants d'application est mise à jour avec les nouveaux noms de composant.
   d) Vous pouvez sélectionner un autre composant auquel ajouter des instances, ou cliquer sur **Fermer**.

   La liste Composants d'application est mise à jour avec les nouveaux noms de composant. Le nombre entre parenthèses après le nom correspond au nombre d'instances qui sont associées au composant.
5. Pour éditer un nom de composant ou changer l'instance qui lui est associée, sélectionnez le composant dans la liste **Composants d'application** et cliquez sur :
   a) Pour associer une autre instance au composant, recherchez l'instance de votre choix et sélectionnez-la.

b) Pour changer le nom de composant qui est utilisé comme nom d'affichage dans le navigateur pour cette application, éditez la zone de **nom du composant**.

c) Cliquez sur **Sauvegarder**.

La liste Composants d'application est mise à jour avec les modifications que vous avez apportées.

6. Pour retirer un composant ou une instance de l'application, sélectionnez-le ou la et cliquez sur ⊖. Cliquez sur **OK** pour confirmer.
7. Si d'autres instances sont liées aux composants dans la liste **Composants d'application**, un bouton qui indique le nombre d'instances liées est affiché, et vous pouvez effectuer les opérations suivantes :

   a) Cliquez sur le bouton (1) pour afficher les instances associées dans la fenêtre **Détails mis à jour**. Une barre s'affiche pour chaque type de mise à jour, y compris le nom d'instance. Par exemple, si l'un des composants a été supprimé, il apparaît sous la barre des composants **Supprimé**.

   b) Sélectionnez une ou plusieurs instances et cliquez sur **Sauvegarder** pour mettre à jour la liste des ressources d'application.
8. Une fois que vous avez terminé d'éditer l'application, fermez l'éditeur d'application en cliquant sur **Sauvegarder** pour sauvegarder vos modifications, ou cliquez sur **Annuler** pour annuler les modifications.

Résultats

Vos mises à jour d'application sont effectuées par le serveur Cloud APM une fois que vous avez sauvegardé vos modifications. L'affichage des modifications dans le tableau de bord peut prendre quelques minutes.

Référence associée

«Rôles et droits», à la page 1031

Suppression d'une application

Lorsque vous n'en n'avez plus besoin, vous pouvez supprimer une application dont vous avez défini l'affichage dans le Tableau de bord d'Application Performance. La suppression d'une application ne désinstalle pas les composants de prise en charge ; seule l'application qui les contient est supprimée. Ces mêmes composants peuvent être ajoutés à d'autres applications et ne sont pas supprimés des applications auxquelles ils appartiennent.

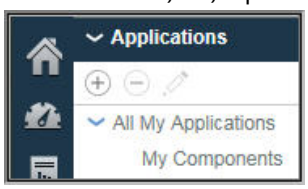
Avant de commencer

Vous devez disposer des droits de modification pour Applications ou pour l'application spécifique pour pouvoir utiliser l'outil Supprimer. Pour plus d'informations, voir «Utilisation des rôles, des utilisateurs et des droits», à la page 1039.

Procédure

Pour supprimer une application du Tableau de bord d'Application Performance, procédez comme suit :

1. Si le Tableau de bord d'Application Performance n'est pas affiché, sélectionnez-le dans le menu **Performance**, ou, à partir d'une autre page de la console, cliquez sur le lien **Accueil**.



2. Dans la section **Applications** du navigateur, sélectionnez l'application que vous voulez supprimer de la liste **Toutes mes applications**, puis cliquez sur ⊖.

   Un message vous demandant de confirmer votre choix s'affiche.
3. Cliquez sur **Oui** pour confirmer la suppression de l'application, ou sur **Non** si vous n'êtes pas sûr de votre choix.

Résultats
Une fois que vous avez cliqué sur **Oui**, l'application est supprimée du Tableau de bord d'Application Performance.

Que faire ensuite
Répétez cette étape pour les autres applications à supprimer.

Affichage et suppression des agents en ligne

Les agents hors ligne pendant quatre jours sont supprimés de la console Cloud APM. Cette rubrique décrit la façon dont les agents hors ligne sont indiqués, ainsi que l'impact sur les groupes de ressources, les vues de topologie et les autres fonctions. Pour supprimer un système géré du tableau de bord avant la période des quatre jours, utilisez l'éditeur d'application. .

Pourquoi et quand exécuter cette tâche
Une fois les agents installés sur les systèmes que vous voulez gérer, ils se connectent au serveur Cloud APM et envoient des échantillons de données au Tableau de bord d'Application Performance à des fins de présentation et d'évaluation des seuils. Si un agent est hors ligne, l'indicateur de statut s'affiche dans le navigateur et le tableau de bord. Si, au bout d'un certain temps, l'agent ne répond pas, le serveur affiche un message indiquant que l'agent est indisponible. Voir «Exemples d'agents hors ligne», à la page 1136 .

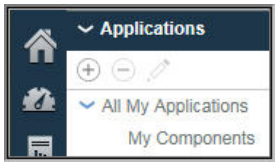
Après quatre jours, l'agent hors ligne est supprimé de l'interface utilisateur, sauf s'il prend en charge le suivi des transactions. Dans ce cas, l'agent hors ligne continue de s'afficher dans les vues Agréger une topologie de transaction et Topologie des instances de transaction.

Vous pouvez supprimer l'agent hors ligne des applications définies ; il est alors supprimé de la console Cloud APM avant que la période des quatre jours ne soit totalement écoulée.

Procédure

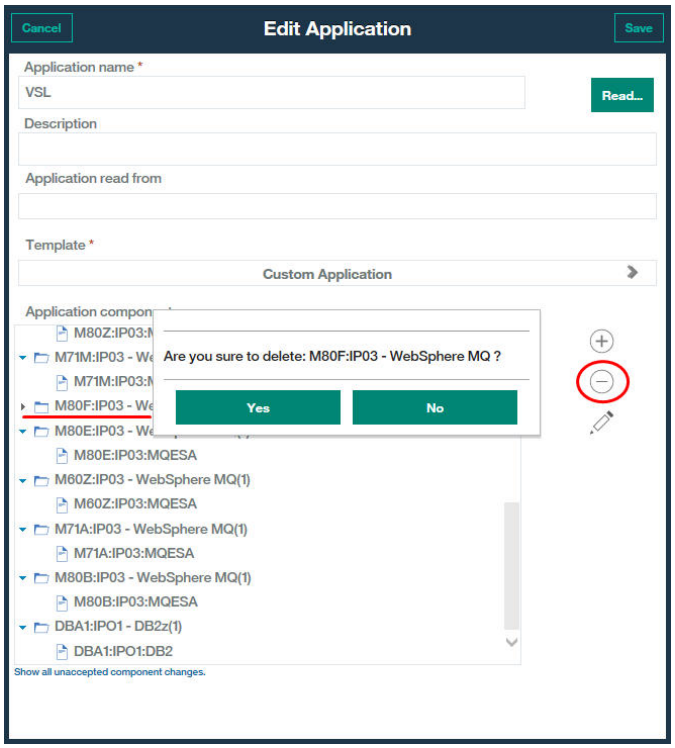
Pour supprimer un agent hors ligne d'une application définie, procédez comme suit :

1. Si le Tableau de bord d'Application Performance n'est pas affiché, sélectionnez-le dans le menu **Performance**, ou, à partir d'une autre page de la console, cliquez sur le lien **Accueil**.
2. Dans la section **Applications** du navigateur, sélectionnez l'application à laquelle l'agent hors ligne appartient, puis cliquez sur **Modifier une application**.



3. Sélectionnez l'agent ou le sous-noeud agent dans la liste Composants d'application, puis cliquez sur .

   Pour les agents comportant des sous-noeuds, sélectionnez l'agent seul en cliquant sur son nom dans l'arborescence alors que celle-ci est réduite, sélectionnez le noeud et tous les sous-noeuds en développant l'arborescence de noeud (cliquez sur), puis cliquez sur le noeud, ou sélectionnez des sous-noeuds individuels en développant l'arborescence de noeud et en cliquant sur l'instance.



4. Une fois que vous avez modifié l'application en vue de supprimer l'agent ou le sous-noeud hors ligne, cliquez sur **Sauvegarder**.

Résultats

Vos mises à jour d'application sont effectuées par le serveur Cloud APM une fois que vous avez sauvegardé vos modifications. La suppression de l'agent hors ligne du Tableau de bord d'Application Performance peut prendre quelques minutes.

Exemples d'agents hors ligne

Cette rubrique décrit les modes d'affichage possibles des agents hors ligne dans la console Cloud APM. Vous pouvez supprimer l'affichage des agents hors ligne que vous ne voulez plus surveiller. La surveillance reprend si l'agent se remet en ligne.

Lorsqu'un agent est hors ligne, aucune donnée n'est envoyée à la console console Cloud APM et le Tableau de bord d'Application Performance affiche un indicateur de statut pour l'agent et pour les applications auxquelles il appartient. L'agent ne peut pas être ajouté à une application définie de l'éditeur d'application ni à un groupe personnalisé du gestionnaire de groupes de ressources, de même qu'il ne peut pas créer de tableaux et de graphiques à courbes d'historique dans l'onglet Détails d'attribut.

Tableau de bord d'Application Performance - Toutes mes applications

La page d'accueil de tableau de bord **Toutes mes applications** fournit la première indication quant au statut hors ligne. Le compteur situé dans la section Applications du navigateur indique le nombre d'applications dont les ressources sont indisponibles.

La zone récapitulative indique le statut d'événement Normal, aucun événement n'étant ouvert pour les ressources gérées de l'application.

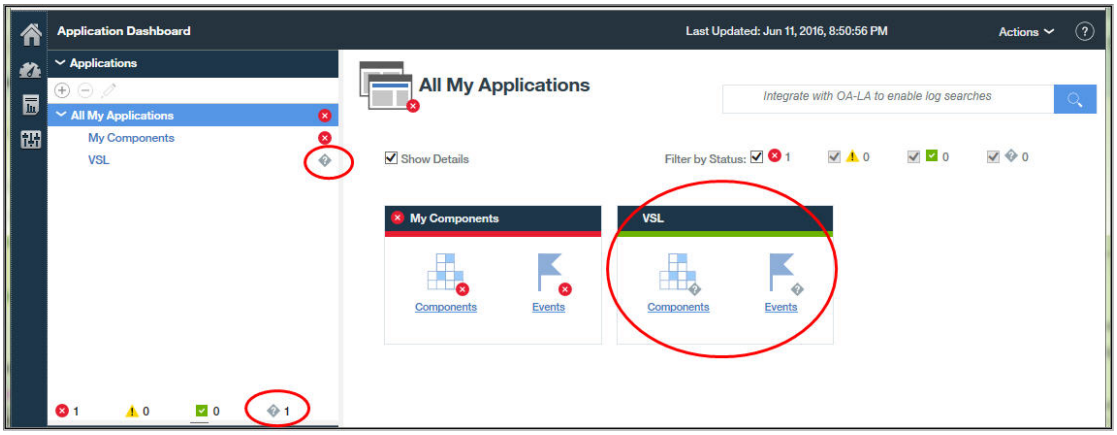


Tableau de bord d'Application Performance - Application

Une fois que l'utilisateur a cliqué sur la barre de titre de la zone récapitulative ou a sélectionné l'application depuis le navigateur, l'onglet **Présentation des statuts** s'affiche avec un graphique **Récapitulatif de la gravité de l'événement** vide. Le graphique à barres **Statut du composant en cours** indique le statut "Inconnu" pour les agents hors ligne.

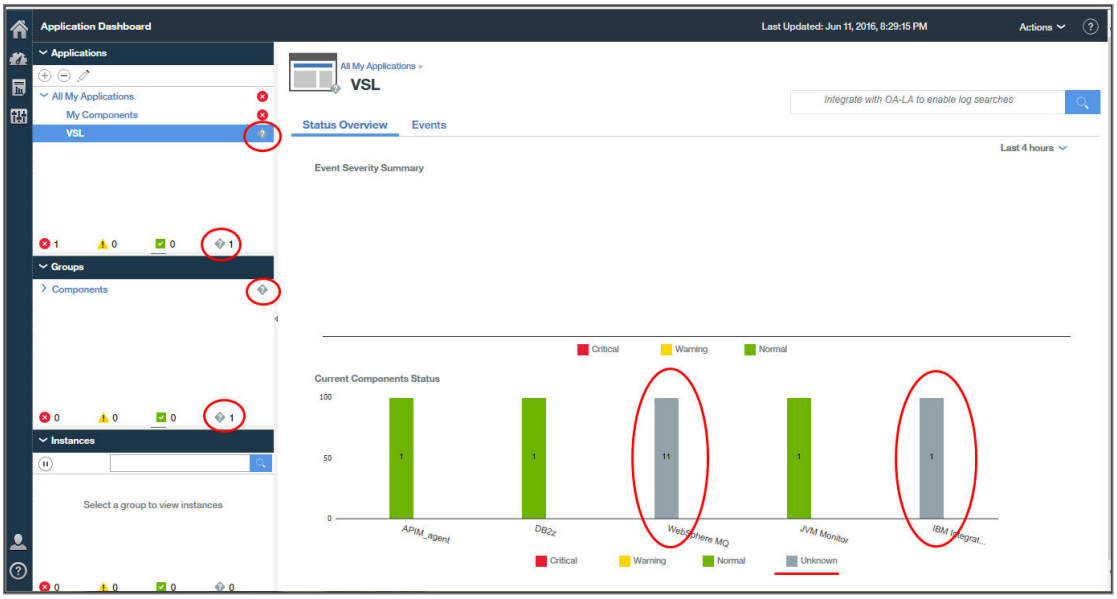


Tableau de bord d'Application Performance - Groupe

Une fois que l'utilisateur a cliqué sur le graphique **Statut de composant en cours** ou sur le groupe **Composants** du navigateur, l'onglet **Présentation des statuts** est modifié et affiche un widget de groupe récapitulatif pour chaque ressource gérée. Les widgets de groupe des agents non disponibles affichent un message indiquant que l'agent est hors ligne au lieu des indicateurs clés de performance.

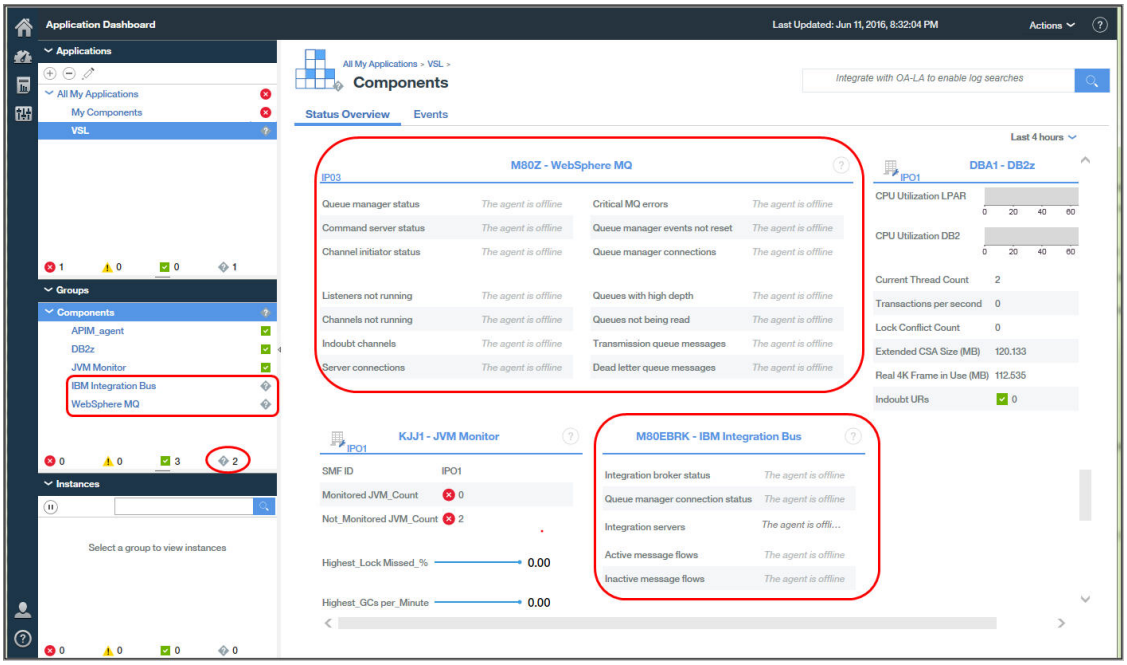
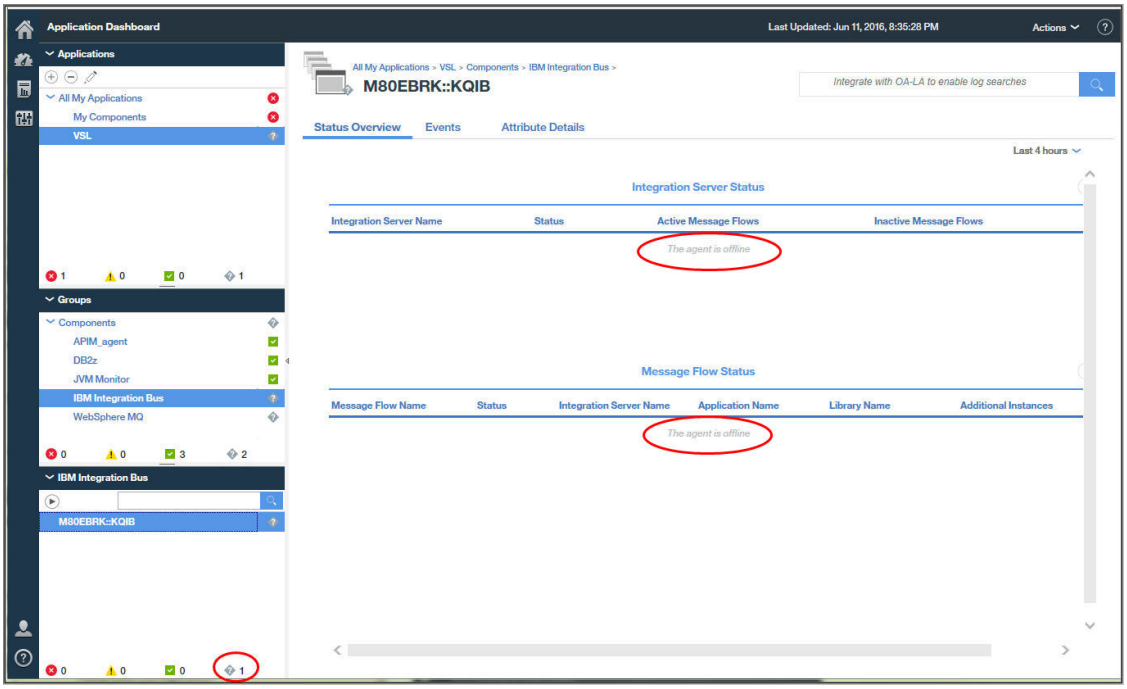
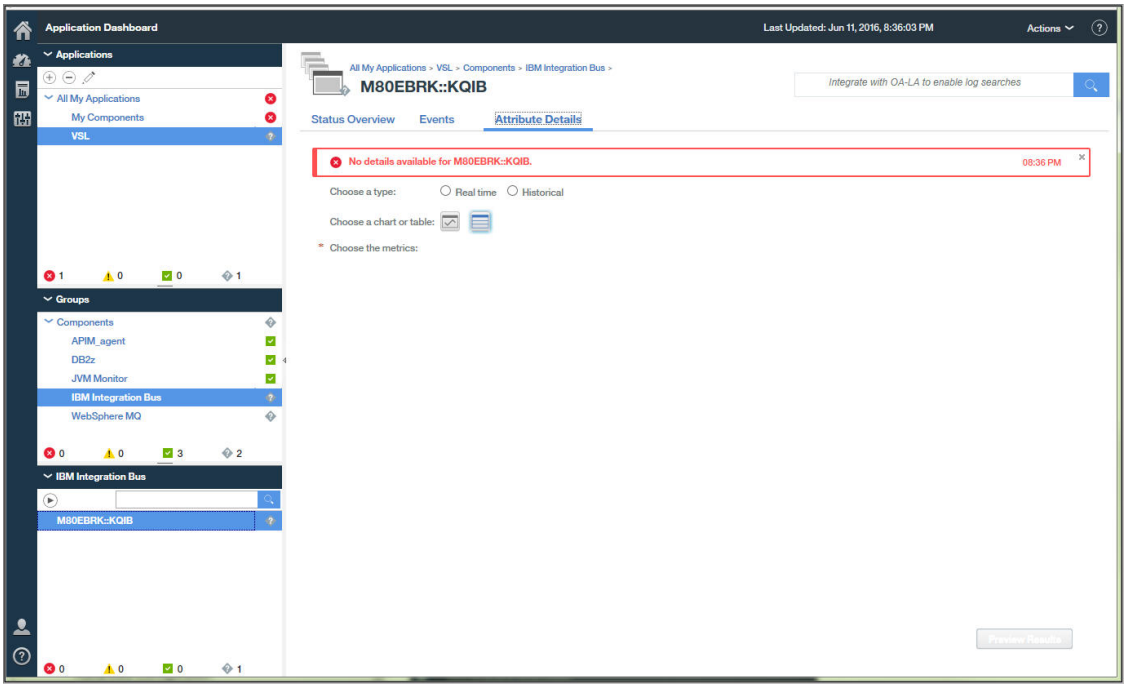


Tableau de bord d'Application Performance - Instance

Une fois que l'utilisateur a cliqué sur l'un des widgets de groupe récapitulatif de l'agent hors ligne, l'onglet **Présentation des statuts** affiche des widgets de table et de graphique pour l'agent sélectionné. Cependant, comme pour le widget de groupe récapitulatif, seul le message indiquant que l'agent est hors ligne s'affiche, au lieu des indicateurs clé de performance pour l'instance d'agent.



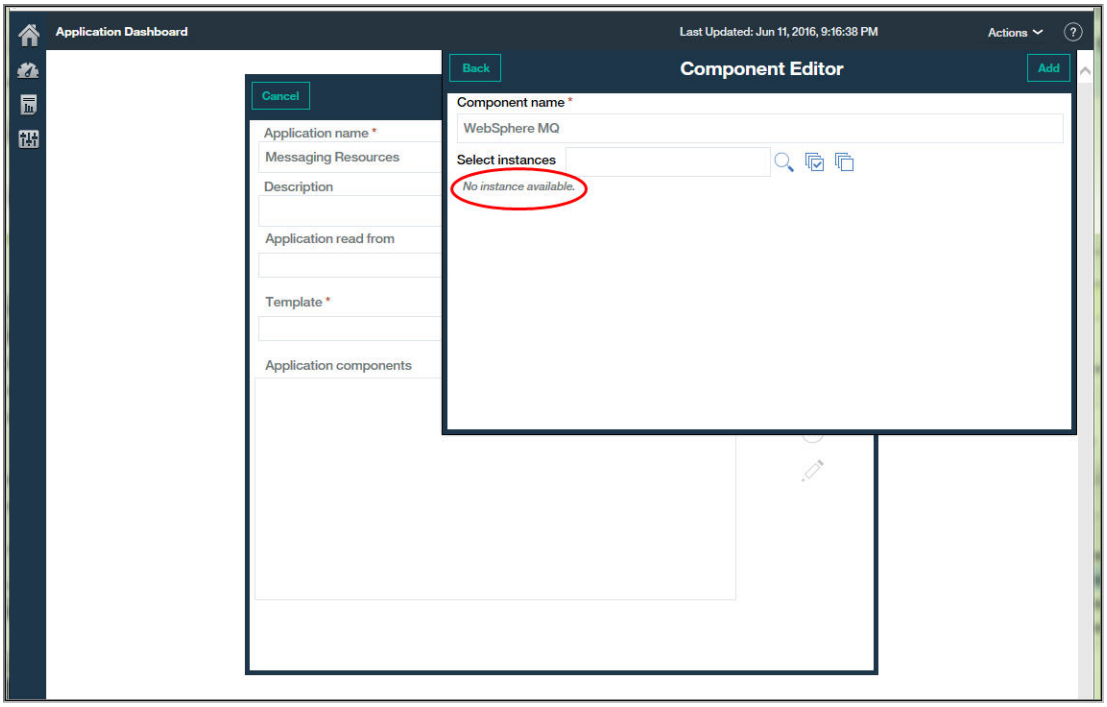
Lorsque l'utilisateur clique sur l'onglet **Détails d'attribut**, un message indiquant qu'aucun détail n'est disponible pour l'instance d'agent s'affiche. Il n'est pas possible de créer un graphique ou un tableau personnalisé pour l'instance d'agent hors ligne.



Editeur d'application

Dans le Tableau de bord d'Application Performance, lorsque l'utilisateur clique sur l'outil **Ajouter une application** ou **Modifier une application** de la section Applications du navigateur, la fenêtre d'éditeur d'application apparaît.

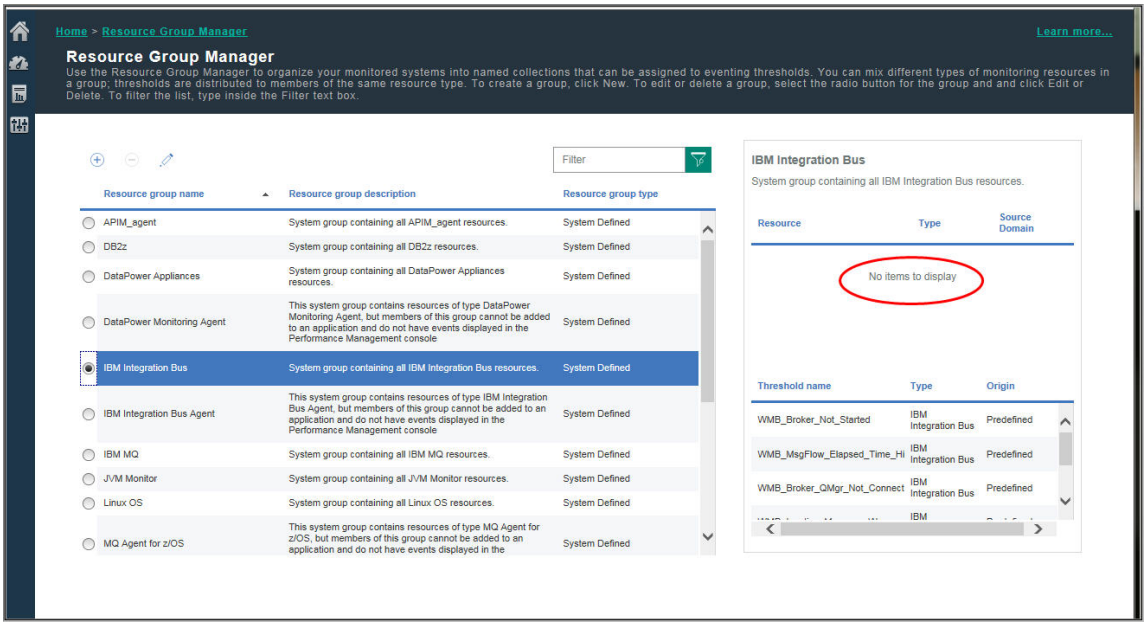
Lorsque l'utilisateur clique sur **Ajouter des composants** et qu'il sélectionne un type d'agent, si aucun agent de ce type n'est installé ou qu'un agent est hors ligne, un message indiquant qu'aucune instance d'agent n'est disponible s'affiche. Si d'autres instances d'agent sont disponibles, elles sont répertoriées dans la liste.



Gestionnaire de groupes de ressources

Lorsque l'utilisateur sélectionne **Configuration du système** > **Gestionnaire de groupes de ressources**, la page s'affiche avec une table des groupes de ressources. Lorsque vous sélectionnez un

groupe, les instances d'agent qui le composent sont répertoriées avec les seuils affectés. Si toutes les instances d'agent sont hors ligne, un message indiquant qu'aucune instance n'est disponible s'affiche.



Concepts associés

«Gestion des applications», à la page 1129
Utilisez les outils disponibles dans le Tableau de bord d'Application Performance pour organiser vos ressources gérées dans les applications.

«Utilisation des tableaux de bord», à la page 1109

Référence associée

«Gestionnaire de groupes de ressources», à la page 1008
Votre environnement surveillé peut comporter plusieurs systèmes gérés pouvant être catégorisés par objectif. Ces systèmes possèdent souvent les mêmes exigences de seuil. Utilisez le **gestionnaire de groupes de ressources** pour organiser les systèmes gérés en groupes auxquels vous pouvez affecter des seuils. Vous pouvez également créer des groupes de ressources correspondant à vos stratégies de contrôle d'accès basé sur les rôles.

Statut de l'événement

Utilisez le **Statut de l'événement** pour obtenir une présentation récapitulative des événements ouverts de l'élément de navigateur sélectionné et pour répondre aux événements ayant le statut critique ou avertissement en accédant aux tableaux de bord détaillés.

Les indicateurs de statut concernent les événements de seuil qui sont exécutés sur vos systèmes gérés. Si des Passerelles hybrides sont configurées, les événements peuvent également être déclenchés par des situations survenant sur les systèmes gérés de votre environnement IBM Tivoli Monitoring. Si votre configuration inclut IBM Operations Analytics - Predictive Insights, toute anomalie détectée est également affichée.

Les événements liés à certains seuils ne sont pas affichés dans le Tableau de bord d'Application Performance. Les seuils utilisent des attributs pour des ressources qui ne sont pas publiées, ce qui peut se produire dans les agents prenant en charge des sous-noeuds. (Pour une description des sous-noeuds, voir la rubrique Agent Builder à l'adresse).

Critique, Avertissement, Normal

- Les indicateurs de statut consolident les gravités d'événement à partir des seuils :

  Le statut Critique indique tous les événements ayant un niveau de gravité Fatal ou Critique

Le statut Avertissement indique tous les événements ayant un niveau de gravité Mineur ou Avertissement

Le statut Normal indique tous les événements ayant un niveau de gravité Inconnu

Le statut Inconnu indique que le système géré est hors ligne. Après avoir passé 4 jours hors ligne, le système géré est supprimé de toutes les applications et n'apparaît plus dans les tableaux de bord.
Pour vérifier le statut, arrêter ou démarrer un agent, voir «Utilisation des commandes de l'agent», à la page 181

- V6-V7 Si une ou plusieurs Passerelles hybrides sont configurées, les indicateurs de statut des événements générés par les situations Tivoli Monitoring sont identiques à ceux des seuils, à l'exception du statut Normal qui indique des événements dont le niveau de gravité est Sans conséquences, Information ou Inconnu.
- Lorsque votre environnement géré inclut IBM Operations Analytics - Predictive Insights, toutes les anomalies détectées sont indiquées par une icône en forme de diamant sur l'indicateur de statut, par exemple . Pour plus d'informations, voir «Recherche d'anomalies à l'aide d'Operations Analytics - Predictive Insights», à la page 1143.

Graphique Récapitulatif de la gravité de l'événement (%)

- Le graphique Récapitulatif de la gravité de l'événement présente les pourcentages de statut d'événement Critique, Avertissement et Normal. Par exemple, 

indique que 50 % des événements sont générés par des seuils de gravité Mineur ou Avertissement et 50 % des événements par des seuils de gravité Fatal ou Critique.
- Le nombre total d'événements est indiqué, ainsi que le nombre d'événements pour chaque niveau de statut.
- Le nombre d'événements inclut toutes les anomalies détectées par Operations Analytics - Predictive Insights. Par exemple, un total de "8 dont 1 anomalie" signifie qu'il existe 7 événements de seuil et 1 événement d'anomalie.

Tableau des événements

- Le tableau des événements ouverts et des statuts est défini par l'élément de navigateur sélectionné : application, groupe, sous-groupe ou instance.
- Les événements sont triés dans la colonne **Gravité**, en commençant par la gravité la plus élevée. Cliquez sur un en-tête de colonne pour modifier l'ordre de tri.
- Chaque ligne fournit les informations suivantes sur l'événement :

  Nom du seuil
  Nom qui a été attribué au seuil.

  V6-V7 Nom qui a été attribué à la situation.

  Statut
  Statut de l'événement, par exemple **Ouvert**.

  Gravité
  Valeur de gravité de l'événement : Critique (s'applique aux gravités de génération d'événement Fatal et Critique), Avertissement (s'applique aux gravités de seuil de génération d'événement Mineur et Avertissement ou Normal (s'applique aux gravités de seuil Inconnu ; pour les événements Tivoli Monitoring, s'applique aux niveaux de gravité Sans conséquences, Information et Inconnu).

  Le statut Inconnu indique que le système géré est hors ligne. Après avoir passé 4 jours hors ligne, le système géré est supprimé de toutes les applications et n'apparaît plus dans les tableaux de bord. (Pour vérifier le statut, arrêter et démarrer un agent, voir «Utilisation des commandes de l'agent», à la page 181.)

Lorsque votre environnement géré inclut IBM Operations Analytics - Predictive Insights, l'analyse appliquée aux données d'historique peut détecter une anomalie et ouvrir un événement. Un événement ouvert pour une anomalie détectée est indiqué par une icône recouvrant l'indicateur de statut, comme l'  . Cliquez sur le lien **Afficher l'analyse des anomalies** pour ouvrir la vue Predictive Insights **Service Diagnosis** dans un nouvel onglet ou une nouvelle fenêtre de navigateur. Utilisez la vue **Service Diagnosis** pour examiner tout comportement anormal dans les composants qui prennent en charge l'application.

Elément affiché
S'applique uniquement à des ensembles de données à plusieurs lignes. L'élément d'affichage est un attribut clé qui a été sélectionné pour le seuil afin de différencier les événements qui ont été ouverts pour le même système géré.

Source
Nom d'hôte du système ou autre nom dérivé de l'agent de surveillance qui identifie la source de l'événement.

Horodatage
Date et heure de survenue de l'événement ou d'observation de la condition par l'agent émetteur, exprimées dans le fuseau horaire de l'utilisateur de la console Cloud APM.

Si un agent est redémarré ou si les définitions de seuil sont modifiées pour un agent, les événements échantillonnés de l'agent sont fermés et rouverts si la condition de seuil est toujours vraie. Dans ces scénarios, la valeur `Horodatage` est mise à jour pour indiquer l'heure à laquelle l'agent émetteur a rouvert l'événement.

Pour les événements purs, un nouvel événement est ouvert par l'agent et remplace l'instance d'événement précédente chaque fois que l'agent émetteur détermine que la condition de seuil est vraie. Un événement pur reste ouvert pendant 24 heures (ou un nombre d'heures configurable) après la dernière évaluation de la condition de seuil comme vraie. Seule l'instance la plus récente d'un événement pur est affichée sur la console Cloud APM.

Description
Description éventuelle du seuil.

- Cliquez sur une ligne pour développer les détails relatifs à l'événement :

Noeud
Nom du système géré de l'instance de noeud.

Pour les agents possédant des sous-noeuds, l'option **`Activer les événements sous-noeud`** contrôle si les sous-noeuds sont affichés, ou non. Pour plus d'informations, voir «Intégration de l'interface utilisateur», à la page 1104.

ID seuil
Identificateur de seuil.

Horodatage global
Date et heure auxquelles serveur Cloud APM a reçu l'événement de l'agent émetteur, exprimées dans le fuseau horaire de l'utilisateur de la console Cloud APM.

Type
Indique si l'événement est pur ou échantillonné. Les événements purs sont des notifications non sollicitées. Aucun intervalle d'échantillonnage n'est défini pour les seuils des événements purs et il n'est pas possible de surveiller les valeurs en cours d'une mesure constante.

Description
Description éventuelle du seuil.

Formule
Formule telle qu'elle est écrite dans l'éditeur de seuil. Par exemple, `Percent Failed > 10.000 AND Transaction Definition Name != 'Ignore_Resources'`.

si la fonction de Personnalisation de l'attribut EIF a été utilisée pour personnaliser la valeur de l'attribut de base **`msg`**, la valeur personnalisée de l'attribut **`msg`** s'affiche à la place de la formule de seuil. Pour plus d'informations, voir «Acheminer l'événement de fonction d'intégration

d'événements ?», à la page 1015 sous la rubrique Gestionnaire de seuils et «Personnalisation d'un événement à transmettre à un récepteur EIF», à la page 1019.

Vous pouvez sélectionner et développer d'autres lignes, ou cliquer de nouveau pour réduire une ligne. Tandis qu'une ligne est développée, vous pouvez effectuer une exploration en aval vers les tableaux de bord du système géré qui peuvent vous aider à déterminer la cause de l'événement.

Recherche d'anomalies à l'aide d'Operations Analytics - Predictive Insights

IBM Cloud Application Performance Management uniquement :Si votre environnement géré inclut IBM Operations Analytics - Predictive Insights, l'analyse appliquée aux données d'historique peut détecter les anomalies et ouvrir des événements. Le Tableau de bord d'Application Performance permet de localiser et de visualiser les anomalies détectées par Operations Analytics - Predictive Insights.

Avant de commencer

Operations Analytics - Predictive Insights doit être intégré à votre environnement Cloud APM pour que vous soyez alerté des anomalies dans le Tableau de bord d'Application Performance. Pour plus d'informations, voir «Intégration à Operations Analytics - Predictive Insights», à la page 997.

Pourquoi et quand exécuter cette tâche

Le Tableau de bord d'Application Performance présente le récapitulatif de statut des applications dans vos domaines ainsi que leurs systèmes gérés de composant. Les indicateurs de statut d'événement des zones récapitulatives du tableau de bord **Toutes mes applications** présentent des gravités de niveau Critique, Avertissement et Inconnu. Si les événements incluent des anomalies détectées par Operations Analytics - Predictive Insights, l'indicateur de statut inclut une icône d'anomalie : , ou . Cet indicateur, identique pour les anomalies d'avertissement et pour les anomalies critiques, apparaît à côté du titre de l'onglet d'**Evénements** à mesure que vous descendez dans la hiérarchie jusqu'aux pages de tableau de bord d'application, de groupe et d'instance : Events 2. Pour accéder à une démonstration pratique, démarrez la Démonstration guidée du produit IBM Cloud Application Performance Management, faites défiler le contenu de l'écran jusqu'à la liste des tâches, puis sélectionnez *Identify & Diagnose Predictive Insights Anomalies*.

Procédure

Pour identifier des anomalies et les afficher dans la vue Operations Analytics - Predictive Insights **Service Diagnosis** :

1. Cliquez sur **Performance** > **Tableau de bord d'Application Performance** pour ouvrir le tableau de bord **Toutes mes applications**.
2. Si une zone récapitulative contient un indicateur de statut **Evénements** qui présente une icône d'anomalie, cliquez sur le lien **Evénements**.

   Le tableau de bord de l'application s'ouvre dans l'onglet **Evénements**. Le **Récapitulatif de la gravité de l'événement** indique le nombre total d'événements, y compris le nombre d'anomalies.
3. Cliquez sur une ligne de table contenant un événement d'anomalie qui est indiqué dans la colonne **Gravité** par , ou .

   La ligne se développe pour afficher les détails d'événement.
4. Cliquez sur **Afficher l'analyse des anomalies** pour ouvrir la vue Operations Analytics - Predictive Insights **Service Diagnosis** dans un nouvel onglet ou une nouvelle fenêtre de navigateur.

Que faire ensuite

- Utilisez la vue **Service Diagnosis** pour examiner tout comportement anormal dans les composants qui prennent en charge l'application. Cliquez sur pour ouvrir l'aide en ligne pour la vue **Service Diagnosis**.
- Revenez au tableau de bord de l'application et recherchez d'autres événements sur le système géré pouvant indiquer un problème associé. Cliquez sur l'onglet **Présentation des statuts** et accédez à l'instance du système géré sur laquelle l'événement s'est produit pour procéder à une recherche plus

approfondie. Utilisez les informations pour déterminer quelles actions doivent être prises pour éviter les problèmes identifiés par Predictive Insights.

- Si vous vous attendez à voir des anomalies mais qu'aucune n'est affichée, le temps de formation d'Operations Analytics - Predictive Insights est peut-être insuffisant pour produire des anomalies. Deux semaines est le temps de formation standard. Il est également possible qu'une configuration supplémentaire soit nécessaire.

Vues personnalisées

Utilisez la vue Vue universelle d'IBM Cloud Application Business Insights pour améliorer la valeur que les pages du Tableau de bord d'Application Performance prédéfinies fournissent déjà en personnalisant vos propres pages.

La Vue universelle peut servir à afficher les données de surveillance des ressources. Elle ne permet pas d'afficher les données de transaction synthétique, les données de suivi des transactions, les données d'agent de temps de réponse et les données de diagnostic d'analyse approfondie. A l'aide de la Vue universelle, vous pouvez générer rapidement des pages de surveillance pour une application et les sauvegarder à des fins d'affichage. Pendant que vous visualisez une page de tableau de bord personnalisée enregistrée, vous pouvez consulter le tableau de bord en mode actualisation automatique, l'exporter en fichier de données brutes, l'éditer ou le supprimer.

Les quatre rôles par défaut dans Cloud APM, Administrateur de rôles, Administrateur de surveillance, Administrateur système et Utilisateur de surveillance disposent de droits différents concernant l'affichage et la modification des pages de tableau de bord. Pour plus d'informations, voir Tableau 1. Rôles et autorisations .

Les options disponibles dans l'onglet **Vues personnalisées** varient selon que la page est modifiée ou affichée.

Création et gestion de pages personnalisées

Utilisez l'onglet Vues personnalisées afin de créer ou d'éditer des pages de tableau de bord pour une application, un groupe ou une instance sélectionné en ajoutant ou en mettant à jour des widgets alimentés avec les mesures de ressource de votre choix.

Pourquoi et quand exécuter cette tâche

Les pages que vous créez et que vous enregistrez sont associées à l'application sélectionnée. Par exemple, l'application Inventory Management dans Cloud APM Démonstration guidée possède les agents de surveillance suivants : Linux OS, MySQL, Node.js, Hadoop et Ruby. Vous pouvez créer et sauvegarder une page personnalisée à n'importe quel niveau du navigateur allant de l'application à l'instance, puis l'ouvrir au niveau où elle a été créée. Une page créée à un niveau particulier ne peut être ouverte qu'au même niveau. Les mesures disponibles pour les widgets peuvent être des ressources, quelles qu'elles soient, de l'application. A l'aide de l'exemple Inventory Management, vous pouvez créer une page avec une table à partir de l'Agent Ruby, un graphique à partir de l'Linux OS, etc.

Procédure

Les pages que vous créez et que vous enregistrez sont associées à l'application sélectionnée. Pour créer et personnaliser une page de tableau de bord, procédez comme suit :

1. Après avoir ouvert le Tableau de bord d'Application Performance à partir du menu **Performance**, sélectionnez une application.

   L'onglet **Vues personnalisées** s'affiche après **Présentation du statut** et **Evénements**. Vous pouvez également explorer en aval jusqu'au groupe, sous-groupe ou niveau d'instance du navigateur.
2. Cliquez sur l'onglet **Vues personnalisées**.

   L'onglet affiche la fenêtre de **sélection d'un modèle pour votre page personnalisée** ou la page par défaut si cette dernière est déjà définie.

- Si la fenêtre de **sélection d'un modèle pour votre page personnalisée** s'ouvre, passez à l'étape 4.
- Si la page par défaut est affichée, passez à l'étape 3.

3. Cliquez sur  **Ajouter** pour créer une page.
4. Cliquez sur un modèle parmi les options de modèle par défaut suivantes :
   - Modèle 1x1
   - Modèle 1x2
   - Modèle 2x2
   - Modèle 2x3
   - Modèle 3x3
   - Modèle 3x2
   - Modèle 2x1
   - Modèle 1x3
   - Modèle 3x1

   Si vous cliquez sur **Précédent**, la page marquée comme favori ou la première page de la liste s'ouvre. S'il n'existe aucune page, la fenêtre de **sélection d'un modèle pour votre page personnalisée** s'ouvre.
5. Personnalisez le modèle. Pour plus de détails, voir Personnalisation des modèles.
6. Créez un widget. Pour plus de détails, voir «Définition des propriétés de widget», à la page 1148.
7. Cliquez sur  **Set Default Timeframe for the page** et définissez la durée de conservation par défaut des données de la page sur 1, 2, 4, 12 ou 24 heures.
8. Lorsque vous êtes prêt à sauvegarder la page, procédez comme suit :
   a) Dans la zone **Nom de page**, entrez un nom de page.

      Important : Les espaces, les traits de soulignement (_) et les tirets (-) sont autorisés dans la zone **Nom de page**. Les tirets suivis d'un trait de soulignement (-_) ne sont toutefois pas autorisés. Par exemple, `System-_Overview` n'est pas autorisé.

   b) Cliquez sur **Sauvegarder**.

      Les modifications suivantes peuvent être effectuées sur le tableau de bord ou un message peut s'afficher :

      - Le message `Tableau de bord enregistré` est affiché.
      - Si ***** est sélectionné dans **Set Conditions**, le message suivant s'affiche :

        ```
        You selected * in Resource Instance or in Set Conditions, which will
        result in a large number of data series (such as lines on a graph). The
        large number of data series can make the page readability or performance
        unusable. The advisable limit for this chart is 50 data series. Adding
        specific values helps to narrow the data within recommended limits and
        results in a better user experience.
        ```

      - Un indicateur rouge s'affiche sur l'icône  pour indiquer que le type de graphique n'est pas sélectionné et que vous devez le sélectionner.
      - Un indicateur rouge s'affiche sur l'icône  pour indiquer que Select Metric n'est pas sélectionné et que vous devez le sélectionner ; le message suivant s'affiche ensuite :

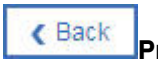
        ```
        A metric must be saved to save a chart.
        ```

9. Sélectionnez l'une des options suivantes dans la barre de titre de la page :

Option	Description

Retrieve latest resource Metric Types	Cliquez sur cette icône pour actualiser les types de mesure. Si le type de mesure ou la mesure a changé lorsqu'un correctif d'agent est appliqué, vous devez actualiser les types de mesure.
	L'intervalle entre deux actualisations est limité à 15 minutes. Si vous cliquez sur **Retrieve latest resource Metric Types** moins de 15 minutes après la dernière actualisation, le message suivant s'affiche :
	`Metadata cache was refreshed recently.`
	`Please wait for` *`time_remaining`* `minute(s) to reload it.`
	Lors du chargement des métadonnées, une image de chargement s'affiche.
	Lorsque les métadonnées sont chargées, le message suivant s'affiche :
	`Metadata Cache reloaded successfully.`
	Si l'actualisation des métadonnées prend plus de 30 secondes, le message suivant s'affiche :
	`Reloading of Metadata cache might take some more time.`
	`Do you want to wait until it is done?`
	Vous pouvez cliquer sur **Ok** ou sur **Annuler**.

Afficher le tableau de bord	Cliquez sur cette icône pour afficher les données dans le tableau de bord. **Important :** Le nombre limite de lignes renvoyées par définition de données est de 11 000 lignes. Par défaut, les données les plus récentes s'affichent lorsque la limite est dépassée. Pour un volume de données important, les données ne s'affichent pas toutes pour l'intervalle sélectionné. Par exemple, si vous choisissez de visualiser les données de ces dernières 24 heures pour une source de données dont le volume est élevé, seules les données de ces 6 dernières heures peuvent s'afficher si la limite de 11 000 lignes est atteinte. Si dans un graphique, la série de données dépasse 50, le message suivant s'affiche dans le widget : `This chart cannot be loaded because the number of data series (such as lines on a graph) exceeds 50. The number of data series is currently` *`current_data_series`*`. You can reduce the number by selecting fewer metrics or resources instances, or by refining the Conditions per Metric. For more information, see Defining widget properties: for Cloud APM -` http://ibm.biz/widgetprops `and for Cloud APM Private -` http://ibm.biz/widgetprops-private Si le chargement d'un graphique prend plus de 30 secondes, le message suivant s'affiche dans le widget : `This chart took too long to load because of a large amount of data, long network latency, or connectivity issue. Reduce the number of Resource Instances or refine the Conditions per Metric to narrow down the data. For more information, see Defining widget properties: for Cloud APM -` http://ibm.biz/widgetprops `and for Cloud APM Private -` http://ibm.biz/widgetprops-private

Option	Description
Enregistrer sous	Cliquez sur la flèche en regard de l'option **Enregistrer**, puis sur **Enregistrer sous** et spécifiez un nom différent dans la zone **Nom de page** pour sauvegarder la page avec un nom différent. **Important :** Si vous spécifiez un nom de page identique à celui d'une page existante, cette dernière est écrasée.
 **Supprimer**	Cliquez sur cette icône pour supprimer la page actuelle.
 **Précédent**	Cliquez sur cette icône pour retourner à la page précédente ou à la page favorite.

Que faire ensuite
Affichez les pages personnalisées comme décrit dans la rubrique «Affichage de pages personnalisées», à la page 1151.

Personnalisation des modèles
Vous pouvez personnaliser le modèle en redimensionnant, déplaçant ou ajoutant des marques de réservation de widget en fonction de vos besoins.

Pourquoi et quand exécuter cette tâche

A faire : Vous pouvez personnaliser un modèle existant et l'utiliser. Le modèle personnalisé ne peut toutefois pas être sauvegardé pour être utilisé ultérieurement dans le but de créer des tableaux de bord.

Procédure

1. Dans l'onglet Vues personnalisées, cliquez sur  **Editer modèle**.
2. Sélectionnez une marque de réservation de widget.
   Vous pouvez redimensionner une marque de réservation de widget de tous les côtés et la faire glisser vers un autre emplacement. Si les widgets se chevauchent pendant que vous les redimensionnez ou que vous les faites glisser, le message `Opération de redimensionnement non valide` ou `Opération de déplacement non valide` est affiché.
3. Pour ajouter une marque de réservation pour le widget à un modèle existant, procédez comme suit :
   a) Cliquez sur **Régler la hauteur de page** dans les options de menu, puis indiquez une valeur plus élevée pour le nombre de lignes et cliquez n'importe où en dehors du menu pour augmenter la hauteur de la page.
   b) Indiquez une marque de réservation pour le widget en fonction de vos besoins dans la zone vide de la page en positionnant et en déplaçant le pointeur pour créer une zone.
4. Utilisez les options de menu suivantes pour effectuer différentes opérations sur le modèle :

Option	Description
Annuler	Permet d'annuler la dernière action.
Rétablir	Permet de rétablir la dernière action.
Désélectionner la case sélectionnée	Pour supprimer un widget, sélectionnez-le et cliquez sur l'icône **Désélectionner la case sélectionnée**.
Réinitialiser	Permet de créer un modèle vide. Pour spécifier une marque de réservation de widget sur le modèle vide, placez le pointeur dans la zone Glisser les modèles ici et faites-le glisser pour créer une zone. Vous pouvez créer des marques de

Option	Description
	réservation de widget de différentes tailles dans la zone Glisser les modèles ici. Les marques de réservation peuvent être déplacées ou redimensionnées, mais elles ne peuvent pas se chevaucher.
Régler la hauteur de page	Permet de définir la hauteur de la page. Vous pouvez spécifier entre 20 et 120 lignes.

5. Cliquez sur **Editer modèle** pour utiliser le modèle créé.

Que faire ensuite
Créez le widget. Passez à l'étape 6 de la rubrique Création et gestion de pages personnalisées.

Définition des propriétés de widget
Définissez les différentes propriétés des widgets, telles que les mesures et les graphiques pour afficher les données en temps réel dans les widgets.

Procédure

Pour définir les propriétés d'un widget, procédez comme suit :

1. Dans un widget, cliquez sur afin de sélectionner un type de graphique pour afficher les données.
   - Linéaire
   - A aires
   - A barres
   - Grille

   Important : Pour les graphiques linéaires, à aires et à barres, s'il existe plus de neuf légendes, la couleur du graphique se répète après la neuvième. La couleur du graphique est la même pour la 1ère et la 10ème légende, la 2ème et la 11ème légende, etc.

   Un indicateur vert s'affiche sur l'icône pour indiquer que le type de graphique est sélectionné.
2. Spécifiez les propriétés de graphique suivantes pour les graphiques linéaires, à aires et à barres :
   - Libellé de l'axe des X
   - Libellé de l'axe des Y
   - Afficher la légende
   - Show Interpolation : données collectées à représenter sur le graphique, qui peuvent inclure des valeurs Null. Par conséquent, lorsque le graphique est tracé, sa ligne est déconnectée si elle rencontre une valeur Null et plusieurs lignes déconnectées apparaissent dans le graphique. Si vous sélectionnez l'interpolation, en présence d'une valeur Null, la ligne ne semble pas déconnectée sur le graphique. Au lieu de cela, elle est connectée à la prochaine valeur valide disponible. Dans ce cas, vous obtenez donc une seule ligne de graphique connectée.

     Remarque : Pour APM version 8.1.4.0 IF0005 et les versions ultérieures, les graphiques à courbes et à aires n'affichent plus de lignes déconnectées pour les valeurs null. Par conséquent, la fonction Show Interpolation n'est plus requise et n'est donc plus prise en charge.

   Important : La grille ne possède pas de propriétés.
3. Cliquez sur pour sélectionner le contenu des mesures.

Option	Description
Type de ressource	Dans la liste **Type de ressource**, sélectionnez une ressource. Les ressources disponibles sont associées à l'application.

Option	Description
	Si une ressource appartenant à l'application n'est pas disponible dans la liste, sa définition de ressource n'a pas été trouvée. La définition de ressource n'a pas été publiée ou le système géré n'est pas connecté au serveur Cloud APM.
Type de mesure	Dans la liste **Type de mesure**, sélectionnez un jeu de données à inclure dans le widget.
Métrique	Dans la liste **Métrique**, sélectionnez un attribut à inclure dans la vue. Les attributs disponibles sont issus du fichier sélectionné. Pour sélectionner des mesures, procédez comme suit : a. Cliquez sur la liste **Métrique**. Une fenêtre en incrustation, dans laquelle les mesures sont classées par ordre alphabétique croissant, s'ouvre. b. Sélectionnez un ou plusieurs attributs répertoriés sous Metrics ou cliquez sur **Select All**. **Remarque :** Lorsque vous cliquez sur **Select All**, toutes les mesures de la liste sont sélectionnées. c. Cliquez sur  pour ajouter les mesures sous la liste **Selected Metrics**. d. Pour supprimer une mesure sous **Selected Metrics**, cliquez sur  . e. Cliquez sur la liste **Resource Instance** pour fermer la fenêtre en incrustation. **Important :** Pour les graphiques linéaires, à aires et à barres, la mesure contenant la valeur numérique doit être sélectionnée. Les mesures contenant des valeurs de chaîne ne peuvent pas être affichées dans ces graphiques. **Conseil :** Pour la grille, sélectionnez les mesures en fonction de la sortie qui s'adapte le mieux à votre visibilité sur l'interface utilisateur.
Instance de ressource	Initialement, la sélection est définie sur *, qui extrait les mesures de toutes les instances de la liste. Conservez la valeur par défaut ou sélectionnez l'instance dans la liste. **Important :** Si vous sélectionnez une instance, ce widget ne peut pas être utilisé pour afficher les données d'un autre agent ou d'une autre instance. Il est toutefois judicieux de préciser l'instance afin d'éviter le traitement de gros volumes de données.
Définir une condition pour le groupe de mesures	Si le **type de mesure** sélectionné comporte plusieurs éléments, tels que des UC ou des disques, l'option de **définition de condition pour le groupe de mesures** affiche d'autres éléments que vous pouvez sélectionner à partir de la zone **WHERE**. **Important :** Indiquez des valeurs pour les éléments dans la zone **WHERE**. Evitez d'indiquer ***** afin de réduire le traitement de gros volumes de données. Par défaut, la condition WHERE affiche les données de ces 4 dernières heures. Cet intervalle de temps peut être redéfini sur une valeur comprise entre 1 et 24 heures par l'administrateur système ; voir

Option	Description
	«Modification de l'intervalle de temps pour les données de condition WHERE», à la page 1150.
Actions	Cliquez sur **Sauvegarder** pour sauvegarder une mesure.
	Cliquez sur **Editer** pour éditer une mesure.
	Cliquez sur **Supprimer** pour supprimer une mesure.

4. Pour ajouter une autre mesure, cliquez sur **+ Ajouter une autre mesure**.

   Important : Non applicable à la grille.
5. Fermez la fenêtre **Sélectionner des mesures** une fois que toutes les mesures ont été ajoutées.

   Toutes les mesures sont sauvegardées automatiquement une fois que vous avez fermé la fenêtre **Sélectionner des mesures**.

   Les modifications suivantes peuvent être effectuées sur le tableau de bord ou un message peut s'afficher :

   - Si ***** est sélectionné dans la liste **Resource Instance** de n'importe quelle mesure, le message suivant s'affiche :

     ```
     You selected * in Resource Instance or in Set Conditions, which will result
     in a large number of data series (such as lines on a graph). The large
     number of data series can make the page readability or performance
     unusable. The advisable limit for this chart is 50 data series. Adding
     specific values helps to narrow the data within recommended limits and
     results in a better user experience.
     ```

   - Un indicateur vert s'affiche sur l'icône pour indiquer que les mesures sont correctement sélectionnées pour limiter les données conformément aux valeurs recommandées.

   - Un indicateur orange s'affiche sur l'icône pour indiquer que les mesures ne sont pas correctement sélectionnées pour limiter les données conformément aux valeurs recommandées. Le symbole ***** est sélectionné dans **Resource Instance** ou **Set Conditions**.

6. Cliquez sur pour entrer le titre du widget.

   Si le titre du widget n'est pas ajouté, le premier nom de mesure est affecté automatiquement comme titre de widget.

Que faire ensuite

De la même manière, ajoutez des graphiques, des mesures et des titres à tous les widgets, puis passez à l'étape 7 de la rubrique Création et gestion de pages personnalisées.

Modification de l'intervalle de temps pour les données de condition WHERE

L'intervalle de temps peut être redéfini sur une valeur comprise entre 1 et 24 heures par l'administrateur système.

Procédure

Pour modifier l'intervalle de temps, l'administrateur système peut procéder comme suit :

1. Se connecter au serveur APM sur lequel l'édition est déployée.
2. Sur la ligne de commande, exécuter les commandes suivantes :

   ```
   export CLASSPATH=$CLASSPATH:/rép_install/gaian/lib/derbytools.jar:
   ```

```
export CLASSPATH=$CLASSPATH:/rép_install/gaian/lib/derbyclient.jar:
export CLASSPATH=$CLASSPATH:/rép_install/gaian/lib/derby.jar:
java org.apache.derby.tools.ij
connect 'jdbc:derby://localhost:port/
gaiandb;user=gaiandb;password=mot_passe_bd_gaian;';
```

Dans ces commandes, *rép_install* correspond au répertoire dans lequel APM a été déployé ; il s'agit de `/opt/ibm` par défaut. Dans la commande **connect**, *port* correspond à la valeur du port sur lequel la base de données est configurée et *mot_passe_bd_gaian* est le mot de passe de la base de données Gaian. Pour ce mot de passe, prenez contact avec le support IBM.

3. Une fois la base de données connectée, exécutez la requête suivante pour modifier les valeurs de l'intervalle :

   ```
   UPDATE "OED_TOOL"."PREFERENCETABLE" SET PREFERENCES='-24H' WHERE
   FIELD='TIMEINTERVAL';

   Commit;

   Exit;
   ```

   La valeur de l'intervalle est exprimée sous la forme `SET PREFERENCES='-24H'`. Elle peut être redéfinie sur une valeur comprise entre 1H et 24H.

Affichage de pages personnalisées

Après avoir créé et sauvegardé des pages de tableau de bord pour une application, un groupe, un sous-groupe ou une instance dans l'onglet **Vues personnalisées**, vous pouvez les visualiser à tout moment. Certaines des options que vous pouvez sélectionner incluent l'actualisation de la page, la sélection d'intervalles de temps différents, l'édition de la page pour extraire les données de diverses sources et l'exportation du tableau de bord sous forme de fichier de données brutes.

Procédure

Procédez comme suit pour afficher une page sauvegardée dans l'onglet **Vues personnalisées** du tableau de bord.

1. Après avoir ouvert le Tableau de bord d'Application Performance à partir du menu **Performance**, sélectionnez une application.

   L'onglet **Vues personnalisées** s'affiche après **Présentation du statut** et **Evénements**. Vous pouvez également explorer en aval jusqu'au groupe, sous-groupe ou niveau d'instance du navigateur.
2. Sélectionnez l'onglet **Vues personnalisées**.

   L'onglet affiche la fenêtre de **sélection d'un modèle pour votre page personnalisée** ou la page par défaut si cette dernière est déjà définie.
3. Cliquez sur dans la liste des pages et sélectionnez l'une des pages sauvegardées de la liste.

   Les pages disponibles ont été sauvegardées par vous ou ont été partagées par un autre utilisateur.

   Une fois que vous avez sélectionné une page sauvegardée, les échantillons de données historique et actuel sont rapportés dans la page.
4. Sélectionnez l'une des options d'affichage dans la barre de titre de la page :

Option	Description
Actualiser	Indique que l'actualisation automatique est désactivée. Cliquez dessus pour l'activer.
Actualiser	Indique que l'actualisation automatique est activée. Cliquez dessus pour la désactiver. **Important :** Le délai d'actualisation par défaut est 1 minute.

Option	Description
Exporter > Données brutes	Cliquez sur cette icône pour exporter la page au format DAT. Comme plusieurs fichiers DAT sont exportés, ils sont téléchargés sur votre ordinateur au format ZIP. **A faire :** Si le fichier téléchargé est dépourvu d'extension, ajoutez-lui l'extension zip. **Important :** Si le fichier n'est pas téléchargé sur votre ordinateur, vérifiez si l'option Bloquer les fenêtres publicitaires intempestives est activée. Vous pouvez ajouter ce site à votre liste d'exceptions. Procédez à l'extraction du fichier zip téléchargé (les fichiers extraits sont des fichiers en texte clair). Ce fichier contient le nom de la page, la durée, les filtres, la date, l'heure, l'intervalle, le titre du graphique et les données. Le délimiteur de données est la barre verticale. Vous pouvez ouvrir les fichiers DAT à l'aide de l'éditeur approprié ou importer des fichiers dans Excel en indiquant les séparateurs de valeurs appropriés.
Exporter > PDF	Cliquez sur cette icône pour exporter la page au format PDF. Le fichier contient le nom de la page, l'intervalle de temps, les widgets, le nom du créateur et la date de création du rapport.
Editer	Cliquez sur cette icône pour éditer la page actuelle. Vous pouvez modifier les graphiques et les métriques dans les widgets, ajouter de nouveaux widgets, modifier la période par défaut de la page ou modifier le nom de cette dernière.
Supprimer	Cliquez sur cette icône pour supprimer la page actuelle.
Ajouter	Cliquez dessus pour créer une page. Pour personnaliser la page et l'enregistrer, voir «Création et gestion de pages personnalisées», à la page 1144.

5. Sélectionnez l'une des options d'affichage suivantes dans le widget :

Option	Description
Type de graphique	Cliquez sur l'icône **Type de graphique** et sélectionnez une option appropriée dans la liste pour modifier le type de graphique existant. • Pour les graphiques à courbes et à aires, les options **Courbes** et **Aires** sont disponibles. • Pour le graphique à barres, les options **Barres groupées** et **Histogramme groupé** sont disponibles. **Important :** Pour le quadrillage, il n'existe aucune option de type de graphique. Pour les données affichées dans une grille, vous pouvez filtrer les données comme suit : a. Cliquez sur **Définir un filtre**. La fenêtre **Filtrer** s'ouvre.

Option	Description
	b. Spécifiez des valeurs pour **Colonne**, **Condition** et **Valeur** pour ajouter une règle de filtrage. **Remarque :** Vous pouvez filtrer des valeurs numériques et des valeurs texte en sélectionnant les conditions appropriées. c. Cliquez sur  **Ajouter une règle de filtrage** pour ajouter une autre règle de filtrage. Vous pouvez ajouter plusieurs règles de filtrage. d. Dans la zone **Correspondance**, sélectionnez **All rules** ou **Any rule** pour filtrer les données. Vous pouvez sélectionner **Respecter la casse** si vous souhaitez effectuer une recherche en fonction de la casse du texte que vous spécifiez dans la zone **Valeur**. e. Cliquez sur **Filtre** pour filtrer les données affichées dans la grille. f. Cliquez sur **Effacer le filtre** pour effacer les résultats du filtrage. g. Cliquez sur **Annuler** pour fermer la fenêtre **Filtrer**.
 **Réduire**	Cliquez sur cette icône pour réduire le widget.
 **Développer**	Cliquez sur cette icône pour développer le widget.
 **Agrandir**	Cliquez sur cette icône pour agrandir le widget à la taille de la page.
 **Restaurer**	Cliquez sur cette icône pour restaurer la taille d'origine du widget.
Légendes	Le widget contient des cases à cocher pour chaque métrique. Cochez ou décochez des cases pour chaque métrique afin d'afficher les données d'une ou plusieurs métriques.

6. Vous pouvez filtrer les données sur la page à l'aide des listes **Date**, **Heure** et **Intervalle**. Vous pouvez également définir un filtre personnalisé pour que la page affiche les données correspondant à la date et aux intervalles sélectionnés. Pour utiliser un filtre personnalisé, dans la liste **Intervalle**, sélectionnez **Custom**, puis, dans la fenêtre **Time Period Selection**, sélectionnez la date et l'heure requises.

   Remarque :

   - L'option de filtre personnalisé est disponible à partir d'APM V8.1.4.0 IF0005. Les pages créées à l'aide de versions précédentes de Cloud APM n'affichent pas l'option de filtre personnalisé.
   - Utilisez un filtre personnalisé pour filtrer les données sur un intervalle minimal d'une minute et un intervalle maximal de 24 heures.
   - Lorsque vous appliquez un filtre personnalisé, dans la fenêtre **Time Period Selection**, si vous cliquez sur **Annuler**, dans la page du tableau de bord, la liste **Intervalle** n'affiche pas l'intervalle que vous avez appliqué précédemment.
   - Si vous appliquez un filtre personnalisé sur une page, les données de cette page ne sont pas actualisées automatiquement.

7. Pour définir une page par défaut, cliquez sur dans la liste de pages, puis cliquez sur  **Favoris** en regard du nom de la page à définir comme page par défaut.

Utilitaires de tableau de bord

Utilisez les options disponibles pour gérer l'apparence et le comportement des pages du **Tableau de bord d'Application Performance**.

Copie de l'URL du tableau de bord

Une fois que vous avez accédé à un emplacement dans votre hiérarchie d'applications, l'URL figurant dans la zone d'adresse du navigateur ne change pas pour la nouvelle vue. Vous pouvez copier l'URL de la page Tableau de bord d'Application Performance que vous affichez. Collez l'URL dans une nouvelle fenêtre de navigateur pour ouvrir la page de tableau de bord ou utilisez l'URL pour accéder au tableau de bord plus tard ou pour le partager avec d'autres utilisateurs.

Procédure

1. Accédez à la page Tableau de bord d'Application Performance que vous voulez mémoriser.
2. Cliquez sur **Actions** > **Copier URL**.
3. Cliquez avec le bouton droit de la souris sur le lien hypertexte **Lien vers la page en cours** et sélectionnez l'option qui permet de copier l'URL.

Que faire ensuite

Conservez une copie de l'URL ou partagez-la avec d'autres utilisateurs dans votre environnement géré. Une fois que vous collez l'URL dans la zone d'adresse de votre navigateur, la page de tableau de bord cible s'ouvre dans la console Cloud APM.

Si vous n'êtes pas connecté au serveur Cloud APM, vous êtes invité à entrer votre ID utilisateur et votre mot de passe avant que la page de tableau de bord cible puisse être affichée. Si la page **Mise en route** s'ouvre à la place de la page de tableau de bord, appuyez sur F5 ou cliquez sur le bouton de barre d'outils d'actualisation du navigateur. Vous pouvez désactiver la page **Mise en route** pour des sessions de travail futures en désélectionnant la case à cocher "Afficher cette page **Mise en route** au démarrage".

Définition d'une trace

Réglez les paramètres de trace de sorte à aider votre administrateur ou le support IBM à diagnostiquer la cause des problèmes liés au Tableau de bord d'Application Performance.Plusieurs niveaux de trace sont disponibles lorsque vous utilisez le navigateur et l'onglet **Présentation des statuts**. Vous pouvez instaurer un niveau de trace détaillé au point exact de l'interface utilisateur où vous rencontrez un problème, puis revenir à un niveau de trace plus général une fois que les données de journal nécessaires ont été capturées. Par exemple, si un tableau de bord donné se comporte de manière inattendue, vous pouvez augmenter le niveau de trace avant d'ouvrir le tableau de bord pour consigner l'activité, puis ramener la consignation de trace à son niveau normal.

Pourquoi et quand exécuter cette tâche

Procédez comme suit pour définir le niveau de trace lorsque vous souhaitez augmenter ou réduire le volume de consignation de trace.

Procédure

1. Si le Tableau de bord d'Application Performance n'est pas ouvert, sélectionnez l'option **Performance** dans la barre de navigation.
2. Sélectionnez Toutes mes applications ou une application depuis le navigateur ou l'onglet Présentation des statuts.
3. Cliquez sur **Actions** > **Niveau de trace** et sélectionnez l'un des niveaux suivants :
   - **Détaillé** pour que toutes les activités soient consignées. Le niveau de trace détaillé inclut la consignation de trace de niveau Intermédiaire, Faible et Minimal.

- **Intermédiaire** pour que les modifications de variable soient consignées (par exemple, pour indiquer quels paramètres ont été transmis et quels calculs ont été effectués). Le niveau de trace Intermédiaire comprend les niveaux de consignation de trace Faible et Minimal.
- **Faible** pour consigner les erreurs et l'activité liée aux variables. Définissez ce niveau de trace si vous rencontrez un problème du type suivant : aucune donnée n'est renvoyée mais le tableau de bord continue de fonctionner. Le niveau de trace Faible comprend le niveau de consignation de trace Minimal.
- **Minimal** est le niveau par défaut où seules les erreurs irrémédiables sont enregistrées. Vous pouvez revenir au niveau de trace Minimal après la collecte d'une séquence d'activités spécifique. Quel que soit le niveau de trace défini avant la déconnexion, la trace revient toujours au niveau le plus bas lors de la connexion suivante.

4. Si vous souhaitez envoyer des enregistrements de performance dans un fichier de consignation commun, sélectionnez **Activer la consignation des statistiques de performance**.

   Les informations de performance issues de la console sont écrites sur le serveur, où elles peuvent être combinées avec des statistiques de performance de ce dernier afin de fournir le temps de réponse de transaction de bout en bout. Les informations de performance requises incluent l'heure à laquelle une fonction a été démarrée et l'heure à laquelle elle s'est terminée.

Résultats

La trace est ajustée au niveau choisi. Lors de la prochaine connexion, le niveau de trace est défini sur **Minimal** tant que vous ne le modifiez pas.

Pour réduire le trafic de communications au minimum, les messages de journal sont transférés par lots. Un transfert final est réalisé après votre déconnexion, qu'elle soit manuelle ou après un délai d'attente. (Si le navigateur rencontre un problème, aucun journal final n'est envoyé.) Le journal est enregistré sur l'ordinateur serveur sous le nom `itp.log`. Un nouveau fichier `itp.log` est créé chaque fois que le serveur est redémarré.

Si vous définissez **Activer la consignation des statistiques de performance**, des enregistrements similaires à ceux de l'exemple suivant sont enregistrés dans *rép_install*`/usr/servers/apmui/logs/itp.log` :

```
<record>
    <date>2013-10-02T10:52:46</date>
    <millis>1380736366788</millis>
    <sequence>28008</sequence>
    <level>INFO</level>
    <class>StatusItemList</class>
    <method>tracing</method>
    <thread>96</thread>
    <message>BeginTrace:onSelectApp:272wt877d05</message>
</record>
<record>
    <date>2013-10-02T10:52:46</date>
    <millis>1380736366809</millis>
    <sequence>28009</sequence>
    <level>INFO</level>
    <class>StatusItemList</class>
    <method>tracing</method>
    <thread>96</thread>
    <message>EndTrace:onSelectApp:272wt877d05</message>
</record>
```

Verrouillage de la console Cloud APM

Vous pouvez verrouiller temporairement votre session de travail sans devoir vous déconnecter de la console Cloud APM. La fonction de verrouillage de session est indisponible sur l'iPad d'Apple.

Procédure

1. Lorsque vous êtes connecté à la console Cloud APM, cliquez sur ***apmadmin*** > **Verrouiller la session** où *apmadmin* correspond à votre nom de connexion.

   L'écran de connexion s'affiche et votre session est verrouillée.

2. Pour déverrouiller votre session, entrez le mot de passe associé à votre ID utilisateur.
   Votre session de travail reprend.

Rapports

Les rapports d'historique sont disponibles dans la console Cloud APM pour les données qui sont recueillies par l'Agent de surveillance des temps de réponse, l'Agent WebSphere Applications et l'Agent Synthetic Playback.

Vous pouvez exécuter les rapports depuis le tableau de bord **Toutes mes applications**. A partir de n'importe quelle page de la console Cloud APM, cliquez sur **Performance** > **Tableau de bord d'Application Performance** pour ouvrir le tableau de bord **Toutes mes applications**.

Remarque : Lorsque vous exécutez un rapport pour la première fois, vous devez vous connecter à Tivoli Common Reporting en tant qu'utilisateur autorisé à exécuter les rapports Cloud APM. IBM Cognos Viewer est le visualiseur de sortie de rapport par défaut.

Rapports Agent de surveillance des temps de réponse

Pour afficher les rapports **Performances des applications et utilisation** ou **Comparer les performances des applications sur deux périodes**, sélectionnez une application qui inclut les systèmes gérés par l'Agent de surveillance des temps de réponse, puis sélectionnez **Actions** > **Rapports de lancement**.

Pour afficher le rapport **Toutes mes applications** ou **Comparer les performances de plusieurs applications**, sélectionnez **Toutes mes applications**, puis **Actions** > **Rapports de lancement**.

Rapports Agent WebSphere Applications

Pour afficher n'importe quel rapport de l'Agent WebSphere Applications, sélectionnez une application qui inclut les systèmes gérés par l'Agent WebSphere Applications, puis sélectionnez **Actions** > **Rapports de lancement**.

Agent Synthetic Playback

Pour afficher n'importe quel rapport de l'Agent Synthetic Playback, sélectionnez une application qui inclut les transactions synthétiques, puis **Actions** > **Rapports de lancement**.

Remarque : Si l'option **Rapports de lancement** ne se trouve pas dans le menu **Actions**, vérifiez que les rapports Cloud APM sont correctement installés.

Pour plus d'informations sur les navigateurs pris en charge pour visualiser les rapports de l'Agent Synthetic Playback, l'Agent de surveillance des temps de réponse et l'Agent WebSphere Applications, voir les Rapports de compatibilité des produits logiciels pour Cognos 10.2.1.7.

Rapports de l'Agent de surveillance des temps de réponse

Les rapports d'historique sont disponibles pour les données collectées par l'Agent de surveillance des temps de réponse. Les rapports de l'Agent de surveillance des temps de réponse sont indisponibles dans Cloud APM, Base. Ils sont uniquement disponibles dans Cloud APM, Advanced.

Deux types de rapport associés aux données collectées par l'Agent de surveillance des temps de réponse sont disponibles, à savoir les rapports actifs et les rapports simples.

Rapports actifs
Ils s'affichent dans un navigateur au format MHTML. Internet Explorer prend en charge MHTML par défaut. Pour les autres navigateurs, un plug-in de prise en charge de MHTML peut être installé. Les rapports actifs sont également appelés rapports interactifs hors ligne.

Rapports simples
Les rapports simples s'affichent dans IBM Cognos Viewer. Ce dernier est le visualiseur de sortie de rapports par défaut.

Les rapports d'historique prédéfinis suivants associés aux données collectées par l'Agent de surveillance des temps de réponse sont disponibles :

Tableau 254. Rapports d'historique prédéfinis	
Rapport	**Type**
Toutes mes applications	Rapports actifs
Performances des applications et utilisation	Rapports actifs
Comparer les performances des applications sur deux périodes	Simple
Comparer les performances de plusieurs applications	Simple

Les données des rapports sont stockées dans la base de données Db2 DATAMART. Les rapports affichent des données récapitulatives quotidiennes, hebdomadaires et mensuelles qui sont conservées pendant 26 semaines, 12 mois et 3 ans respectivement. Cloud APM ne fournit pas de scripts ni d'instructions permettant de modifier ces durées de conservation.

Pour plus d'informations sur le mappage entre les rapports de l'Agent de surveillance des temps de réponse et de Performance Management, voir Mappages des attributs de l'agent de surveillance des temps de réponse.

Rapport Toutes mes applications
Utilisez le rapport Toutes mes applications pour afficher des informations sur les unités utilisateur, le volume de données, le temps de réponse et le nombre d'erreurs.

Dans ce rapport, vous affichez des informations pour toutes les applications. Spécifiez la période du rapport **Dernier jour** (par défaut), **Semaine dernière** ou **Mois dernier**. Affichez les informations suivantes en fonction de la période sélectionnée par application :

- Graphique à colonnes empilées représentant le nombre de transactions
- Graphique à colonnes représentant le volume des données de transaction
- Graphique à colonnes représentant le temps de réponse moyen des transactions
- Graphique à colonnes empilées représentant les nombres d'erreurs

Rapport Performances des applications et utilisation
Utilisez ce rapport afin d'afficher des informations sur les performances, la disponibilité et les unités utilisateur pour des applications uniques.

Dans la fenêtre **Sélection d'une application**, sélectionnez une application. Cliquez sur **Suivant**. Dans la fenêtre de **sélection des transactions clés pour l'application**, sélectionnez les transactions en fonction desquelles vous voulez filtrer le rapport. Cliquez sur **OK**. Ce rapport se compose de trois onglets : Performances, Disponibilité et Unités. L'intervalle par défaut est semaine.

Dans l'onglet Performances, affichez les informations suivantes en fonction de l'intervalle de temps sélectionné pour l'application que vous consultez actuellement dans le tableau de bord d'Application Performance :

- Graphique à courbes représentant le temps de réponse moyen par transactions (clés)
- Graphique à courbes représentant le temps de réponse moyen des transactions par réussite, erreur de serveur et erreur de client.
- Graphique à courbes et à barres représentant le volume des données de transaction. Les barres représentent le volume des données de transaction et la courbe représente la moyenne du volume de données de transaction.
- Graphique à courbes et à barres représentant le nombre de transactions. Les barres représentent le nombre de transactions et la courbe représente les valeurs polynomiales et la moyenne mobile.

Dans l'onglet Disponibilité, affichez les informations suivantes en fonction de l'intervalle de temps sélectionné pour l'application que vous consultez actuellement dans le tableau de bord d'Application Performance :

- Graphique à barres empilées représentant le pourcentage des transactions réussies et le pourcentage des transactions ayant échoué ; les échecs sont répartis en deux catégories, les erreurs de serveur et les erreurs de client.
- Graphique à barres empilées représentant le nombre de transactions réussies et le nombre de transactions ayant échoué ; les échecs sont répartis en deux catégories, les erreurs de serveur et les erreurs de client.
- Graphique circulaire représentant les codes d'erreur les plus fréquents

Dans l'onglet Unités, affichez les informations suivantes en fonction de l'intervalle de temps sélectionné pour l'application que vous consultez actuellement dans le tableau de bord d'Application Performance :

- Graphique à barres représentant les transactions par type d'unité
- Graphique à barres représentant les transactions par système d'exploitation d'unité
- Graphique à barres représentant les transactions par navigateur d'unité
- Tableau représentant les performances des transactions par dimensions. Vous pouvez filtrer ce tableau par type d'unité, système d'exploitation d'unité, marque d'unité et navigateur d'unité.

Rapport Comparer les performances des applications sur deux périodes
Utilisez ce rapport pour examiner les performances d'une application sélectionnée.

Dans la fenêtre **Sélection de l'application et de la fréquence**, spécifiez une application et une fréquence (hebdomadaire, quotidienne, mensuelle). Dans la fenêtre **Sélection des périodes**, choisissez les périodes appropriées pour l'intervalle et cliquez sur **OK**.

Le rapport affiche les graphiques suivants pour l'application sélectionnée, pour les périodes sélectionnées, par intervalle de temps sélectionné :

- Graphique à courbes représentant le nombre de transactions pour le type d'unité
- Graphique à courbes représentant le volume des transactions
- Graphique à courbes représentant le temps de réponse moyen
- Graphique à courbes représentant le nombre d'erreurs

Rapport Comparer les performances de plusieurs applications
Utilisez ce rapport pour comparer les performances de plusieurs applications pour la même période de temps.

Dans la fenêtre **Sélection de l'application et de la fréquence**, spécifiez une application et une fréquence (hebdomadaire, quotidienne, mensuelle). Cliquez sur **Suivant**. Choisissez une période appropriée pour l'intervalle.

Le rapport affiche les graphiques suivants pour les applications sélectionnées, pour les périodes sélectionnées, par intervalle de temps sélectionné :

- Graphique à courbes représentant le nombre de transactions
- Graphique à courbes représentant le volume des données de transaction
- Graphique à courbes représentant le temps de réponse moyen
- Graphique à courbes représentant le nombre d'erreurs

Mappage des attributs de l'Agent de surveillance des temps de réponse
Certains rapports Cloud APM se basent sur les données collectées par l'Agent de surveillance des temps de réponse. Les données contenues dans ces rapports sont mappées aux attributs de l'Agent de surveillance des temps de réponse.

Le tableau suivant décrit le mappage des éléments de données dans les rapports de l'Agent de surveillance des temps de réponse aux attributs de l'agent :

Tableau 255. Mappage des attributs de l'Agent de surveillance des temps de réponse

Elément de données du rapport	Description	Nom de l'attribut ODI	Colonne du fichier ODI
Nom de l'application	Nom de l'application surveillée signalé à la console Cloud APM	Nom de l'application	T5TXCS.APPLICATIN
Nombre de transactions	Nombre total de séquences de demandes et de réponses qui sont observées par l'agent de surveillance au cours de l'intervalle d'agrégat.	Nombre total de requêtes	T5TXINS.TOTREQ
Erreurs client	Nombre de requêtes HTTP ayant le code d'état 400 - 499.	Erreurs client	T5TXCS.NUM4XX
Erreurs de serveur	Nombre de requêtes HTTP ayant le code d'état 500 - 599.	Erreurs de serveur	T5TXCS.NUM5XX
Nom de transaction	Nom de transaction signalé à Application Management Console.	Nom de transaction	T5TXCS.TRANSACTN
Statut de la transaction	Code de réponse associé à la transaction.	Code de statut	T5TXCS.STATUSCODE
Nombre de kilooctets de réponse du code	Nombre total de kilooctets dans chaque réponse de la demande au cours de l'intervalle de données.	Octets de réponse	T5TXCS.REPLYBYT
Nombre de kilooctets de demande	Nombre total de kilooctets dans la demande au cours de l'intervalle de données.	Demande ko	T5TXCS.REQBYTES
Nombre total de kilooctets	Nombre total de kilooctets transférés pour toutes les demandes au cours de la période.	Total des octets	T5TXCS.TOTBYTES
Nombre total d'objets	Nombre total d'objets imbriqués dans une page Web au cours de la période	Nombre total d'objets	T5TXCS.OBJCNT

Tableau 255. Mappage des attributs de l'Agent de surveillance des temps de réponse (suite)

Elément de données du rapport	Description	Nom de l'attribut ODI	Colonne du fichier ODI
Taille totale des objets	Taille totale de tous les objets imbriqués dans la page Web au cours de la période.	Taille totale des objets	T5TXCS.OBJSIZE
Temps de réponse (en secondes)	Nombre total de secondes nécessaires à l'exécution de la transaction serveur.	Temps de réponse	T5TXCS.RESPTIME
Temps de rendu	Délai exprimé en secondes nécessaire au rendu complet de la page Web dans le navigateur en utilisant des balises JavaScript intégrées.	Temps de rendu	T5TXCS.RENDERTIME
Temps client	Délai d'exécution moyen exprimé en secondes d'une transaction sur le client au cours de la période de surveillance en cours.	Délai client moyen	T5TXCS.CLIENTTIME
Temps de chargement	Temps moyen, en secondes, qui s'est écoulé depuis la demande de téléchargement d'un utilisateur jusqu'à la fin du téléchargement de l'objet Web.	Temps de chargement moyen	T5TXCS.LOADTIME
Navigateur	Description du navigateur Web dans lequel la page Web s'affiche.	Description du navigateur	T5TXCS.BROWSEDESC
Serveur	Nom ou adresse IP du serveur pour la Transaction TCP.	Description du serveur	T5TXCS.SERVERDESC
Nom d'hôte d'URL	Nom d'hôte TCP/IP de l'URL.	Nom d'hôte d'URL	T5TXCS.URLHOST
URL de la méthode	Méthode utilisée pour exécuter des requêtes HTTP (GET, POST, HEAD, PUT, OPTIONS, DELETE, TRACE ou CONNECT).	Méthode	T5TXCS.METHOD

Tableau 255. Mappage des attributs de l'Agent de surveillance des temps de réponse (suite)			
Elément de données du rapport	**Description**	**Nom de l'attribut ODI**	**Colonne du fichier ODI**
Détails de l'adresse URL	Chemin d'URL du fichier sur le serveur hébergeant la page Web.	Chemin de l'adresse URL	T5TXCS.URLPATH

Pour plus d'informations sur l'Agent de surveillance des temps de réponse, voir Transaction Monitoring Reference.

Génération de rapports sur l'Agent Synthetic Playback

Exécutez des rapports pour les applications associées à des transactions synthétiques.

Pourquoi et quand exécuter cette tâche

Sélectionnez une application et une transaction synthétique associée dans le Tableau de bord d'Application Performance, puis générez des rapports reposant sur votre sélection. Les données des rapports sont stockées dans la base de données Db2 DATAMART. Les rapports affichent des données récapitulatives horaires, hebdomadaires et mensuelles qui sont conservées pendant 371 jours, 53 semaines et 12 mois respectivement. Cloud APM ne fournit pas de scripts ni d'instructions permettant de modifier ces durées de conservation.

Cinq rapports de plusieurs pages sont disponibles :

Vue globale des transactions

Ce rapport de deux pages affiche les temps de réponse et les facteurs de disponibilité de la transaction synthétique sélectionnée sur une plage de dates définie.

La première page affiche les données suivantes :

- Un graphique à courbes des temps de réponse des transactions synthétiques sélectionnées à des intervalles définis sur une plage de dates définie
- Un tableau répertoriant les temps de réponse moyens, en secondes, de chaque transaction synthétique sur la plage de dates définie

La deuxième page affiche les données suivantes :

- Un graphique à courbes des facteurs de disponibilité des transactions synthétiques sélectionnées à des intervalles définis sur une plage de dates définie
- Un tableau répertoriant le facteur de disponibilité moyen de chaque transaction synthétique sur la plage de dates définie

Vous avez accès à deux rapports supplémentaires à partir du rapport **Vue globale des transactions** : **Timely Analysis by Transactions** et **HTTP Metrics by Transactions**.

Timely Analysis by Transaction affiche les indicateurs HTTP de la transaction synthétique sélectionnée à des intervalles définis sur une plage de dates définie. Le rapport comprend les éléments suivants :

- Un graphique à colonnes des indicateurs HTTP de la transaction synthétique sélectionnée à des intervalles définis sur la plage de dates définie
- Un tableau des indicateurs HTTP en millisecondes de la transaction synthétique sélectionnée sur la plage de dates définie

HTTP Metrics by Transaction affiche les indicateurs HTTP de la transaction synthétique sélectionnée à des intervalles définis sur une plage de dates définie. Le rapport comprend les éléments suivants :

- Un graphique à colonnes des indicateurs HTTP de la transaction synthétique sélectionnée à des intervalles définis sur la plage de dates définie

- Un tableau des indicateurs HTTP en millisecondes de la transaction synthétique sélectionnée sur la plage de dates définie

Transaction Detail By Locations

Ce rapport de deux pages affiche les temps de réponse et les facteurs de disponibilité par emplacement des transactions et des sous-transactions synthétiques sélectionnées sur une plage de dates définie.

La première page affiche les données suivantes :

- Des graphiques à courbes retraçant les temps de réponse, par emplacement, des transactions et sous-transactions synthétiques sélectionnées à des intervalles définis sur une plage de dates définie
- Des tableaux répertoriant les temps de réponse moyens, en secondes, de toutes les sous-transactions synthétiques sur une plage de dates définie, sur chaque emplacement

La deuxième page affiche les données suivantes :

- Des graphiques à courbes des facteurs de disponibilité, par emplacement, des transactions et sous-transactions synthétiques sélectionnées à des intervalles définis sur une plage de dates définie
- Des tableaux répertoriant les facteurs de disponibilité moyens de toutes les sous-transactions synthétiques sur une plage de dates définie, sur chaque emplacement

Vous pouvez accéder à quatre rapports supplémentaires à partir du rapport **Détails de transaction par emplacements** : **Timely Analysis by Locations of Transaction**, **HTTP Metrics by Locations of Transaction**, **Timely Analysis by Locations of Subtransaction** et **HTTP Metrics by Locations of Subtransaction**.

Timely Analysis by Locations of Transaction affiche les indicateurs HTTP d'une transaction synthétique par emplacements à des intervalles définis sur une plage de dates définie. Le rapport comprend les éléments suivants :

- Un graphique à colonnes des indicateurs HTTP de la transaction synthétique sélectionnée par emplacements à des intervalles définis sur la plage de dates définie
- Un tableau des indicateurs HTTP en millisecondes de la transaction synthétique sélectionnée par emplacements sur la plage de dates définie

HTTP Metrics by Locations of Transaction affiche les indicateurs HTTP d'une transaction synthétique par emplacements à des intervalles définis sur une plage de dates définie. Le rapport comprend les éléments suivants :

- Un graphique à colonnes des indicateurs HTTP de la transaction synthétique sélectionnée par emplacements à des intervalles définis sur la plage de dates définie
- Un tableau des indicateurs HTTP en millisecondes de la transaction synthétique sélectionnée par emplacements sur la plage de dates définie

Timely Analysis by Locations of Subtransaction affiche les indicateurs HTTP d'une sous-transaction par emplacements à des intervalles définis sur une plage de dates définie. Le rapport comprend les éléments suivants :

- Un graphique à colonnes des indicateurs HTTP de la sous-transaction sélectionnée par emplacements à des intervalles définis sur la plage de dates définie
- Un tableau des indicateurs HTTP en millisecondes de la sous-transaction sélectionnée par emplacements sur la plage de dates définie

HTTP Metrics by Locations of Subtransaction affiche les indicateurs HTTP d'une sous-transaction synthétique par emplacements à des intervalles définis sur une plage de dates définie. Le rapport comprend les éléments suivants :

- Un graphique à colonnes des indicateurs HTTP de la sous-transaction sélectionnée par emplacements à des intervalles définis sur la plage de dates définie
- Un tableau des indicateurs HTTP en millisecondes de la sous-transaction sélectionnée par emplacements sur la plage de dates définie

Transaction Detail By Subtransactions

Ce rapport de deux pages affiche les temps de réponse et les facteurs de disponibilité des sous-transactions à des intervalles définis, sur une plage de dates définie.

La première page affiche les données suivantes :

- Un graphique à courbes retraçant les temps de réponse des sous-transactions synthétiques sélectionnées à des intervalles définis sur une plage de dates définie
- Un tableau répertoriant les temps de réponse moyens, en secondes, de chaque sous-transaction synthétique sur la plage de dates définie

La deuxième page affiche les données suivantes :

- Un graphique à courbes des facteurs de disponibilité des sous-transactions synthétiques sélectionnées à des intervalles définis sur une plage de dates définie
- Un tableau répertoriant les facteurs de disponibilité de chaque sous-transaction synthétique sur la plage de dates définie

Vous avez accès à deux rapports supplémentaires à partir du rapport **Détails de transaction par sous-transactions** : **Timely Analysis by Subtransactions** et **HTTP Metrics by Subtransactions**.

Timely Analysis by Locations of Subtransaction affiche les indicateurs HTTP d'une sous-transaction par emplacements à des intervalles définis sur une plage de dates définie. Le rapport comprend les éléments suivants :

- Un graphique à colonnes des indicateurs HTTP de la sous-transaction sélectionnée à des intervalles définis sur une plage de dates définie
- Un tableau des indicateurs HTTP en millisecondes de la sous-transaction sélectionnée sur la plage de dates définie

HTTP Metrics by Locations of Subtransaction affiche les indicateurs HTTP d'une sous-transaction synthétique par emplacements à des intervalles définis sur une plage de dates définie. Le rapport comprend les éléments suivants :

- Un graphique à colonnes des indicateurs HTTP de la sous-transaction sélectionnée à des intervalles définis sur une plage de dates définie
- Un tableau des indicateurs HTTP en millisecondes de la sous-transaction sélectionnée sur la plage de dates définie

Tendance des transactions

Ce rapport de quatre pages affiche une analyse des tendances des temps de réponse, des facteurs de disponibilité et des indicateurs HTTP au cours de la semaine précédente et des cinq semaines précédentes.

La première page affiche les données de tendance pour les temps de réponse et les facteurs de disponibilité d'une transaction synthétique :

- Un graphique à courbes combiné des temps de réponse moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des cinq semaines précédentes
- Un graphique à courbes combiné du facteur de disponibilité d'une transaction synthétique sélectionnée qui compare le facteur de disponibilité pour la semaine précédente au facteur de disponibilité de référence au cours des 5 semaines précédentes
- Un tableau du temps de réponse moyen et du facteur de disponibilité d'une transaction synthétique au cours de la semaine précédente et au cours de la plage de dates des cinq semaines précédentes
- Un graphique à courbes combiné des temps de réponse moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des cinq semaines précédentes, par emplacement
- Un graphique à courbes combiné du facteur de disponibilité d'une transaction synthétique sélectionnée qui compare le facteur de disponibilité pour la semaine précédente au facteur de disponibilité de référence de base au cours des 5 semaines précédentes, par emplacement

- Un tableau des temps de réponse moyens et des facteurs de disponibilité d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des cinq semaines précédentes, par emplacement
- Un graphique à courbes combiné des temps de réponse moyens des sous-transactions d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des cinq semaines précédentes
- Un graphique à courbes combiné des facteurs de disponibilité moyens des sous-transactions d'une transaction synthétique sélectionnée qui compare le facteur de disponibilité pour la semaine précédente au facteur de disponibilité de référence au cours des 5 semaines précédentes
- Un tableau des temps de réponse moyens et des facteurs de disponibilité des sous-transactions d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des cinq semaines précédentes

La deuxième page affiche des données de tendance pour les métriques HTTP d'une transaction synthétique :

- Un graphique à courbes combiné des temps de blocage moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes
- Un graphique à courbes combiné des temps DNS moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes
- Un graphique à courbes combiné des temps SSL moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes
- Un graphique à courbes combiné des temps de connexion moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes
- Un graphique à courbes combiné des temps d'envoi moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes
- Un graphique à courbes combiné des temps de réception moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes
- Un graphique à courbes combiné des temps de rendu moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes
- Un tableau des indicateurs HTTP moyens d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes

La troisième page affiche des données de tendance relatives aux indicateurs HTTP, en millisecondes, d'une transaction synthétique par emplacement. Les graphiques et le tableau comparent les moyennes des indicateurs HTTP au cours de la semaine précédente avec la moyenne des mesures de référence au cours des 5 semaines précédentes :

- Sept graphiques à courbes combinés qui comparent les valeurs moyennes de différents indicateurs HTTP d'une transaction synthétique sélectionnée pour la semaine précédente avec l'indicateur de référence au cours des 5 semaines précédentes par emplacement
- Un tableau des valeurs moyennes des indicateurs HTTP d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes

La quatrième page affiche des données de tendance relatives aux indicateurs HTTP, en millisecondes, pour des sous-transactions. Les graphiques et le tableau comparent les moyennes des indicateurs HTTP au cours de la semaine précédente avec les moyennes des mesures de référence au cours des 5 semaines précédentes :

- Sept graphiques à courbes combinés qui comparent les valeurs moyennes de différents indicateurs HTTP d'une transaction synthétique sélectionnée pour la semaine précédente avec l'indicateur de référence au cours des 5 semaines précédentes par sous-transaction
- Un tableau des valeurs moyennes des indicateurs HTTP d'une transaction synthétique sélectionnée, au cours de la semaine précédente et au cours des 5 semaines précédentes par sous-transaction

Tendance des sous-transactions

Ce rapport de deux pages affiche une analyse des tendances des temps de réponse, des facteurs de disponibilité et des indicateurs HTTP pour des sous-transactions au cours de la semaine précédente et des 5 semaines précédentes.

La première page affiche les données de tendance pour les temps de réponse et les facteurs de disponibilité de sous-transactions pour le dimanche précédent, la semaine précédente et les 5 semaines précédentes :

- Un tableau qui compare les données de tendance pour les temps de réponse et les facteurs de disponibilité de sous-transactions pour le dimanche précédent, la semaine précédente et les 5 semaines précédentes
- Un graphique à courbes combiné qui compare les temps de réponse moyens de sous-transactions au cours de la semaine précédente avec le temps de réponse de référence au cours des 5 semaines précédentes
- Un graphique à courbes combiné qui compare les fréquences de disponibilité moyennes de sous-transactions au cours de la semaine précédente avec la fréquence de disponibilité de référence au cours des 5 semaines précédentes
- Un tableau des temps de réponse moyens et des fréquences de disponibilité moyennes de sous-transactions pour la semaine précédente.
- Un tableau des temps de réponse moyens et des fréquences de disponibilité moyennes de sous-transactions pour les 5 semaines précédentes.

La deuxième page affiche des données de tendance relatives aux indicateurs HTTP, en millisecondes, pour des sous-transactions. Les graphiques et les tableaux comparent les moyennes des indicateurs HTTP des sous-transactions au cours de la semaine précédente avec les moyennes des mesures de référence au cours des 5 semaines précédentes :

- Sept tableaux contenant les valeurs moyennes des indicateurs HTTP de la transaction sélectionnée pour le dimanche précédent, la semaine précédente et au cours des 5 semaines précédentes par sous-transactions
- Sept graphiques à courbes combinés qui comparent les valeurs moyennes de différents indicateurs HTTP en millisecondes de la transaction sélectionnée pour la semaine précédente avec le rapport de disponibilité de référence au cours des 5 semaines précédentes par sous-transactions
- Un tableau des valeurs moyennes des indicateurs HTTP des sous-transactions pour la semaine précédente.
- Un tableau des valeurs moyennes des indicateurs HTTP des sous-transactions pour les 5 semaines précédentes.

Procédure

Pour générer des rapports, procédez comme suit :

1. Cliquez sur l'icône **Performance** et sélectionnez **Tableau de bord d'Application Performance**. Pour sélectionner une application, développez **Toutes mes applications**, puis sélectionnez une application. Pour afficher toutes les transactions synthétiques associées à l'application sélectionnée, cliquez sur **Groupes** > **Transactions** > **Transactions synthétiques**.
2. Sélectionnez une transaction synthétique dans le tableau Liste des transactions. Pour exécuter un rapport, cliquez sur **Actions** > **Rapports de lancement** et sélectionnez l'un des rapports suivants :
   - **Vue globale des transactions**
   - **Transaction Detail By Locations**
   - **Transaction Detail By Subtransactions**
   - **Tendance des transactions**
   - **Tendance des sous-transactions**

   Une page de configuration s'ouvre dans un nouvel onglet de votre navigateur Web.

3. Pour définir une plage de dates pour votre rapport, sélectionnez une plage de dates prédéfinie ou entrez une plage de dates personnalisée.
4. Pour définir un intervalle de temps pour votre rapport, sélectionnez un intervalle dans **Time Type**. Configurez votre rapport pour qu'il affiche des données à partir de vos transactions et sous-transactions synthétiques à intervalles **horaires**, **journaliers** ou **hebdomadaires**, sur la plage de dates définie. Pour générer votre rapport, cliquez sur **Terminer**.
5. Pour visualiser les rapports sur les indicateurs HTTP pour les transactions, les sous-transactions ou les emplacements, vous devez sélectionner une transaction, une sous-transaction ou un emplacement dans les rapports **Vue globale des transactions**, **Détails de transaction par emplacements** ou **Détails de transaction par sous-transactions**.
   - Pour visualiser le rapport **Timely Analysis by Transactions**, cliquez avec le bouton droit de la souris sur un nom de transaction dans le rapport **Vue globale des transactions** et sélectionnez **Go To** > **Http Metrics Analysis by Time**.
   - Pour visualiser le rapport **HTTP Metrics by Transactions**, cliquez avec le bouton droit de la souris sur un nom de transaction dans le rapport **Vue globale des transactions** et sélectionnez **Go To** > **Http Metrics Aggregation**.
   - Pour visualiser le rapport **Timely Analysis by Locations of Transaction**, cliquez avec le bouton droit de la souris sur un nom de transaction dans le rapport **Détails de transaction par emplacements** et sélectionnez **Go To** > **Http Metrics Analysis by Time**.
   - Pour visualiser le rapport **HTTP Metrics by Locations of Transaction**, cliquez avec le bouton droit de la souris sur un nom de transaction dans le rapport **Détails de transaction par emplacement** et sélectionnez **Go To** > **Http Metrics Aggregation**.
   - Pour visualiser le rapport **Timely Analysis by Locations of Subtransaction**, cliquez avec le bouton droit de la souris sur un nom de sous transaction dans le rapport **Détails de transaction par emplacement** et sélectionnez **Go To** > **Http Metrics Analysisc by Time**.
   - Pour visualiser le rapport **HTTP Metrics by Locations of Subtransaction**, cliquez avec le bouton droit de la souris sur un nom de sous transaction dans le rapport **Détails de transaction par emplacement** et sélectionnez **Go To** > **Http Metrics Aggregation**.
   - Pour visualiser le rapport **Timely Analysis by Subtransactions**, cliquez avec le bouton droit de la souris sur un nom de sous-transaction dans le rapport **Tendance des sous-transactions** et sélectionnez **Go To** > **Http Metrics Analysis by Time**.
   - Pour visualiser le rapport **HTTP Metrics by Subtransactions**, cliquez avec le bouton droit de la souris sur un nom de sous-transaction dans le rapport **Tendance des sous-transactions** et sélectionnez **Go To** > **Http Metrics Aggregation**.

Rapports de l'Agent WebSphere Applications

Les rapports prédéfinis sont disponibles pour les données collectées par l'Agent WebSphere Applications.

Les données des rapports sont stockées dans la base de données Db2 WAREHOUS. Les rapports affichent les données horaires, quotidiennes, hebdomadaires et mensuelles qui sont conservées pendant 1 mois, 3 mois, 1 an et 1 an respectivement. Cloud APM ne fournit pas de scripts ni d'instructions permettant de modifier ces durées de conservation. Les rapports suivants associés aux données collectées par l'Agent WebSphere Applications sont disponibles :

Performances des demandes d'application

Description

Ce rapport analyse la manière dont les applications sont exécutées à un niveau d'agrégation sur un serveur d'applications. Le graphique circulaire illustre les demandes de niveau d'agrégation des applications. Le graphique à barres représente le temps de réponse moyen des applications à un niveau d'agrégation. Les deux graphiques en lignes de série temporelle affichent le temps de réponse moyen et la tendance du nombre total de demandes pour toutes les applications. Pour explorer les demandes individuelles d'une application, cliquez sur un secteur de graphique ou une barre.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement et Type de serveur d'applications

Tables utilisées

Request_Analysis_*V

Pools de connexions de base de données

Description

Ce rapport analyse les pools de connexions à la base de données dans un serveur d'applications. Le tableau contient des statistiques clés pour tous les pools de connexions à un niveau d'agrégation. Lorsque vous sélectionnez une source de données spécifique, deux graphiques de tendance indiquent la tendance des statistiques clés.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement, Nom du serveur d'applications

Tables utilisées

DB_Connection_Pools_*V

Performances EJB

Description

Ce rapport analyse la façon dont les EJB déployés dans le serveur d'applications s'exécutent. Le graphique circulaire illustre le nombre de méthodes au niveau d'agrégation pour les EJB. Le graphique à barres représente le temps de réponse moyen des méthodes dans les EJB à un niveau d'agrégation. Les deux graphiques de série temporelle illustrent une tendance de nombre d'appels de méthode et une tendance de temps de réponse moyen de méthode pour tous les EJB. Les lignes de tendance peuvent être filtrées par EJB via un clic sur une ligne de la liste.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement, Nom du serveur d'applications

Tables utilisées

Enterprise_Java_Beans_*V

Utilisation de la récupération de place du serveur d'applications

Description

Ce rapport analyse la récupération de place. Utilisez-le pour déterminer si la récupération de place est source de problèmes ou si la taille du segment de mémoire est incorrecte. Le premier graphique illustre le pourcentage de segment de mémoire moyen utilisé et le pourcentage de récupération de place moyen en temps réel dans le temps. Le deuxième graphique illustre le pourcentage d'exécution de la récupération de place moyen en temps réel et le taux de récupération de place moyen.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement, Type de serveur d'applications

Tables utilisées

Garbage_Collection_Analysis_*V

Utilisation de la JVM pour le serveur d'applications

Description

Ce rapport analyse la manière dont la JVM d'un serveur d'applications s'exécute. Le graphique à barres empilées indique la manière dont la mémoire JVM est utilisée et libérée. Le graphique à double courbe indique la consommation d'UC de la JVM au regard de l'utilisation de la mémoire JVM.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement, Type de serveur d'applications

Tables utilisées

Application_Server_*V

Pools d'unités d'exécution

Description

Ce rapport analyse les pools d'unités d'exécution dans un serveur d'applications. Le tableau contient des statistiques clés pour tous les pools d'unités d'exécution à un niveau d'agrégation. Une fois qu'un pool d'unités d'exécution est sélectionné dans la liste, le diagramme de tendances indique la tendance des statistiques clés pour le pool d'unités d'exécution sélectionné. Si aucun pool d'unités d'exécution n'est sélectionné, les tendances indiquent un récapitulatif de tous les pools d'unités d'exécution.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement, Type de serveur d'applications

Tables utilisées

Thread_Pools_*V

Performances des applications Web

Description

Ce rapport analyse la manière dont les applications s'exécutent dans le conteneur Web d'un serveur d'applications (données PMI). Le graphique circulaire illustre les demandes de niveau d'agrégation des applications. Le graphique à barres représente le temps de réponse moyen des applications à un niveau d'agrégation. Les deux graphiques en lignes de série temporelle affichent le temps de réponse moyen et la tendance du nombre total de demandes pour toutes les applications. Cliquez sur un secteur de graphique, une barre ou une ligne pour explorer le(s) servlet(s)/page(s) jsp d'une application.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement, Type de serveur d'applications

Tables utilisées

Thread_Pools_*V

Performances des demandes d'application pour les clusters

Description

Ce rapport analyse la manière dont les serveurs s'exécutent dans un cluster. Le premier graphique illustre le nombre de demandes effectuées par chacun des membres du cluster au cours de l'intervalle de temps sélectionné. Le deuxième graphique fournit des informations sur la tendance de temps de réponse moyen pour chaque membre du cluster. Le graphique contient une ligne distincte pour chaque serveur du cluster. Cliquez sur une ligne pour explorer les données du serveur individuel. Le rapport Performances des demandes d'application associé à ce serveur s'ouvre.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement, Nom du cluster

Tables utilisées

Request_Analysis_*V

Utilisation de la JVM et de la récupération de place pour les clusters

Description

Ce rapport analyse la JVM et les tendances d'utilisation de la récupération de place par chacun des membres du cluster. Le premier graphique illustre le pourcentage d'exécution de la récupération de place moyen en temps réel. Le deuxième graphique illustre le pourcentage de segment de mémoire moyen utilisé. Les derniers graphiques illustrent l'utilisation de la mémoire de l'unité centrale et de la JVM. Tous ces graphiques illustrent des données relatives à chaque membre du cluster sur une ligne distincte.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement, Nom du cluster

Tables utilisées

Garbage_Collection_Analysis_*V, Application_server_*V

Applications principales avec les temps de réponse les plus lents sur l'ensemble des serveurs

Description

Ce rapport analyse la manière dont les applications sont exécutées à un niveau d'agrégation sur tous les serveurs d'applications. Un graphique à barres représente le temps de réponse moyen des applications à un niveau d'agrégation.

Paramètres

Plage de dates : sélectionnez l'une des périodes de génération de rapports prédéfinie ou sélectionnez les heures de début et de fin exactes dans le calendrier.

Paramètres requis : Type de regroupement, Nombre d'applications

Chapitre 11. Mise à niveau

Mettez à niveau vos agents et collecteurs de données pour bénéficier des toutes dernières fonctions et fonctionnalités qui sont disponibles dans l'édition en cours.

Mise à niveau de vos agents

De nouveaux fichiers archive contenant des agents de surveillance mis à niveau sont régulièrement disponibles pour téléchargement. Les fichiers archive sont disponibles à partir de Produits et services sur le site Web IBM Marketplace.

Avant de commencer

Pour les agents suivants, une tâche spécifique à l'agent doit être exécutée avant de suivre la procédure de mise à niveau :

- Pour les agents sous AIX, si vous êtes connecté en tant qu'utilisateur non superutilisateur, vous devez supprimer l'une des bibliothèques de la mémoire avant de lancer la procédure d'installation pour mettre à niveau l'agent. Suivez les instructions décrites dans «Agents sous AIX : arrêt de l'agent et exécution de slibclean avant la mise à niveau», à la page 1174.
- Pour l'agent HMC Base sous AIX, si vous le mettez à niveau en tant qu'utilisateur non superutilisateur, vous devez d'abord arrêter l'agent HMC Base et effacer les bibliothèques dépendantes du cache. Suivez les instructions de la rubrique «agent HMC Base sous AIX : Arrêt de l'agent en tant qu'utilisateur non superutilisateur et exécution de slibclean avant la mise à niveau», à la page 1175
- Pour l'agent Microsoft .NET, vous devez supprimer le collecteur de données de vos applications .NET avant de mettre à niveau l'agent. Suivez les instructions décrites dans «agent Microsoft .NET : suppression du collecteur de données .NET avant la mise à niveau», à la page 1178.
- Pour l'Agent Node.js, supprimez les plug-in de collecteur de données des applications Node.js avant de le mettre à niveau. Suivez les instructions décrites dans «Agent Node.js : suppression des plug-in de collecteur de données avant la mise à niveau», à la page 1175.
- Pour l'Agent Ruby, vous devez supprimer le collecteur de données de vos applications Ruby avant de mettre à niveau l'agent. Suivez les instructions décrites dans «Agent Ruby : suppression des plug-in de collecteur de données avant la mise à niveau», à la page 1178.
- Pour l'agent HTTP Server, vous devez arrêter le serveur HTTP avant de mettre à niveau l'agent.
- Pour l'agent WebSphere MQ, si vous avez activé le suivi des transactions pour l'agent dans la version antérieure, vous devez arrêter l'instance d'agent avant de mettre à niveau l'agent.
- Pour l'Agent SAP NetWeaver Java Stack, lors d'une mise à niveau de la version V8.1.3.2 vers la version V8.1.4, vous devez arrêter toutes les instances SAP NetWeaver Java Stack configurées avec le collecteur de données avant de mettre à niveau l'agent.
- Pour l'Agent Skype for Business Server, si vous effectuez une mise à niveau d'une ancienne version vers la version 8.1.4.0.2 côté agent, le nom de l'agent est modifié en Skype for Business Server. De plus, après avoir mis à niveau le support via SDA, vous devez redémarrer le service APMUI de sorte à répercuter le nouveau nom de l'agent (Skype for Business Server) côté MIN Server ; dans le cas contraire, l'ancien nom de l'agent (MS Lync Server) s'affichera sur le tableau de bord MIN Server.
- Pour Agent Tomcat, si vous souhaitez mettre à niveau TEMA Core Framework sous Windows, vous devez arrêter l'agent et le serveur. Suivez les instructions de la rubrique Agent Tomcat : mise à niveau de TEMA Core Framework sous Windows

Pourquoi et quand exécuter cette tâche

Si une nouvelle version de l'agent est disponible, l'exécution du script d'installation met automatiquement l'agent à niveau. Si aucune version plus récente de l'agent n'est disponible, un message s'affiche pour indiquer que l'agent est déjà installé ; l'agent installé n'est pas affecté.

Pour installer un agent mis à niveau, procédez comme suit :

Procédure

- «Installation des agents sur les systèmes UNIX», à la page 124
- «Installation des agents sur les systèmes Linux», à la page 130
- «Installation des agents sur les systèmes Windows», à la page 139

Résultats

L'agent est mis à niveau vers la version la plus récente. Si aucune version plus récente de l'agent de surveillance n'est disponible, un message s'affiche pour indiquer que l'agent est déjà installé ; l'agent installé n'est pas affecté.

Que faire ensuite

Après une mise à niveau d'un agent Windows, redémarrez celui-ci s'il n'est pas automatiquement configuré et démarré par le programme d'installation de Windows. Exécutez la commande suivante pour vérifier le statut de l'agent :

```
./nom-agent.bat status
```

Utilisez l'une des méthodes suivantes pour démarrer l'agent :

- Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Monitoring agents** > **IBM Performance Management**. Cliquez avec le bouton droit de la souris sur un agent et cliquez sur **Start**.
- Exécutez la commande suivante :

  ```
  ./nom-agent.bat start
  ```

Pour plus d'informations sur les commandes relatives à l'agent de surveillance, y compris le nom à utiliser, le contrôle du statut, etc., voir «Utilisation des commandes de l'agent», à la page 181. Pour plus d'informations sur les agents démarrés automatiquement et manuellement, voir Chapitre 5, «Déploiement d'agents et de collecteurs de données», à la page 115.

- Pour l'agent Hadoop, procédez comme suit après la mise à niveau de l'agent basé sur un socket (version 8.1.2, groupe de correctifs 2 ou antérieure) vers l'agent basé sur une API REST (version 8.1.3 ou ultérieure) :

  1. Pour éviter la génération de journaux inutiles, supprimez le code de 17 lignes dans les fichiers `hadoop-metrics2.properties` de tous les noeuds Hadoop.
  2. Arrêtez les services Hadoop.
  3. Supprimez de tous les noeuds du cluster Hadoop le fichier `Plugin.jar` qui a été copié par le programme d'installation d'agent.
  4. Démarrez les services Hadoop.

  Pour plus d'informations sur le code de 17 lignes et le fichier `Plugin.jar`, voir Configuration de noeuds Hadoop.
- Pour l'agent HMC Base, après l'avoir mis à niveau de la version 6.2.2.6 à la version 6.2.2.7, vous devez de nouveau le configurer et le redémarrer. Pour obtenir des instructions, voir «Configuration de la surveillance de HMC Base», à la page 270.
- Pour l'agent HTTP Server, si vous mettez à niveau l'agent à partir d'une version antérieure à 1.0.0.4 vers 1.0.0.4 ou ultérieure, vous devez également mettre à jour le fichier `.conf`, utilisé par le serveur HTTP, pour remplacer le fichier de configuration du collecteur de données précédent par le fichier qui vient

d'être généré. Vous devez également ajouter la nouvelle instance d'agent à la console. Pour obtenir des instructions, voir «Configuration de la surveillance de HTTP Server», à la page 275.

- Pour l'agent Microsoft .NET, après l'avoir mis à niveau, configurez le collecteur de données. Pour obtenir des instructions, voir «Enregistrement du collecteur de données», à la page 535.

  Si vous avez installé l'agent dans un nouveau répertoire, vous devez modifier le chemin du répertoire Bin du service Profiler à l'aide de la commande service controller (sc). Par exemple,

  ```
  sc \\localhost config DotNetProfilerService binPath=
  "${rép_install}\qe\bin\DotNetProfilerService.exe
  ```

  où *rép_install* correspond au nouveau répertoire d'installation.
- Pour l'Agent Node.js, après l'avoir mis à niveau, configurez les collecteurs de données d'agent. Pour obtenir des instructions, voir «Configuration de l'Agent Node.js», à la page 602.
- Pour l'Agent OpenStack, si vous souhaitez le configurer pour utiliser OpenStack Identity API v3, reconfigurez toutes les instances d'agent et mettez à jour le fichier de configuration du collecteur de données d'agent. Pour obtenir des instructions, voir «Agent OpenStack : reconfiguration des instances de l'agent pour utiliser OpenStack Identity API v3», à la page 1178.
- Pour l'Agent Ruby, après l'avoir mis à niveau, configurez le collecteur de données. Pour obtenir des instructions, voir «Configuration du collecteur de données de diagnostic», à la page 741.
- Pour l'Agent WebSphere Applications, après l'avoir mis à niveau, migrez le collecteur de données en exécutant la commande *base_cd*`/bin/migrate.sh/bat` à partir du répertoire d'installation de la nouvelle version de l'agent et redémarrez l'instance de serveur d'applications. Pour obtenir des instructions, voir «Agent WebSphere Applications : migration du collecteur de données», à la page 1179.
- Linux Si vous souhaitez mettre à niveau une ancienne version de l'agent installée dans le répertoire `/opt/ibm/ccm/agent`, procédez comme suit sur le système Linux :

  1. Si vous confirmez vouloir migrer la configuration d'agent de l'ancien répertoire d'installation `/opt/ibm/ccm/agent` vers le nouveau répertoire d'installation (par exemple, `/opt/ibm/apm/agent`), vous devez démarrer l'agent dans le nouvel emplacement d'installation.

     Restriction : L'ancienne version de l'agent est arrêtée automatiquement dans l'ancien emplacement d'installation, mais elle n'est pas démarrée automatiquement dans le nouvel emplacement d'installation.
  2. Une fois que vous avez vérifié que l'agent fonctionne dans le nouveau répertoire d'installation, vous devez désinstaller l'ancienne version de l'agent du répertoire `/opt/ibm/ccm/agent`. Si vous souhaitez supprimer tous les agents, exécutez la commande **`/opt/ibm/ccm/agent/bin/smai-agent.sh uninstall_all`**.
- Linux Si vous mettez à niveau des agents à partir du FP6 ou antérieur, après avoir terminé la mise à niveau des agents dans un nouveau répertoire et la configuration ou la reconfiguration des agents, vous pouvez juger utile de supprimer le répertoire de l'ancienne installation. Procédez comme suit :

  1. Sur la machine virtuelle ou le système où est installé l'agent de surveillance, lancez une ligne de commande et accédez au dossier binaire dans le répertoire de l'ancienne installation, `/opt/ibm/ccm/agent/bin`.
  2. Pour désinstaller tous les agents de surveillance installés à partir du répertoire de l'ancienne installation, entrez `:./smai-agent.sh uninstall_all`
  3. Supprimez le répertoire de l'ancienne installation.

Conservation des changements apportés à la configuration des agents

Les utilisateurs avancés peuvent appliquer des valeurs de substitution à la personnalisation des composants. L'application de valeurs de substitution permet de conserver les valeurs lors d'une mise à niveau. Avant de les appliquer d'une manière globale, testez les changements apportés à votre environnement.

Pourquoi et quand exécuter cette tâche

- Ces instructions s'appliquent aux agents Linux et AIX. Pour obtenir la liste des codes produit et des commandes utilisées pour arrêter et démarrer les agents, voir «Utilisation des commandes de l'agent», à la page 181.
- Le processus de l'agent Windows conserve les changements de configuration par conception : les variables mises à jour dans le fichier k*cp*cma.ini, où *cp* correspond au code produit, sont conservées dans la section Override Local Settings. Elles sont utilisées lors de chaque configuration pour mettre à jour les entrées du registre Windows que les agents utilisent au moment de l'exécution.
- Les paramètres personnalisés dans les fichiers .*cp*.environment et .global.environment sont perdus après la mise à niveau de l'agent. Pour conserver vos paramètres, effectuez les modifications de personnalisation dans les fichiers *cp*.environment et global.environment. Les paramètres de ces fichiers ne sont pas écrasés par une mise à niveau de l'agent.

Procédure

Pour sauvegarder les changements de configuration apportés au fichier d'environnement et les conserver après la mise à niveau de l'agent, procédez comme suit :

1. Créez et mettez à jour l'un des fichiers suivants, où *rép_install* est le répertoire d'installation de l'agent (par exemple, le répertoire Linux par défaut /opt/ibm/apm/agent/ ou le répertoire AIX par défaut /opt/ibm/ccm/agent/) :

Nom du fichier	Description
***rép_install*/config/*cp*.environment**	Le terme *cp* dans le nom de fichier désigne le code produit de l'agent, par exemple mq ou rz.
***rép_install*/config/global.environment**	Mettez à jour le fichier d'environnement global de manière à appliquer les changements devant affecter tous les types d'agent.

   Par exemple, as.environment est le fichier d'environnement persistant de l'Agent WebSphere Applications. .as.environment est remplacé lorsque l'agent est mis à niveau vers une nouvelle version.

   Définissez les variables au format *clé*=*valeur*, où *clé* est le nom de la variable d'environnement et *valeur* est la valeur ou le paramètre (tel que **KDC_FAMILIES=${KDC_FAMILIES}HTTP:10001**).
2. Une fois que vous avez mis à jour les paramètres de variable, enregistrez et fermez le fichier d'environnement, puis redémarrez les agents concernés.

Résultats

Les mises à jour sont appliquées à tous les agents de même type ou, si vous avez mis à jour le fichier d'environnement global, à tous les agents relevant du serveur Cloud APM. Les changements sont conservés malgré les mises à niveau des versions de l'agent.

Agents sous AIX : arrêt de l'agent et exécution de slibclean avant la mise à niveau

Si vous mettez à niveau un agent en tant qu'utilisateur non superutilisateur sur les systèmes AIX, vous devez effectuer cette tâche. Avant d'exécuter le programme d'installation de l'agent, vous devez arrêter l'agent et exécuter la commande **slibclean** pour nettoyer la bibliothèque libkududp.a.

Procédure

1. Arrêtez l'agent en exécutant l'une des commandes suivantes, dans le cas où l'agent prendrait en charge plusieurs instances ou non :
   - ./*nom*-agent.sh stop
   - ./*nom*-agent.sh stop *nom_instance*

Voir «Utilisation des commandes de l'agent», à la page 181 .

2. Exécutez la commande suivante avec les privilèges de superutilisateur.

```
slibclean
```

Voir slibclean Command dans le composant IBM Knowledge Center.

Résultats
L'agent est arrêté et la bibliothèque `libkududp.a` est nettoyée.

Que faire ensuite
Exécutez le programme d'installation pour mettre à niveau l'agent vers la version que vous avez téléchargée. Voir Chapitre 6, «Installation des agents», à la page 123 . Si la mise à niveau échoue, réamorcez le serveur et répétez la procédure.

agent HMC Base sous AIX : Arrêt de l'agent en tant qu'utilisateur non superutilisateur et exécution de `slibclean` avant la mise à niveau

Avant de mettre à niveau l'agent HMC Base en tant qu'utilisateur non superutilisateur sous AIX, vous devez l'arrêter et exécuter **slibclean** pour effacer les bibliothèques dépendantes du cache.

Pourquoi et quand exécuter cette tâche

Procédure

1. Exécutez la commande suivante en tant qu'utilisateur non superutilisateur pour arrêter l'agent.

```
hmc_base-agent.sh stop
```

2. Exécutez la commande suivante avec les privilèges de superutilisateur.

```
slibclean
```

Voir slibclean Command dans le composant IBM Knowledge Center.

Résultats
L'agent HMC Base est arrêté et les bibliothèques dépendantes sont effacées.

Que faire ensuite
Exécutez le programme d'installation d'agent pour mettre à niveau l'agent HMC Base.

Agent Node.js : suppression des plug-in de collecteur de données avant la mise à niveau

Avant de mettre à niveau l'Agent Node.js, supprimez les plug-in de surveillance de votre application Node.js.

Pourquoi et quand exécuter cette tâche
En fonction de la version de votre Agent Node.js, vous devez suivre une procédure spécifique pour supprimer les plug-in de surveillance de votre application Node.js. Pour connaître la version de l'agent, voir Commande de version d'agent.

Procédure

1. Supprimez les plug-in de collecteur de données au début du fichier d'application Node.js :
   - Si vous mettez à niveau l'Agent Node.js à partir de la version 01.00.12.00 vers la version 01.00.13.00, procédez comme suit :

– Si vous avez activé la collecte des données de ressource, supprimez la ligne ci-après au début du fichier d'application Node.js :

```
require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_index.js');
```

où *KNJ_NPM_LIB_LOCATION* correspond au répertoire du dossier `lib` de votre répertoire d'installation global du package npm. Le répertoire par défaut est `/usr/local/lib`.

– Si vous avez activé la collecte des données de ressource et la collecte des données de diagnostics approfondis, supprimez la ligne ci-après au début du fichier d'application Node.js :

```
require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_deepdive.js');
```

– Si vous avez activé la collecte des données de ressource, la collecte des données de diagnostics approfondis et la collecte des traces de méthode, supprimez la ligne ci-après au début du fichier d'application Node.js :

```
require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_methodtrace.js');
```

- Si vous mettez à niveau l'Agent Node.js à partir de la version 01.00.10.00 vers la version 01.00.13.00, procédez comme suit :
  – Si vous avez activé la collecte des données de ressource, supprimez la ligne ci-après au début du fichier d'application Node.js.

```
require('rép_install/lx8266/nj/bin/plugin/knj_index.js');
```

, où *rép_install* correspond au répertoire d'installation de l'Agent Node.js.

  – Si vous avez activé la collecte des données de ressource et la collecte des données de diagnostics approfondis, supprimez la ligne ci-après au début du fichier d'application Node.js.

```
require('rép_install/lx8266/nj/bin/plugin/knj_deepdive.js');
```

  – Si vous avez activé la collecte des données de ressource, la collecte des données de diagnostics approfondis et la collecte des traces de méthode, supprimez la ligne ci-après au début du fichier d'application Node.js .

```
require('rép_install/lx8266/nj/bin/plugin/knj_methodtrace.js');
```

2. Redémarrez l'application Node.js pour désactiver les plug-in de collecteur de données.
   - Si la version actuelle de l'Agent Node.js est01.00.10.00, les plug-in du collecteur de données sont supprimés dès maintenant.
   - Si la version de votre Agent Node.js actuel est la version 01.00.12.00, passez à l'étape suivante.
3. Exécutez la commande `./uninstall.sh` à partir du répertoire *rép_install*`/lx8266/nj/bin` pour supprimer les paramètres d'agent précédents.

Que faire ensuite
Mettez à niveau l'Agent Node.js. Voir «Mise à niveau de vos agents», à la page 1171 .

Agent Response Time Monitoring : mise à niveau de module IBM HTTP Server Response Time

Si vous surveilliez IBM HTTP Server à l'aide du module IBM HTTP Server Response Time ou de l'agent HTTP Server, mettez à niveau votre installation.

Pourquoi et quand exécuter cette tâche

Le tableau ci-après présente des scénarios d'installation qui peuvent correspondre à la manière dont vous surveillez IBM HTTP Server.

Agent Response Time Monitoring	Utilisation du module IBM HTTP Server Response Time ?	Utilisation du Analyseur de paquets ?	L'agent HTTP Server est-il installé ?
AIX et xLinux : 08.11.00 et ultérieure Windows : 08.14.02 et ultérieure	✓	–	✓
AIX et xLinux : 08.10.00	✓	–	–
AIX et xLinux : 08.10.00	✓	–	✓
7.40.07 ou les versions antérieures	–	✓	–
7.40.07 ou les versions antérieures	–	✓	✓

Pour tous ces scénarios, la procédure d'installation est semblable.

Procédure

1. Installez l'agent HTTP Server à partir de la version 8.1.1 ou ultérieure sous AIX ou Linux et à partir de la version 8.1.4.02 ou ultérieure sous Windows.

   Le module IBM HTTP Server Response Time est installé automatiquement avec l'agent.
2. Configurez l'agent HTTP Server.

   Remarque : Si vous utilisiez précédemment le module IBM HTTP Server Response Time, mettez à jour le fichier de configuration de serveur Web (`httpd.conf`) avec l'emplacement du nouveau module IBM HTTP Server Response Time et supprimez l'ancien fichier de configuration de module de chargement (`mod_wrt.so`).

   Remarque : L'agent Response Time Monitoring version 8.1.1 et ultérieure ne fonctionne pas avec le fichier du module de chargement (`mod_wrt.so`) issu d'éditions antérieures. Si vous tentez d'utiliser une version antérieure de ce fichier, plusieurs messages seront consignés dans le journal des erreurs. Les transactions peuvent toujours être suivies mais les données de l'instance de transaction ne s'afficheront pas.

   Pour plus d'informations, voir le PDF de référence de l'agent HTTP Server, que vous pouvez télécharger à partir de http://ibm.biz/agent-httpserver.
3. Vérifiez qu'IBM HTTP Server et que l'agent HTTP Server sont en cours d'exécution. Si le programme d'installation de Response Time Monitoring détecte l'agent HTTP Server, l'agent Response Time Monitoring active le module IBM HTTP Server Response Time plutôt que l'Analyseur de paquets.
4. Installez l'agent Response Time Monitoring au même emplacement `AGENT_HOME` que l'agent HTTP Server.
   - Linux AIX Installez la version 8.1.1 ou ultérieure en tant que **`root`**. Exemple d'emplacement `AGENT_HOME` : `/opt/ibm/apm/agent/`
   - Windows Installez la version 8.1.4.0.2 ou ultérieure avec des droits d'administrateur. Exemple d'emplacement `AGENT_HOME` : `C:\IBM\APM\`.
5. Si vous avez utilisé l'Analyseur de paquets dans les éditions précédentes, vous devrez peut-être désactiver l'Analyseur de paquets pour démarrer la surveillance d'IBM HTTP Server avec le module IBM HTTP Server Response Time.
6. Redémarrez IBM HTTP Server.

agent Microsoft .NET : suppression du collecteur de données .NET avant la mise à niveau

Avant de mettre à niveau l'agent Microsoft .NET, supprimez le collecteur de données .NET de vos applications .NET.

Procédure

1. Désenregistrez tous les modules du collecteur de données.

   En tant qu'administrateur, entrez :

   ```
   cd rép_install\qe\bin configdc unregisterdc all
   ```

   Où *rép_install* correspond au répertoire d'installation de l'agent Microsoft .NET.
2. Redémarrez les applications .NET.

Que faire ensuite

Mettez à niveau l'agent Microsoft .NET. Voir «Mise à niveau de vos agents», à la page 1171.

Agent OpenStack : reconfiguration des instances de l'agent pour utiliser OpenStack Identity API v3

Pour mettre à niveau l'Agent OpenStack afin d'utiliser OpenStack Identity API v3, vous devez, après avoir installé la dernière version de l'agent, reconfigurer toutes les instances de l'agent et mettre à jour le fichier de configuration du collecteur de données.

Pourquoi et quand exécuter cette tâche

Cette tâche est requise uniquement si vous mettez à niveau l'agent pour utiliser OpenStack Identity API v3.

Procédure

1. Reconfigurez toutes les instances de l'agent existantes. Pour des instructions détaillées, voir «Configuration de l'Agent OpenStack», à la page 626.
2. Recherchez le fichier de configuration ksg_dc_*nom_instance*.cfg du collecteur de données d'agent, où *nom_instance* correspond au nom que vous avez spécifié pour l'instance d'agent.

   Si le fichier n'existe pas, copiez *rép_install*/lx8266/sg/bin/ksg_dc.cfg dans le répertoire *rép_install*/config et renommez le fichier ksg_dc_*nom_instance*.cfg.

   Par exemple, si le nom de l'instance est 0S1, changez le nom en ksg_dc_0S1.cfg.
3. Ajoutez la section suivante au fichier ksg_dc_*nom_instance*.cfg :

   ```
   #OpenStack authentication information
   [OS_authentication_info]
   OS_project_domain_name=Default
   OS_user_domain_name=Default
   OS_cert_path=
   ```
4. Redémarrez l'instance d'agent en exécutant les commandes suivantes :

   ```
   rép_install/bin/openstack-agent.sh stop nom_instance
   rép_install/bin/openstack-agent.sh start nom_instance
   ```

   , où *nom_instance* correspond au nom de l'instance d'agent à configurer.

Agent Ruby : suppression des plug-in de collecteur de données avant la mise à niveau

Avant de mettre à niveau l'Agent Ruby, supprimez les plug-in de surveillance de votre application Ruby.

Procédure

1. Supprimez le collecteur de données de l'ancienne version en lançant la commande suivante :

```
gem uninstall stacktracer
```

2. Accédez au répertoire de base de votre application, ouvrez son `Gemfile` et supprimez la ligne suivante : `gem 'stacktracer', 'version'`
   Où *version* correspond au numéro de version de l'Agent Ruby.
3. Dans le répertoire de base de votre application, entrez : `bundle install`

Que faire ensuite

Mettez à niveau l'Agent Ruby. Voir «Mise à niveau de vos agents», à la page 1171.

Agent WebSphere Applications : migration du collecteur de données

Après avoir mis à jour l'agent, vous devez migrer le collecteur de données de manière interactive ou en mode silencieux.

Migration du collecteur de données en mode interactif

Vous pouvez migrer un niveau de maintenance antérieur du collecteur de données en mode interactif à l'aide de l'utilitaire de migration.

Avant de commencer

Linux AIX Si vous avez installé WebSphere Application Server ou WebSphere Portal Server à l'aide d'un compte utilisateur non superutilisateur, avant d'exécuter les utilitaires de configuration, vérifiez que l'utilisateur non superutilisateur dispose des privilèges de lecture et écriture sur les répertoires d'agent suivants dans *rép_install*`/yndchome/7.3.0.14.08`, *rép_install* représentant le répertoire d'installation de l'Agent WebSphere Applications :

- `data`
- `bin`
- `runtime`
- `logs`

Le cas échéant, utilisez la commande `chmod 777` pour attribuer les droits en lecture et écriture. En outre, connectez-vous à l'aide du même ID utilisateur qui a servi pour installer le serveur d'applications.

Pourquoi et quand exécuter cette tâche

Vous pouvez migrer un niveau de maintenance antérieur du collecteur de données en mode interactif à l'aide de l'utilitaire de migration. Si vous souhaitez migrer un grand nombre d'instances de serveur d'applications, il peut être plus pratique d'utiliser l'utilitaire de migration en mode silencieux.

Important :

- Vous pouvez uniquement migrer les niveaux de maintenance antérieurs à la version 7.3 du collecteur de données. La version du collecteur de données est indiquée dans le répertoire de base du collecteur de données.
- Il n'est pas possible de migrer les niveaux de maintenance de la version 7.3 vers la version 7.3, groupe de correctifs 1. Vous devez annuler la configuration du collecteur de données et désinstaller la version d'agent 7.3, puis installer la version d'agent 7.3, groupe de correctifs 1 et configurer à nouveau le collecteur de données.

Procédure

1. Linux AIX Connectez-vous sous le nom de l'utilisateur utilisé pour installer le serveur d'applications.
2. Démarrez l'utilitaire de migration à partir du répertoire d'installation de la dernière version de l'agent.

   Linux AIX Lancez la commande *base_cd*`/bin/migrate.sh`

Windows Exécutez la commande *base_cd*\bin\migrate.bat

3. L'utilitaire affiche les adresses IP de toutes les cartes réseau qui sont trouvées sur le système informatique local.

   Entrez le nombre qui correspond à l'adresse IP à utiliser.

4. L'utilitaire recherche et répertorie tous les serveurs configurés par niveau de maintenance antérieur de collecteur de données. Les collecteurs de données sont regroupés par niveau de maintenance.

   Sélectionnez une ou plusieurs instances de serveur d'applications dans la liste.

   La liste peut comporter les instances de serveur WebSphere et Liberty traditionnelles. Les instances de serveur WebSphere traditionnelles peuvent figurer sous différents profils.

   Conseil :

   - Si plusieurs instances d'un profil sont surveillées, vous devez toutes les sélectionner afin de les migrer simultanément.
   - Migrez tous les serveurs figurant sous le profil Liberty en même temps. Une migration partielle des serveurs configurés pourrait provoquer des problèmes de stabilité.

   A faire :

   - Pour un environnement autonome, les instances de serveur d'applications doivent s'exécuter.
   - Dans un environnement de déploiement réseau, l'agent de noeud et le gestionnaire de déploiement doivent s'exécuter.
   - Il n'est pas nécessaire d'exécuter les serveurs Liberty au cours de la migration.

5. Entrez le numéro correspondant à l'instance de serveur d'applications dont le collecteur de données est en train de migrer ou entrez un astérisque (*) pour faire migrer le collecteur de données de toutes les instances de serveur d'applications.

   Pour spécifier un sous-ensemble de serveurs, entrez les numéros des serveurs en les séparant par une virgule. Par exemple : `1,2,3`.

   L'utilitaire de migration intègre automatiquement chaque collecteur de données à l'agent de surveillance. Les valeurs d'hôte et de port de l'agent de surveillance sont récupérées dans les fichiers de configuration existants.

6. Entrez un alias pour chaque serveur sélectionné.

   La valeur par défaut correspond à l'alias de serveur existant.

7. Pour l'instance de serveur Liberty, entrez le répertoire de base de la JVM lorsque vous y êtes invité. Par exemple, `/opt/IBM/java`.

8. L'utilitaire détermine si WebSphere Global Security est activé pour chacun des profils dans lesquels la collecte de données est migrée.

   Si WebSphere Global Security est activé pour un ou plusieurs profils, indiquez s'il faut récupérer les paramètres de sécurité dans le fichier de propriétés d'un client :

   Le collecteur de données communique avec les services d'administration de WebSphere en utilisant l'invocation RMI (Remote Method Invocation) ou le protocole SOAP (Simple Object Access Protocol). Si la sécurité globale est activée pour un profil, vous devez indiquer l'ID utilisateur et le mot de passe d'un utilisateur qui est autorisé à se connecter à IBM WebSphere Application Server la console d'administration pour le profil.

   Vous avez également la possibilité de chiffrer le nom d'utilisateur et le mot de passe et de les stocker dans des fichiers de propriétés de client Application Server avant de configurer le collecteur de données. Vous devez utiliser le fichier `sas.client.props` pour une connexion RMI et le fichier `soap.client.props` pour une connexion SOA.

9. Entrez 1 pour permettre à l'utilitaire d'extraire le nom d'utilisateur et le mot de passe à partir du fichier de propriétés de client approprié et passez à l'étape «11», à la page 1181. Sinon, entrez 2 pour saisir le nom d'utilisateur et le mot de passe.

   Important : La connexion à la console d'administration WebSphere Application Server peut prendre du temps.

10. Indiquez le nom d'utilisateur et le mot de passe pour chaque profil où WebSphere Global Security est activé.
11. L'utilitaire migre la collecte de données pour chaque instance de serveur d'applications sélectionnée. Il affiche un message d'état indiquant si la migration de chaque serveur s'est effectuée correctement.
12. Redémarrez les instances comme indiqué par l'utilitaire. La configuration du collecteur de données entre en vigueur une fois que les instances de serveur d'applications ont redémarré.

Résultats
Le collecteur de données est migré au dernier niveau de maintenance installé.

Que faire ensuite
L'utilitaire de migration conserve les paramètres configurés dans la version antérieure du collecteur de données. Pour modifier ces paramètres, vous pouvez exécuter l'utilitaire de configuration ou de reconfiguration en mode interactif ou silencieux à partir du répertoire *base_cd*\bin du nouveau collecteur de données. Pour plus d'informations, voir «Configuration ou reconfiguration du collecteur de données à l'aide des utilitaires de configuration complète», à la page 863.

Migration du collecteur de données en mode silencieux
Vous pouvez migrer un niveau de maintenance antérieur du collecteur de données en mode silencieux à l'aide de l'utilitaire de migration.

Avant de commencer

Linux AIX Si vous avez installé WebSphere Application Server ou WebSphere Portal Server à l'aide d'un compte utilisateur non superutilisateur, avant d'exécuter les utilitaires de configuration, vérifiez que l'utilisateur non superutilisateur dispose des privilèges de lecture et écriture sur les répertoires d'agent suivants dans *rép_install*/yndchome/7.3.0.14.08, *rép_install* représentant le répertoire d'installation de l'Agent WebSphere Applications :

- data
- bin
- runtime
- logs

Le cas échéant, utilisez la commande chmod 777 pour attribuer les droits en lecture et écriture. En outre, connectez-vous à l'aide du même ID utilisateur qui a servi pour installer le serveur d'applications.

Pourquoi et quand exécuter cette tâche
Un exemple de fichier de propriétés silencieux, sample_silent_migrate.txt, est fourni avec l'utilitaire de migration. Ce fichier se trouve dans le répertoire *rép_install*/yndchome/7.3.0.14.08/bin.

Lorsque vous créez votre fichier de propriétés silencieux, tenez compte des remarques suivantes :

- Dans le fichier, une ligne commençant par un signe dièse (#) est considérée comme un commentaire, et n'est pas traitée. Si le signe dièse est utilisé ailleurs dans la ligne, on ne le considère pas comme le début d'un commentaire. Vous pouvez donc utiliser le caractère dièse dans les mots de passe ou à d'autres fins.
- Chaque propriété est décrite sur une ligne distincte, au format suivant : propriété = valeur.

  propriété
  Le nom de la propriété. La liste de propriétés valides que vous pouvez configurer est affichée dans le Tableau 256, à la page 1182. Ne modifiez pas ou ne supprimez pas les propriétés du fichier d'échantillon qui ne sont pas mentionnées dans la table.

  valeur
  La valeur de la propriété. Des valeurs par défaut pour certaines propriétés sont déjà fournies. Vous pouvez supprimer des valeurs par défaut pour laisser des valeurs de propriété en blanc. Une valeur

vide est traitée comme si la propriété n'était pas indiquée, par opposition à l'utilisation de la valeur par défaut. Si vous voulez utiliser des valeurs par défaut, vous pouvez mettre en commentaire la propriété dans le fichier.

- Les mots de passe sont en texte en clair.
- Les propriétés et leurs valeurs distinguent les majuscules et minuscules.

Le Tableau 256, à la page 1182 décrit les propriétés disponibles lors de la migration du collecteur de données en mode silencieux.

Tableau 256. Propriétés disponibles pour l'exécution de l'utilitaire de migration en mode silencieux

Propriété	**Commentaire**
migrate.type	Doit avoir pour valeur AD.
default.hostip	Si le système informatique utilise plusieurs adresses IP, indiquez l'adresse IP que le collecteur de données doit utiliser.
itcam.migrate.home	Indique le répertoire de base du collecteur de données correspondant à la version de maintenance antérieure du collecteur de données. Le répertoire n'est pas supprimé au cours de la migration.
was.wsadmin.connection.host	Indique le nom de l'hôte auquel l'outil wsadmin se connecte. Dans un environnement Network Deployment, spécifiez la connexion wsadmin au gestionnaire de déploiement. Dans un environnement autonome, indiquez la connexion wsadmin au serveur.
was.wsadmin.username	Spécifie l'ID utilisateur d'un utilisateur autorisé à se connecter à la console d'administration d'IBM WebSphere Application Server. Cet utilisateur doit posséder le rôle d'agent sur le serveur d'applications.
was.wsadmin.password	Indique le mot de passe qui correspond à l'utilisateur indiqué dans la propriété `was.wsadmin.username`.
was.appserver.profile.name	Indique le nom du profil de serveur d'applications à configurer. **A faire :** Cette propriété n'est pas requise pour le profil Liberty.
was.appserver.home	Indique le répertoire de base de WebSphere Application Server.
was.appserver.cell.name	Indique le nom de cellule de WebSphere Application Server. **A faire :** Cette propriété n'est pas requise pour le profil Liberty.
was.appserver.node.name	Indique le nom de noeud de WebSphere Application Server. **A faire :** Cette propriété n'est pas requise pour le profil Liberty.

Tableau 256. Propriétés disponibles pour l'exécution de l'utilitaire de migration en mode silencieux (suite)	
Propriété	**Commentaire**
was.appserver.server.name	Spécifie l'instance de serveur d'applications figurant dans le profil de serveur d'applications devant être migrée vers la nouvelle version du collecteur de données. Le fichier de propriétés silencieux peut comporter plusieurs occurrences de cette propriété.

Important :

- Vous pouvez uniquement migrer les niveaux de maintenance antérieurs à la version 7.3 du collecteur de données. La version du collecteur de données est indiquée dans le répertoire de base du collecteur de données.
- Il n'est pas possible de migrer les niveaux de maintenance de la version 7.3 vers la version 7.3, groupe de correctifs 1. Vous devez annuler la configuration du collecteur de données et désinstaller la version d'agent 7.3, puis installer la version d'agent 7.3, groupe de correctifs 1 et configurer à nouveau le collecteur de données.

Procédure

1. Spécifiez les options de configuration dans le fichier de propriétés de migration en mode silencieux.
2. Lancez la commande de démarrage de l'utilitaire de migration en mode silencieux à partir du répertoire d'installation de la dernière version de l'agent.
   - Linux AIX *base_cd*/bin/migrate.sh -silent *sample_silent_migration_filename*
   - Windows *base_cd*\bin\migrate.bat -silent *sample_silent_migration_filename*

Résultats
Le collecteur de données est migré au dernier niveau de maintenance installé.

Que faire ensuite
L'utilitaire de migration conserve les paramètres configurés dans la version antérieure du collecteur de données. Pour modifier ces paramètres, vous pouvez exécuter l'utilitaire de configuration ou de reconfiguration en mode interactif ou silencieux à partir du répertoire *dc_home*\bin du nouveau collecteur de données. Pour plus d'informations, voir «Configuration ou reconfiguration du collecteur de données à l'aide des utilitaires de configuration complète», à la page 863.

Agent Tomcat : mise à niveau de TEMA Core Framework sous Windows

Pour mettre à niveau TEMA Core Framework sous Windows pour l'Agent Tomcat, vous devez arrêter l'agent et le serveur pour que la mise à jour de l'infrastructure TEMA aboutisse.

Procédure

1. Préparez la configuration du serveur Tomcat.
2. Installez et configurez l'agent Tomcat.
3. Connectez-vous au tableau de bord IBM Cloud Application Performance Management, accédez à **Configuration d'agent** > **Tomcat**, sélectionnez une instance de l'Agent Tomcat et cliquez sur **Enable TT/DD**.
4. Redémarrez le serveur Tomcat.
5. Pour appliquer IBM APM CORE FRAMEWORK, arrêtez l'agent et le serveur Tomcat.
6. Accédez à TEMA/<IBM APM CORE FRAMEWORK_HOME>. Exécutez la commande **apmpatch.bat <répertoire d'installation de l'agent Tomcat>**.

L'infrastructure est mise à niveau.

7. Vérifiez la version IBM APM CORE FRAMEWORK mise à niveau en exécutant les instructions ci-après.
   `Goto <répertoire d'installation de l'agent Tomcat>\InstallITM`
   `Run: KinCInfo.exe -i`.
8. Démarrez le serveur et l'agent Tomcat.

Mise à niveau de vos collecteurs de données

De nouveaux fichiers archive contenant des collecteurs de données mis à niveau sont régulièrement disponibles pour téléchargement. Les fichiers archive sont disponibles à partir de Produits et services sur le site Web d'IBM Marketplace..

Avant de commencer

Pourquoi et quand exécuter cette tâche

Pour mettre à niveau un collecteur de données, procédez comme suit :

Procédure

- Annulez la configuration du collecteur de données à partir de vos applications locales et/ou IBM Cloud :
  - Pour le collecteur de données J2SE, les étapes d'annulation de la configuration ne sont pas requises.
  - Pour le collecteur de données Liberty, suivez les instructions dans «Annulation de la configuration du collecteur de données pour les applications IBM Cloud», à la page 916 et/ou «Annulation de la configuration du collecteur de données pour les applications sur site», à la page 909.
  - Pour le collecteur de données Node.js, suivez les instructions dans «Annulation de la configuration du collecteur de données Node.js autonome pour les applications IBM Cloud», à la page 614 et/ou «Annulation de la configuration du collecteur de données Node.js autonome pour les applications sur site», à la page 620.
  - Pour le collecteur de données Python, suivez les instructions dans «Annulation de la configuration du collecteur de données Python pour les applications IBM Cloud», à la page 695 et/ou «Annulation de la configuration du collecteur de données Python pour les applications sur site», à la page 701.
  - Pour le collecteur de données Ruby, suivez les instructions dans «Annulation de la configuration du collecteur de données Ruby pour les applications IBM Cloud», à la page 749.
- Téléchargez le module du collecteur de données.
- Reconfigurez le collecteur de données pour surveiller vos applications locales et/ou IBM Cloud :
  - Pour le collecteur de données Node.js, après avoir mis à niveau le collecteur de données, reconfigurez ce dernier. Pour obtenir les instructions, voir «Configuration du collecteur de données Node.js autonome pour les applications IBM Cloud(anciennement Bluemix)», à la page 608 et/ou «Configuration du collecteur de données Node.js autonome pour les applications sur site», à la page 615.
  - Pour le collecteur de données Python, après avoir mis à niveau le collecteur de données, reconfigurez ce dernier. Pour obtenir les instructions, voir «Configuration du collecteur de données Python pour les applications IBM Cloud», à la page 689 et/ou «Configuration du collecteur de données Python pour les applications sur site», à la page 695.
  - Pour le collecteur de données Liberty, après avoir mis à niveau le collecteur de données, reconfigurez ce dernier. Pour obtenir les instructions, voir «Configuration du collecteur de données Liberty pour les applications IBM Cloud», à la page 910 et/ou «Configuration du collecteur de données Liberty pour les applications sur site», à la page 906.

- Pour le collecteur de données J2SE, après avoir mis à niveau le collecteur de données, reconfigurez ce dernier. Pour obtenir des instructions, voir «Configuration de la surveillance de J2SE», à la page 461.
- Pour le collecteur de données Ruby, après avoir mis à niveau le collecteur de données, reconfigurez ce dernier. Pour obtenir des instructions, voir «Configuration du collecteur de données Ruby pour les applications IBM Cloud», à la page 745.

Résultats

Le collecteur de données est mis à niveau vers la version la plus récente.

Chapitre 12. Traitement des incidents et support

Consultez les entrées sur le traitement des incidents que vous pouvez rencontrer lors de l'installation, la configuration ou l'utilisation de IBM Cloud Application Performance Management.

Le contenu de traitement des incidents est disponible dans ce Knowledge Center. Auparavant, le contenu de traitement des incidents était disponible dans forum Cloud Application Performance Management sous developerWorks. Vous pouvez continuer à rechercher des entrées plus anciennes sur ce forum. Recherchez les entrées qui commencent par "Traitement des incidents".

Pour le traitement des incidents liés à la Passerelle hybride d'IBM Cloud Application Performance Management, voir «Gestion de la passerelle hybride», à la page 989.

Traitement des incidents liés aux agents

Traitez les incidents liés à l'installation et la configuration de l'agent .

Nous migrons notre contenu de traitement des incidents depuis le forum Cloud Application Performance Management de developerWorks vers ce Knowledge Center. Auparavant, le contenu de traitement des incidents était disponible dans forum Cloud Application Performance Management sous developerWorks. Vous pouvez continuer à rechercher des entrées plus anciennes sur ce forum. Recherchez les entrées qui commencent par "Traitement des incidents".

Internet Service Monitoring

Vous trouverez ici de plus amples informations sur les problèmes connus d'Internet Service Monitoring.

Le profil ne sera pas créé une fois que la page création de profil est ouverte pendant plus de 10 minutes et qu'un autre profil portant le même nom ne sera pas créé

Incident

Le profil ne sera pas créé une fois que la **page créer un profil** est ouverte pendant plus de 10 minutes et qu'un autre profil portant le même nom ne sera pas créé.

Symptôme

Lors de la création d'un profil si l'utilisateur garde la **page créer un profil** inactive (ouverte sans activité) pendant plus de 10 minutes, puis tente de créer le profil, il ne sera pas créé. Après cela, si l'utilisateur tente de créer à nouveau le profil avec le même nom, le profil ne sera pas créé.

Cause

Un fichier de verrouillage est créé au niveau MIN au moment de la création du profil et verrouille l'activité de création de profil pour le même profil pour les autres utilisateurs. Le fichier de verrouillage est supprimé après la création du profil. Mais si la fenêtre de création est inactive pendant plus de 10 minutes, l'événement de création est verrouillé et l'utilisateur ne peut pas créer le profil.

Solution

- L'utilisateur ne doit pas laisser la fenêtre inactive pendant plus de 10 minutes lors de la création d'un profil.
- L'administrateur peut supprimer le fichier de verrouillage du profil créé à partir du côté MIN dans le chemin `/opt/ibm/wlp/usr/servers/min/dropins/CentralConfigurationServer.war/data_source/is`.
  Par exemple, si le nom de profil est ABC, un fichier de verrouillage `$$ABC$$1UjQ9wy1boIHTAQeoWSj1IU.lock` est créé.

Surveillance de Microsoft Active Directory

Vous trouverez ici de plus amples informations sur les problèmes connus de la surveillance de Microsoft Active Directory.

L'agent Microsoft Active Directory n'affiche pas le contenu à jour de l'aide en ligne

Incident

Les pages de l'aide en ligne ne sont pas mises à jour avec le contenu le plus récent de l'agent Microsoft Active Directory.

Symptôme

Dans l'aide Eclipse du tableau de bord APM pour l'agent Microsoft Active Directory, le contenu d'aide n'est pas affiché pour l'intervalle de collecte de données et la durée de conservation des groupes d'attributs ajoutés suivants :

- Services d'annuaire
- Vérificateur de cohérence kerberos
- Centre de distribution de clés kerberos
- Fournisseur de service d'annuaire
- Service d'annuaire Exchange

Cause

Le problème se produit en raison de la contrainte sur le serveur de génération.

Solution

L'utilisateur peut trouver le contenu d'aide dans les groupes d'attributs respectifs dans l'aide contextuelle du tableau de bord APM.

Remarque : Le problème apparaît dans APM version 8.1.4.10.

Surveillance de Microsoft IIS

Vous trouverez ici de plus amples informations sur les problèmes connus de Microsoft Internet Information Services.

Les pages de l'aide en ligne ne sont pas mises à jour avec le contenu le plus récent de l'agent Microsoft IIS APM.

Incident

Les pages de l'aide en ligne ne sont pas mises à jour avec le contenu le plus récent de l'agent Microsoft IIS APM.

Symptôme

Les groupes d'attributs nouvellement ajoutés ne sont pas affichés dans le contenu de l'aide en ligne :

- WPROCESS
- MEMIISUS
- Récupération de place d'ASP
- IISSVRINFO

Cause

Ce problème se produit en raison d'erreurs liées au serveur de génération.

Solution de contournement

Non disponible. Cependant, vous pouvez afficher le contenu de l'aide d'un groupe d'attributs particulier sur le tableau de bord APM.

Surveillance de Microsoft .NET

Vous trouverez ici de plus amples informations sur les problèmes connus de la surveillance de Microsoft .NET.

L'agent Microsoft .NET n'affiche pas le contenu d'aide en ligne mis à jour

Incident

Les pages de l'aide en ligne ne sont pas mises à jour avec le contenu le plus récent de l'agent Microsoft .NET.

Symptôme

Dans l'aide Eclipse du tableau de bord APM pour l'agent Microsoft .NET, le contenu d'aide de l'attribut Nom de la demande n'est pas affiché sous le groupe d'attributs Database Call Details.

Cause

Le problème se produit en raison de la contrainte sur le serveur de génération.

Solution

L'utilisateur peut trouver le contenu d'aide dans l'aide contextuelle du widget de groupe d'attributs Database Call Details sur le tableau de bord APM.

Remarque : Le problème apparaît dans APM version 8.1.4.10.

Surveillance de Microsoft SharePoint Server

Vous trouverez ici de plus amples informations sur les problèmes connus de la surveillance de Microsoft SharePoint Server.

L'agent Microsoft SharePoint Server n'affiche pas le contenu à jour de l'aide en ligne

Incident

Les pages de l'aide en ligne ne sont pas mises à jour avec le contenu le plus récent de l'agent MicrosoftSharePoint Server.

Symptôme

Dans l'aide Eclipse du tableau de bord APM pour l'agent MicrosoftSharePoint Server, le contenu d'aide n'est pas affiché pour les widgets de groupe nouvellement ajoutés appelés `Last 1 Hour Trace Log Count` et `Trace Log Details`.

Cause

Le problème se produit en raison de la contrainte sur le serveur de génération.

Solution

L'utilisateur peut trouver le contenu d'aide dans les widgets de groupe respectifs dans l'aide contextuelle du tableau de bord APM.

Remarque : Le problème apparaît dans APM version 8.1.4.10.

Surveillance de PostgreSQL

Vous trouverez ici de plus amples informations sur les problèmes connus de la surveillance de PostgreSQL.

Le widget Pourcentage de réussite de la mémoire tampon pour les bases de données sans connexion active n'affichent pas le contenu d'aide

Incident

Les informations ne sont pas disponibles pour les bases de données qui n'ont pas de connexions actives.

Symptôme

Les bases de données sans connexions actives ne sont pas affichées dans le widget Pourcentage de réussite de la mémoire tampon. Les informations doivent être affichées dans le contenu d'aide du widget.

Cause

Limitation due à la compatibilité avec IBM Cloud App Management.

Solution

Non disponible. L'utilisateur doit prendre note de la limitation.

Les valeurs de mémoire et d'adresse IP ne sont pas affichées sur la plateforme SUSE15

Incident

Les valeurs de mémoire et d'adresse IP ne sont pas affichées lorsque l'agent surveille le serveur PostgreSQL en local sur la plateforme SUSE15.

Symptôme

Les valeurs de mémoire et d'adresse IP ne sont pas affichées si l'agent surveille le serveur PostgreSQL sur la plateforme SUSE15.

Cause

La commande **`netstat`** échoue pour l'agent sur la plateforme SUSE15.

Solution

L'utilisateur peut utiliser la plateforme SUSE12 pour surveiller le serveur PostgreSQL en local.

Collecte des journaux d'agent de surveillance pour le support IBM

Utilisez l'outil de collecte d'identification de problème, *pdcollect*, pour rassembler les journaux requis et d'autres informations d'identification de problème demandées par le support IBM pour les agents de surveillance. L'outil de collecte PD est installé avec chaque agent de surveillance.

Avant de commencer
Des droits d'administrateur ou root sont requis pour que l'outil de collecte PD puisse rassembler les informations système des agents de surveillance. Vous pouvez consulter les journaux des agents individuellement dans les dossiers suivants :

- Windows [64 bits] *rép_install*\TMAITM6_x64\logs
- Windows [32 bits] *rép_install*\TMAITM6\logs
- Linux AIX *rép_install*/logs

Restriction : Il n'est possible d'exécuter qu'une seule instance du script `pdcollect`.

Pourquoi et quand exécuter cette tâche

L'emplacement par défaut de *rép_install* est :

- Windows `C:\IBM\APM`
- Linux `/opt/ibm/apm/agent`
- AIX `/opt/ibm/apm/agent`

Pour exécuter l'outil de collecte PD, procédez comme suit :

Procédure

1. Sur la ligne de commande, accédez au répertoire de l'agent :
   - Linux AIX *rép_install*`/bin`
   - Windows *rép_install*`\BIN`
2. Exécutez la commande suivante :
   - Linux AIX **`./pdcollect`**
   - Windows **`pdcollect`**

   Un fichier dont le nom comporte un horodatage est généré dans le répertoire `tmp`, comme `/tmp/pdcollect-nc049021.tar.Z`.
3. Envoyez les fichiers de sortie à votre représentant du support IBM.

Que faire ensuite

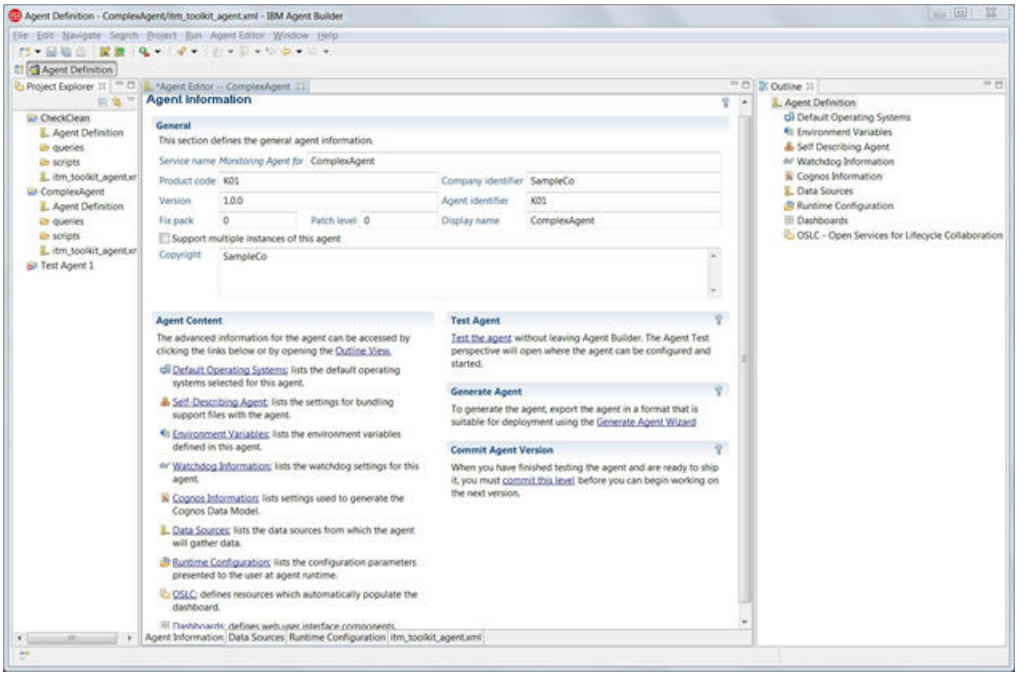
Si vous avez installé l'Agent Ruby et l'avez configuré pour les tableaux de bord de diagnostic, exécutez l'outil de collecte kkm, *kkmCollector*, sur des systèmes Linux afin de rassembler les fichiers de configuration, les fichiers de sortie, comme des fichiers JSO et des fichiers journaux.

1. Accédez au répertoire *rép_install*`/lx8266/km/bin`.
2. Exécutez la commande **`./kkmCollector`**

   Un fichier dont le nom comporte un horodatage est généré dans le répertoire `tmp`, comme `/tmp/kkm_dchome.tar.gz`
3. Envoyez les fichiers de sortie à votre représentant du support IBM.

Chapitre 13. Agent Builder

L'outil IBM Agent Builder offre une interface graphique permettant de créer, de modifier, de déboguer et de conditionner des agents pour surveiller les sources de données dans IBM Cloud Application Performance Management.



Présentation d'Agent Builder

Vous pouvez utiliser IBM Agent Builder pour créer et modifier des agents personnalisés qui développent les fonctions de surveillance d'un environnement IBM Tivoli Monitoring ou IBM Cloud Application Performance Management. Un agent personnalisé utilise ces environnements pour surveiller tout type de logiciel interne ou personnalisé.

Agent Builder est basé sur l'environnement de développement intégré open source Eclipse.

Agent Builder inclut les fonctions suivantes pour les environnements Tivoli Monitoring et Cloud APM :

Définir et modifier des agents
Vous pouvez créer et modifier des agents. Les agents collectent et analysent les données sur l'état et les performances de différentes ressources, telles que les disques durs, la mémoire, l'unité centrale ou les applications et fournissent ces données à l'environnement de surveillance.

Tester et préparer des agents pour déploiement
Vous pouvez tester un agent dans Agent Builder en collectant des données sur l'hôte sur lequel Agent Builder s'exécute (dans certains cas, vous pouvez également collecter des informations sur un autre hôte). Vous pouvez mettre l'agent en package pour faciliter sa distribution et son déploiement.

Les fonctions supplémentaires suivantes sont disponibles pour Tivoli Monitoring :

Espaces de travail, situations et commandes Action personnalisés
Vous pouvez utiliser Agent Builder pour mettre en package des espaces de travail, situations et commandes Action supplémentaires sous forme d'extensions de prise en charge d'application avec un nouvel agent ou un agent existant exécuté dans l'environnement Tivoli Monitoring.

Modèles de données de rapport
Vous pouvez utiliser Agent Builder pour générer un modèle de données Cognos qui vous permet à son tour de créer des rapports Tivoli Common Reporting. Ces rapports peuvent être fournis dans le cadre de votre image d'agent.

Procédures Agent Builder communes

Le tableau ci-dessous répertorie les principales procédures que vous pouvez exécuter avec Agent Builder.

Vous pouvez utiliser Agent Builder pour créer des agents pour les environnements IBM Tivoli Monitoring et IBM Cloud Application Performance Management. Vous pouvez également l'utiliser pour créer des extensions de prise en charge d'application pour l'environnement Tivoli Monitoring. Les extensions de prise en charge d'application sont créées en générant des espaces de travail et des situations pour améliorer un ou plusieurs agents existants.

Avant d'utiliser Agent Builder, vous devez l'installer. Pour plus d'informations, voir «Installation et démarrage d'Agent Builder», à la page 1199.

Pour créer, tester et utiliser un agent, suivez les procédures de la table suivante, dans l'ordre indiqué :

Tableau 257. Informations de référence pour la création d'agents

Objectif	**Reportez-vous à**
Création d'un agent à l'aide de l'assistant **Agent**.	• «Création d'un agent», à la page 1204
Création de sources de données et d'attributs pour votre agent. **Important :** Pour un environnement Cloud APM, un tableau de bord récapitulatif peut afficher jusqu'à cinq attributs ; l'un des attributs doit indiquer le statut global de l'agent ou du sous-noeud.	• «Modification des propriétés de sources de données et d'attributs», à la page 1227
(Pour l'environnement Tivoli Monitoring) Création d'espaces de travail et de situations pour votre agent • Exécution de Tivoli Monitoring version 6.1 avec le groupe de correctifs 1 au minimum • Remise à "00" de la version de la solution Tivoli Universal Agent • Définition de la valeur d'"AppTag"	• «Création d'espaces de travail, de commandes Action et de situations», à la page 1411 • «Importation des fichiers de prise en charge de l'application», à la page 1447
(Pour l'environnement Cloud APM) Création de définitions de ressource et de tableaux de bord pour votre agent	• «Préparation de l'agent pour Cloud APM», à la page 1417
(Pour l'environnement Tivoli Monitoring) Création de modèles de données Cognos pour les rapports pour votre agent	• «Génération d'un modèle de données Cognos», à la page 1519
Test et débogage de votre agent créé en garantissant la disponibilité des informations de surveillance.	• «Test de votre agent dans Agent Builder», à la page 1420 • «Options de ligne de commande», à la page 1457 • «Utilisation de l'éditeur d'agent pour modifier l'agent», à la page 1207.
Génération d'un package d'installation et installation de l'agent sur l'hôte surveillé.	• «Installation d'un agent», à la page 1430

Tableau 257. Informations de référence pour la création d'agents (suite)	
Objectif	**Reportez-vous à**
Suppression d'un agent créé à l'aide d'Agent Builder.	• «Désinstallation d'un agent», à la page 1445

Vous pouvez également utiliser Agent Builder pour mettre en package des espaces de travail, situations et commandes Action personnalisés sous forme d'extensions de prise en charge d'application pour les agents existants. Ces fonctions ne sont disponibles que pour l'environnement Tivoli Monitoring :

Tableau 258. Informations de références pour créer d'autres fonctions	
Objectif	**Reportez-vous à**
Création d'espaces de travail, de situations et de commandes Action personnalisés.	• «Création d'espaces de travail, de commandes Action et de situations», à la page 1411
Mise en package de votre extension de support d'application.	• «Création d'extensions de prise en charge d'application pour des agents existants», à la page 1516
Génération de regroupements personnalisés.	• «Création d'ensembles de fichiers sans agent», à la page 1540

Sources de données et fichiers

Un agent peut surveiller les informations à partir d'une ou plusieurs sources de données. Il présente les informations à l'infrastructure de surveillance sous la forme d'attributs, organisés en fichiers.

Quand vous créez un agent, vous devez définir une *source de données* correspondante. Vous pouvez ajouter d'autres sources de données. La source de données définit comment l'agent regroupe les informations de surveillance.

Vous pouvez utiliser Agent Builder pour créer des agents qui utilisent des informations de surveillance des sources de données à partir des *fournisseurs de données* suivants :

- Disponibilité des processus et des services
- Disponibilité du système de réseau (avec la commande PING ICMP)
- Codes retour de commande
- Sortie de script
- Journal des événements Windows
- Windows Management Instrumentation (WMI)
- Windows Performance Monitor (Perfmon)
- Protocole SNMP (Simple Network Management Protocol)
- Evénements SNMP
- Disponibilité et temps de réponse du protocole HTTP
- SOAP ou autre source de données HTTP
- Java Database Connectivity (JDBC)
- Interface de programme d'application Java (API)
- Java Management Extensions (JMX)
- Modèle CIM (Common Information Model)
- Fichiers journaux
- Journaux binaires AIX
- Socket

Vous pouvez également utiliser d'autres outils de développement pour créer des applications de surveillance personnalisées qui transmettent les informations à l'agent via un journal, une sortie de script et les source de données de l'API Java.

Quand vous ajoutez une source de données, Agent Builder ajoute le *fichier* correspondant à l'agent. Le fichier organise les informations présentées à l'environnement de surveillance. Dans IBM Tivoli Monitoring, un fichier est connu comme *groupe d'attributs*.

Un fichier peut se composer de plusieurs *attributs*, qui sont des valeurs fournies par la source de données. Chaque fois que l'environnement de surveillance interroge l'agent, il extrait des valeurs des sources de données et les renvoie comme attributs dans les fichiers.

Certaines sources de données peuvent renvoyer plusieurs *lignes* de valeurs d'attribut dans la même requête. Par exemple, si la source de données surveille plusieurs services en une seule fois.

La plupart des sources de données présentent les informations sous forme de fichier unique. Les sources de données SNMP et JMX peuvent, selon la configuration, fournir plusieurs ensembles d'informations. Lorsque vous ajoutez une source de données SNMP ou JMX, Agent Builder crée plusieurs fichiers pour s'adapter à ces informations.

Vous pouvez éditer les fichiers pour filtrer les données et pour créer des attributs *dérivés* supplémentaires, à savoir calculés à partir d'attributs existants avec une formule. Vous pouvez également joindre des fichiers, en créant un nouveau fichier avec des informations de deux fichiers ou plus. De cette façon, les utilisateurs peuvent afficher des informations combinées à partir de différentes sources de données.

Dans IBM Tivoli Monitoring, vous pouvez afficher tout le contenu d'attribut. Vous pouvez également créer des espaces de travail qui présentent des informations à partir de tous les fichiers d'agent dans une vue personnalisée. Vous pouvez utiliser IBM Tivoli Monitoring pour créer des situations déclenchées quand n'importe quel attribut atteint une certaine valeur. Une situation peut émettre une alerte et appeler une commande de système.

Dans IBM Cloud Application Performance Management, vous devez définir un tableau de bord *récapitulatif* pour l'agent, en sélectionnant jusqu'à cinq attributs visibles dans le tableau de bord. Vous pouvez également définir un tableau de bord des *détails* qui affiche les informations des fichiers sous forme de tables. Vous pouvez créer des seuils déclenchés lorsqu'un attribut atteint une certaine valeur ; vous n'êtes pas obligé d'ajouter cet attribut au tableau de bord. Un seuil peut émettre des alertes.

Surveillance de plusieurs serveurs ou instances de serveur

Un agent peut surveiller plusieurs serveurs, y compris plusieurs instances du même serveur. Il existe deux moyens de créer de tels agents : avoir plusieurs instances d'un agent et des sous-noeuds dans un agent.

L'utilisation de plusieurs instances est une méthode standard permettant de surveiller les serveurs d'applications qui peuvent avoir un certain nombre d'instances semblables sur le même hôte. De nombreux agents standard dans IBM Tivoli Monitoring et IBM Cloud Application Performance Management prennent en charge plusieurs instances.

Avec *plusieurs instances*, vous installez un agent sur des hôtes surveillés, puis configurez une ou plusieurs instances, en définissant un nom pour chacune d'entre elles. Configurez une instance de l'agent pour chaque instance du serveur à surveiller. Chaque instance est une copie identique distincte de l'agent et peut être démarrée et arrêtée séparément.

Vous pouvez également définir un ou plusieurs types de *sous-noeud* dans un agent. Chaque type doit correspondre à un type de ressource différent pouvant être surveillé par un agent. Un type de sous-noeud contient des sources de données et des fichiers ; vous pouvez également définir des sources de données et des fichiers au niveau de l'agent, en dehors de tout sous-noeud. Quand vous installez l'agent sur un hôte, vous pouvez configurer le nombre obligatoire de sous-noeuds de chaque type ; pour chaque type de sous-noeud, vous pouvez définir le nombre de sous-noeuds de manière indépendante. Pour IBM Cloud Application Performance Management, vous pouvez créer un tableau de bord pour l'agent et un tableau de bord distinct pour chaque sous-noeud.

Les sous-noeuds ont besoin d'étapes de configuration différentes sur l'hôte surveillé. En outre, pour reconfigurer le système, pour ajouter ou supprimer un sous-noeud, vous devez arrêter et redémarrer tout l'agent; une instance peut être reconfigurée, ajoutée ou supprimée sans affecter d'autres instances. Cependant, les sous-noeuds ont un certain nombre d'avantages :

- Avec des sous-noeuds, vous pouvez surveiller un grand nombre d'instances de serveur tout en consommant moins de ressources. En général, le nombre d'instances d'agent d'un type spécifique pris en charge sur un système unique est 10. Cependant, un agent peut surveiller jusqu'à 100 serveurs locaux ou distants à l'aide de sous-noeuds.
- Un seul agent peut inclure des types de sous-noeud pour quelques types de serveurs différents. Sur le système contrôlé, vous pouvez configurer n'importe quel nombre de sous-noeuds de chaque type. Vous pouvez utiliser cette fonction pour préserver des ressources.
- Un agent avec des sous-noeuds peut fournir des données système au niveau de l'agent.

Vous pouvez définir à la fois plusieurs instances et sous-noeuds pour le même agent. Dans ce cas, chaque instance peut inclure un certain nombre de sous-noeuds. Vous pouvez arrêter et redémarrer chaque instance indépendamment d'autres instances ; tous les sous-noeuds d'une instance sont arrêtés et redémarrés ensemble.

Test, installation et configuration d'un agent

Vous pouvez créer un module d'installation pour un agent et l'installer sur n'importe quel nombre d'hôtes surveillés. Pour certaines sources de données, vous devez définir des valeurs de configuration pour collecter des données.

Après avoir défini des sources de données et des attributs pour un agent, vous pouvez le tester en l'exécutant dans Agent Builder. Vous pouvez tester un fichier unique (groupe d'attributs) ou l'agent complet.

Pour tester l'agent de manière plus étendue et pour l'utiliser, vous pouvez créer une image d'installation. Cette image fournit des scripts pour installer et configurer l'agent sur n'importe quel hôte surveillé.

Conseil : Avant d'installer l'agent, assurez-vous que l'agent de système d'exploitation de votre environnement de surveillance (IBM Tivoli Monitoring ou IBM Cloud Application Performance Management) est installé sur l'hôte.

Après avoir installé l'agent, vous devrez sans doute le configurer. Si l'agent prend en charge plusieurs instances, vous devez configurer l'agent pour créer au moins une instance.

Certaines sources de données nécessitent des valeurs de configuration supplémentaires ; par exemple, pour la source de données de SNMP, vous devez configurer l'adresse IP de l'hôte que vous surveillez avec le protocole de SNMP. Utilisez le script de configuration déployé par le module d'installation pour définir ces valeurs.

Vous pouvez également définir ces valeurs dans Agent Builder avant de créer l'image d'installation. Dans ce cas, vous n'avez pas besoin de les redéfinir sur les hôtes surveillés.

Conseil : Les fichiers d'aide pour votre agent personnalisé peuvent ne pas s'afficher dans le Contenu de l'aide après la mise à niveau du serveur Cloud APM. Pour afficher les fichiers d'aide, effectuez les étapes suivantes :

1. Téléchargez la dernière version d'IBM Agent Builder à partir de votre abonnement Cloud APM dans IBM Marketplace.
2. Recréez votre agent personnalisé. Veillez à affecter un numéro de version, un groupe de correctifs ou un niveau de module de correction supérieur dans la page Informations sur l'agent.
3. Installez votre agent personnalisé sur l'hôte surveillé.
4. Dans la Console Cloud APM, cliquez sur **Aide** > **Contenu de l'aide** dans la barre de navigation. Votre agent personnalisé s'affiche.

Configuration requise pour le système d'exploitation

Les agents créés avec Agent Builder sont pris en charge sur divers systèmes d'exploitation, selon l'environnement de surveillance et les paramètres que vous sélectionnez lors de la création de l'agent.

Dans un environnement Tivoli Monitoring, les agents créés par Agent Builder peuvent prendre en charge les systèmes d'exploitation suivants :

- AIX
- HP-UX
- Linux
- Solaris
- Authentification Windows

Les agents prennent en charge les mêmes versions de système d'exploitation que les agents de système d'exploitation. Pour plus de détails, accédez au site Web Software Product Compatibility Reports. Recherchez le nom de produit `Tivoli Monitoring` et cochez la case du composant `OS Agents & TEMA (Tivoli Enterprise Monitoring Agent)`.

Dans un environnement IBM Cloud Application Performance Management, les agents créés par Agent Builder peuvent prendre en charge les systèmes d'exploitation suivants :

- AIX
- Linux
- Authentification Windows

Les agents prennent en charge les mêmes versions que les agents de système d'exploitation. Pour plus de détails, utilisez les liens dans la section Component de System requirements (APM Developer Center).

Pour exécuter votre agent de surveillance dans un environnement Tivoli Monitoring, installez l'agent de système d'exploitation approprié sur chaque système contrôlé où votre agent s'exécute.

Pour exécuter votre agent de surveillance dans un environnement IBM Cloud Application Performance Management, installez l'un des agents fourni avec IBM Cloud Application Performance Management sur chaque système contrôlé où votre agent s'exécute.

Remarque : Les navigateurs d'Agent Builder utilisent les sources de données et les informations accessibles à partir du système sur lequel Agent Builder est exécuté. Veillez à exécuter Agent Builder sur l'un des types de systèmes suivants :

- Un système qui fonctionne au même niveau que le système d'exploitation et les applications surveillées pour lesquelles vous développez l'agent.
- Un système qui se connecte à un autre système qui fonctionne au même niveau que le système d'exploitation et les applications surveillées pour lesquelles vous développez l'agent.

Fonctions spécifiques à IBM Tivoli Monitoring

Agent Builder fournit plusieurs fonctions qui s'appliquent seulement à IBM Tivoli Monitoring.

Vous pouvez utiliser des groupes de navigation pour organiser les données que l'agent affiche dans les vues Navigateur et les espaces de travail IBM Tivoli Monitoring. Un groupe de navigation combine les données à partir de plusieurs groupes d'attributs (fichiers) dans une vue unique, tout en masquant les fichiers distincts originaux de l'utilisateur.

Vous pouvez utiliser Tivoli Enterprise Portal pour créer des espaces de travail, des situations et des commandes Action pour votre agent. Vous pouvez alors utiliser Agent Builder pour sauvegarder les espaces de travail, les situations, et les commandes Action comme fichier de supports d'application et pour les regrouper avec l'agent. D'ailleurs, Agent Builder peut également importer des espaces de travail, des situations et des commandes Action pour d'autres agents et créer des fichiers d'assistance d'application personnalisée pour ces éléments.

Agent Builder peut générer un modèle de données Cognos pour l'agent. Utilisez le modèle de données pour importer des informations sur l'agent dans Cognos Framework Manager, composant d'IBM Tivoli Common Reporting, pour créer des rapports.

Installation et démarrage d'Agent Builder

Avant d'installer IBM Agent Builder, vérifiez que le système remplit les conditions requises. Puis, utilisez l'assistant d'installation ou la procédure d'installation en mode silencieux pour installer Agent Builder.

Conseil : Pour obtenir des informations sur l'installation ou la modification d'un *agent*, voir «Installation d'un agent», à la page 1430.

Conditions préalables à l'installation et l'exécution d'Agent Builder

Pour installer et exécuter Agent Builder, votre système doit répondre à certaines conditions.

Avant d'installer Agent Builder, vérifiez que vous disposez d'un :

- Système doté d'au moins 1 Go d'espace disque libre. Les agents que vous développez auront besoin d'un espace disque supplémentaire.
- Système d'exploitation compatible. Agent Builder peut s'exécuter sur les systèmes d'exploitation suivants :
  - Windows Windows
  - Linux Linux (x86 64 bits uniquement)
- Linux Si vous utilisez le système d'exploitation Linux, vous devez installer la bibliothèque `libstdc++.so.5`. Vous pouvez installer les packages suivants qui contiennent cette bibliothèque :
  - Sur Red Hat Enterprise Linux, `compat-libstdc++-33`
  - Sur SUSE Enterprise Linux, `libstdc++-33`

Windows Sur un système Windows, vous devez pouvoir exécuter Agent Builder en tant qu'utilisateur disposant des droits d'administrateur. Ces droits garantissent que l'environnement d'Agent Builder est cohérent avec les agents développés avec celui-ci.

Linux Sur un système Linux, vous pouvez exécuter Agent Builder en tant que superutilisateur ou utilisateur standard. Toutefois, si vous l'exécutez en tant qu'utilisateur standard, le test des agents sera limité et risque de ne pas être disponible dans certains cas.

Configuration requise détaillée d'Agent Builder

Utilisez les rapports de compatibilité des produits logiciels pour afficher la configuration requise détaillée d'Agent Builder.

Accédez au site Web de Software Product Compatibility Reports et recherchez le nom de produit `IBM Agent Builder`.

Installation d'Agent Builder

Vous pouvez utiliser l'assistant d'installation ou la procédure d'installation automatique pour installer Agent Builder.

Conseil : Avant d'installer Agent Builder, désinstallez les versions précédentes. Pour plus d'informations sur la désinstallation, voir («Désinstallation d'Agent Builder», à la page 1203). Aucune des données concernant vos agents existants ne sont perdues lors de la désinstallation.

Installation d'Agent Builder à l'aide de l'assistant d'installation

Vous pouvez utiliser l'assistant d'installation pour installer IBM Agent Builder.

Avant de commencer

Vérifiez que le système répond aux conditions requises. Pour plus d'informations sur les conditions requises, voir «Conditions préalables à l'installation et l'exécution d'Agent Builder», à la page 1199

Procédure

1. Si vous n'êtes pas connecté à IBM Marketplace, connectez-vous avec vos ID utilisateur et mot de passe IBM, et accédez à **Produits et services**.

   La page **Produits et services** est disponible pour les abonnés actifs. En cas de problème, accédez au forum Cloud Application Performance Management ou au Support Marketplace.
2. Téléchargez le fichier archive d'installation Agent Builder :
   a) Dans la boîte de souscription de Cloud APM, cliquez sur **Gérer** > **Téléchargements**.
   b) Sélectionnez **Multi-Platform** en tant que système d'exploitation.
   c) Sélectionnez le package IBM Agent Builder.
   d) Cliquez sur **Télécharger** et sauvegardez le fichier `IBM_Agent_Builder_Install.tar` sur votre système.
3. Procédez à l'extraction du fichier archive d'installation.
4. Utilisez la commande suivante dans le répertoire d'images extraites pour lancer l'installation :
   - Windows `setup.bat`
   - Linux AIX `./setup.sh`

   Important : Exécutez le programme d'installation avec le même ID utilisateur que celui avec lequel vous comptez exécuter Agent Builder.
5. Lorsque la fenêtre **IBM Agent Builder** s'ouvre, sélectionnez votre langue, puis cliquez sur **OK**.
6. Sur la page **Introduction**, cliquez sur **Suivant**.
7. Dans la page **Contrat de licence du logiciel**, cliquez sur **J'accepte les termes du contrat de licence**et cliquez sur **Suivant**.
8. Sur la page **Choix du dossier d'installation**, cliquez sur l'une des options suivantes :
   - **Suivant** pour installer Agent Builder dans le répertoire indiqué dans la zone **Indiquez le dossier dans lequel installer le produit**.
   - **Restaurer le dossier par défaut** pour installer Agent Builder dans un répertoire par défaut.
   - **Choisir** pour sélectionner un répertoire différent.

   Remarque : Le nom de répertoire choisi ne doit pas contenir les caractères suivants :

   !
   #
   %
   ;

   S'il contient l'un de ces caractères, Agent Builder risque de ne pas démarrer.
9. Sur la page **Récapitulatif avant installation**, cliquez sur **Installer**.
10. Sur la page **Installation d'IBM Agent Builder**, attendez que la page **Installation terminée** s'ouvre, puis cliquez sur **Terminé**.

Résultats

Windows Une fois Agent Builder installé, une option est ajoutée au menu Démarrer et une icône Agent Builder est ajoutée sur votre bureau. Les fichiers journaux d'installation se trouvent dans le répertoire *rép_install*\IBM_Agent_Builder_InstallLog.xml.

Linux AIX Une fois Agent Builder installé, le fichier exécutable d'Agent Builder se nomme *emplacement_install*/agentbuilder. Les fichiers journaux d'installation se trouvent dans le répertoire *rép_install*/IBM_Agent_Builder_InstallLog.xml.

Installation en mode silencieux

Vous pouvez installer Agent Builder au moyen d'une méthode d'installation en mode silencieux. Cette méthode ne nécessite pas d'environnement graphique et peut facilement être répliquée sur plusieurs hôtes.

Pourquoi et quand exécuter cette tâche

Le fichier d'options d'installation en mode silencieux, installer.properties, est inclus dans l'image d'installation à la racine du répertoire d'installation. Vous devez modifier ce fichier pour répondre à vos besoins, puis exécuter le programme d'installation en mode silencieux. Vous pouvez copier ce fichier sur d'autres hôtes et installer rapidement Agent Builder sur tous les hôtes.

Procédure

1. Si vous n'êtes pas connecté à IBM Marketplace, connectez-vous avec vos ID utilisateur et mot de passe IBM, et accédez à **Produits et services**.

   La page **Produits et services** est disponible pour les abonnés actifs. En cas de problème, accédez au forum Cloud Application Performance Management ou au Support Marketplace.
2. Téléchargez le fichier archive d'installation Agent Builder :
   a) Dans la boîte de souscription de Cloud APM, cliquez sur **Gérer** > **Téléchargements**.
   b) Sélectionnez **Multi-Platform** en tant que système d'exploitation.
   c) Sélectionnez le package IBM Agent Builder.
   d) Cliquez sur **Télécharger** et sauvegardez le fichier IBM_Agent_Builder_Install.tar sur votre système.
3. Procédez à l'extraction du fichier archive d'installation.
4. Créez une copie du fichier installer.properties qui se trouve dans le répertoire d'image d'installation.
5. Editez le nouveau fichier et adaptez-le à vos besoins. Vous trouverez ci-dessous un exemple de contenu :

```
# ------------------------------------------------------------------------
# IBM Agent Builder
#
# (C) Copyright IBM Corporation 2009.  All rights reserved.
#
# Fichier de réponses exemple pour l'installation en mode silencieux
#
# Pour utiliser ce fichier, utilisez la commande suivante :
#
# Windows :
#    setup.bat -i silent -f <chemin>\installer.properties
#
# Linux ou AIX :
#    setup.sh -i silent -f <chemin>/installer.properties
#
# Où
#    <chemin> représente le chemin complet du fichier installer.properties
#    (comprenant la lettre de l'unité ou le nom de chemin UNC sous Windows).
#    <chemin> ne peut pas contenir d'espaces.
# ------------------------------------------------------------------------


# ------------------------------------------------------------------------
```

```
# Cette propriété indique que la licence a été acceptée
# ------------------------------------------------------------------
# LICENSE_ACCEPTED=FALSE

# ------------------------------------------------------------------
# Cette propriété indique le répertoire d'installation
#
# Sous Windows, la valeur par défaut est :
#     C:\\Program Files (x86)\\IBM\\AgentBuilder
#
# Sous Linux, la valeur par défaut est :
#     /opt/ibm/AgentBuilder
# ------------------------------------------------------------------
#USER_INSTALL_DIR=C:\\Program Files (x86)\\IBM\\AgentBuilder
#USER_INSTALL_DIR=/opt/ibm/AgentBuilder
```

6. Démarrez l'installation en mode silencieux en exécutant la commande suivante dans le répertoire d'image d'installation extrait :

   Windows `setup.bat -i silent -f chemin/installer.properties`

   Linux AIX `./setup.sh -i silent -f chemin/installer.properties`

   où *chemin* représente le chemin complet du fichier `installer.properties` (y compris l'identificateur d'unité ou le nom de chemin UNC sous Windows). Le chemin ne doit pas contenir d'espace.

Démarrage d'Agent Builder

Une fois que vous avez installé Agent Builder, vous pouvez le démarrer.

Procédure

- Démarrez Agent Builder à l'aide de l'une des méthodes suivantes :
  - Windows Sur les systèmes Windows :
    - A partir d'une ligne de commande : *Emplacement_Installation*\agentbuilder.exe.
    - Sélectionnez **Démarrer** > **Tous les programmes** > **IBM** > **Agent Builder**.
    - Cliquez sur l'icône **Agent Builder sur le bureau**.
  - Linux Sur les systèmes Linux, lancez le fichier exécutable suivant : *REP_INSTALL*/agentbuilder

  Remarque : Lorsque vous exécutez Agent Builder, il vous demande l'emplacement de votre répertoire d'espace de travail. Les fichiers qui créent vos agents sont enregistrés dans ce répertoire. Vous pouvez désigner n'importe quel répertoire comme espace de travail.

Définition du navigateur par défaut dans Agent Builder

Linux Sur les systèmes Linux, il peut s'avérer nécessaire de définir le navigateur par défaut d'Agent Builder pour que les écrans d'aide s'affichent.

Procédure

1. Sélectionnez **Fenêtre** > **Préférences** pour ouvrir la fenêtre **Préférences**.
2. Sélectionnez et développez le noeud **Général**.
3. Sélectionnez **navigateur Web**.
4. Sélectionnez **Utiliser un navigateur Web externe**.
5. Sélectionnez le navigateur à utiliser.
6. Facultatif : Pour ajouter un navigateur Web, procédez comme suit :
   a) Cliquez sur **Nouveau**.
   b) Dans la zone **Nom**, entrez un nom descriptif pour le navigateur.

c) Dans la zone **Emplacement**, saisissez le chemin d'accès complet vers le fichier exécutable du navigateur.

d) Cliquez sur **OK**.

7. Cliquez sur **OK**.

Définition de l'autorité d'horodatage par défaut dans Agent Builder

Vous pouvez définir l'autorité d'horodatage des fichiers JAR dans la fenêtre **Préférences** d'Agent Builder. Si le certificat de signataire de l'autorité d'horodatage par défaut arrive à expiration, en définissant une nouvelle autorité, vous pouvez continuer de vérifier les fichiers JAR.

Procédure

1. Sélectionnez **Fenêtre** > **Préférences** pour ouvrir la fenêtre **Préférences**.
2. Sélectionnez et développez le noeud **IBM Agent Builder**.
3. Sélectionnez **Signature de fichiers JAR**.
4. Sélectionnez **Ajouter un horodatage aux fichiers JAR signés**.
5. Entrez l'URL de l'autorité d'horodatage.
6. Cliquez sur **OK**.

Désinstallation d'Agent Builder

Selon votre système d'exploitation, vous pouvez utiliser différentes procédures pour désinstaller Agent Builder.

Procédure

- Linux

  Sur les systèmes Linux, exécutez la commande suivante :

  a) *REP_INSTALL*`/uninstall/uninstaller`

  où *REP_INSTALL* représente le nom du répertoire dans lequel Agent Builder est installé.

- Windows

  Sous Windows 7, Windows Server 2008 R2 et les versions ultérieures de Windows, procédez comme suit :

  a) Ouvrez Windows Programmes et fonctionnalités en sélectionnant **Démarrer** > **Panneau de configuration** > **Programmes** > **Programmes et fonctionnalités**.

  b) Sélectionnez **IBM Agent Builder** dans la liste des programmes installés.

  c) Cliquez sur **Désinstaller/Modifier**.

  d) Cliquez sur **Désinstaller** sur la page de **désinstallation d'IBM Agent Builder**.

  e) Cliquez sur **Terminé** sur la page **Désinstallation terminée**.

  Conseil : Sous Windows 7 et Windows Server 2008 R2, vous pouvez également accéder à la fenêtre **Programmes et fonctionnalités Windows** en sélectionnant **Démarrer** > **Ordinateur** > **Désinstaller ou modifier un programme**. Continuez ensuite à partir de l'étape «2», à la page 1203.

- Windows

  Sur les autres systèmes Windows, procédez comme suit :

  a) Dans le Panneau de configuration Windows, sélectionnez **Ajout/Suppression de programmes**.

  b) Cliquez sur **IBM Agent Builder**.

  c) Cliquez sur **Modifier/Supprimer**.

- Sur tous les systèmes d'exploitation, vous pouvez également utiliser la méthode de désinstallation en mode silencieux. Démarrez la désinstallation en mode silencieux en exécutant la commande suivante :

- Windows Sur les systèmes Windows, *REP_INSTALL*`/uninstall/uninstaller.exe -i silent`
- Linux Sur les systèmes Linux, *REP_INSTALL*`/uninstall/uninstaller -i silent`

Désinstallation en mode silencieux

Vous pouvez utiliser la méthode de désinstallation silencieuse pour la désinstallation.

Procédure

- Démarrez la désinstallation en mode silencieux en exécutant la commande suivante :

```
REP_INSTALL/uninstall/uninstaller[.exe] -i silent
```

Création d'un agent

Pour commencer à créer un agent dans Agent Builder, utilisez le nouvel assistant de création d'agent. Cet assistant permet de définir la configuration de l'agent de base et de créer une source de données. Vous pouvez alors utiliser l'agent dans Agent Builder et ajouter plus de sources de données et d'autres options, notamment des sous-noeuds et des groupes de navigation.

Désignation et configuration de l'agent

Utilisez l'assistant d'**agent** pour nommer votre agent, définir sa version, ses systèmes d'exploitation pris en charge, ainsi que d'autres paramètres de configuration.

Procédure

1. Utilisez l'une des méthodes suivantes pour lancer l'assistant de création d'agent :
   a) Cliquez sur l'icône **Créer un agent** dans la barre d'outils.
   b) Dans le menu principal, sélectionnez **Fichier** > **Nouveau** > **Agent**.
   c) Dans le menu principal, sélectionnez **Fichier** > **Nouveau** > **Autre**. Sur la page de **sélection d'un assistant**, cliquez deux fois sur le dossier **Agent Builder**, puis deux fois sur **Agent**.

   L'assistant d'**agent** s'ouvre.
2. Cliquez sur **Suivant**.
3. Sur la page **Nouveau projet d'agent**, définissez le nom du projet dans la zone **Nom du projet**. Agent Builder utilise ce nom pour le dossier contenant les fichiers d'agent. Vous pouvez éventuellement modifier les paramètres suivants :
   - Pour stocker les fichiers d'agent à un emplacement différent, désélectionnez l'option **Utiliser l'emplacement par défaut** et cliquez sur **Parcourir** pour sélectionner le nouveau répertoire dans la zone **Emplacement**.
   - Vous pouvez modifier la façon dont la vue du navigateur Eclipse affiche les ressources, en les ajoutant dans diverses parties actives d'un programme. Pour plus d'informations, consultez l'aide Eclipse. Pour ajouter l'agent à des jeux de documents Eclipse, sélectionnez **Ajouter le projet aux parties actives d'un programme**, puis cliquez sur le bouton **Sélectionner** pour ajouter les jeux à la zone **Parties actives d'un programme**.
4. Cliquez sur **Suivant**.
5. Sur la page **Informations générales**, configurez les paramètres suivants :
   - Saisissez la mention de copyright que vous voulez utiliser pour vos nouveaux agents dans la zone **Copyright**. Cette mention doit satisfaire vos exigences légales de copyrights. Cette déclaration de droit d'auteur est insérée dans tous les fichiers générés pour l'agent ; vous pouvez la modifier ultérieurement.

- Sélectionnez les systèmes d'exploitation pour lesquels votre agent sera créé.

  Important : Pour exécuter un test complet de l'agent dans Agent Builder (pour obtenir des instructions, voir «Test complet de l'agent», à la page 1424), vérifiez que :

  – Si vous exécutez Agent Builder sous Windows, la version 32 bits du système d'exploitation est installée.
  – Si vous exécutez Agent Builder sous Linux, la version 64 bits du système d'exploitation est installée.

  Important : Dans certains cas, il se pourrait que vous deviez installer votre agent sur un système 64 bits où seul un agent de système d'exploitation 32 bits est installé. Dans ce cas, vérifiez que la version 64 bits du système d'exploitation n'est pas sélectionnée et que la version 32 bits est sélectionnée.

  Important : Les systèmes Windows Server 2003 R2 64 bits et les systèmes Windows antérieurs ne sont pas pris en charge par les agents créés à l'aide d'Agent Builder.

6. Cliquez sur **Suivant**.
7. Sur la page **Informations sur l'agent**, configurez les paramètres suivants :

- Définissez le nom de service pour l'agent dans la zone **Nom de service**. Ce nom s'affiche dans la fenêtre **Manage Tivoli Monitoring Services** dans un environnement IBM Tivoli Monitoring et dans l'utilitaire **Manage Monitoring Services** et l'éditeur de seuil dans IBM Cloud Application Performance Management. Sous Windows, il correspond également au nom du service Windows qui exécute l'agent. Le nom du service commence toujours par `Monitoring Agent for`. Vous devez entrer le reste du nom, qui décrit normalement le service surveillé par cet agent. Le nom peut contenir des lettres, des nombres, des espaces et des traits de soulignement.
- Définissez pour l'agent un code produit comportant trois caractères dans la zone **Code produit**. Ce code produit est requis pour IBM Tivoli Monitoring et IBM Cloud Application Performance Management. Une plage de codes produit est réservée pour l'utilisation avec Agent Builder. Les valeurs admises sont `K00-K99`, `K{0-2}{A-Z}` et `K{4-9}{A-Z}`.

  Important : Ces valeurs sont réservées à une utilisation interne uniquement et ne sont pas destinées aux agents prévus pour être partagés ou vendus en dehors de l'organisation. Si vous créez un agent à partager avec d'autres personnes, vous devez envoyer une note à toolkit@us.ibm.com pour réserver un code produit. La demande de code produit doit inclure une description de l'agent à générer. Un code produit est ensuite attribué et enregistré, puis il vous est renvoyé. Lorsque vous recevez le code produit de 3 lettres, vous devez permettre à Agent Builder d'utiliser le code produit attribué.
- Définissez une chaîne qui identifie de manière unique l'organisation ayant développé l'agent dans la zone **Identificateur de société** (`IBM` est réservé). Vous pouvez utiliser l'adresse URL de votre société ; par exemple, si le site Web de la société est `mycompany.com`, utilisez le texte `mycompany`.
- Définissez une chaîne qui identifie de manière unique l'agent dans la zone **Identificateur d'agent**. Par défaut, Agent Builder définit l'identificateur d'agent de sorte qu'il soit identique au code produit.

  Important : La longueur combinée de la zone **Identificateur d'agent** et de la zone **Identificateur de société** ne peut pas excéder 11 caractères.
- Définissez la version d'agent dans la zone **Version**. La version d'agent contient trois chiffres au format *V.R.R*, où :

  V = Version
  R = Edition
  R = Edition

  Aux fins de l'affichage dans l'environnement de surveillance, la valeur *V.R.R* est convertie au format suivant : `0V.RR.00.00`

Conseil : Dans l'éditeur d'agent, une zone de **niveau de correctif** est disponible. Elle peut être utilisée lorsque vous avez besoin d'appliquer un correctif pour un agent et que vous ne souhaitez pas mettre à jour la version.

- Si vous voulez que votre agent prenne en charge plusieurs instances, cochez la case **Prendre en charge plusieurs instances de cet agent**. Vous pouvez utiliser plusieurs instances d'un agent pour surveiller plusieurs instances d'une application sur un même hôte, ou vous pouvez utiliser un agent installé sur un hôte pour surveiller plusieurs serveurs logiciels sur différents hôtes. Lorsque vous installez un agent prenant en charge plusieurs instances, vous pouvez créer et configurer autant d'instances que nécessaire.

Que faire ensuite
Cliquez sur **Suivant** pour définir une source de données initiale pour votre agent. Pour plus d'informations, voir «Définition de sources de données initiales», à la page 1206.

Définition de sources de données initiales

Lorsque vous créez un agent, définissez les données initiales qui seront surveillées par l'agent. Vous pourrez ajouter d'autres sources de données ultérieurement dans l'éditeur d'agent.

Pourquoi et quand exécuter cette tâche
Définissez les sources de données que votre nouvel agent doit surveiller à l'aide de la page **Source de données initiale de l'agent**. Pour obtenir des instructions détaillées sur la création de sources de données associées à différents fournisseurs de données, voir «Définition et test de sources de données», à la page 1255.

Procédure

1. Sur la page **Source de données initiale de l'agent**, sélectionnez l'une des **Catégories de données de surveillance** et l'une des **Sources de données**.
2. Cliquez sur **Suivant**. L'assistant vous guide à travers le processus de définition et de configuration des types de collecte de données que vous indiquez.

   Conseil : Vous pouvez utiliser cet assistant pour définir une source de données ou pour ajouter un sous-noeud ou un groupe de navigation afin d'organiser l'agent. Pour plus d'informations sur les sous-noeuds, voir «Utilisation des sous-noeuds», à la page 1386. Pour plus d'informations sur les groupes de navigation, qui sont utilisés uniquement pour IBM Tivoli Monitoring, voir «Création d'un groupe de navigation», à la page 1385.
3. Si vous avez défini une nouvelle source de données susceptible de renvoyer plusieurs lignes de données, vous êtes invité à sélectionner des attributs de clé. Pour plus d'informations, voir «Sélection des attributs de clé», à la page 1206.
4. Une fois que vous avez défini la première source de données, la fenêtre **Définition de la source de données** s'affiche. Pour ajouter une autre source de données, sélectionnez l'agent, ou un sous-noeud ou un groupe de navigation, le cas échéant, puis cliquez sur le bouton **Ajouter à la sélection**.
5. Pour finir de définir les sources de données, cliquez sur **Terminer**. Agent Builder crée le nouvel agent et l'ouvre dans l'éditeur d'agent.

Sélection des attributs de clé
Lorsqu'un groupe d'attributs renvoie plusieurs lignes de données, vous devez sélectionner les attributs de clé.

Pourquoi et quand exécuter cette tâche

Lorsqu'un groupe d'attributs peut renvoyer plusieurs lignes de données, chaque ligne représente une entité surveillée. Chaque fois que des données surveillées sont échantillonnées, l'environnement de surveillance fait correspondre une ligne à l'entité surveillée et à des échantillons précédents pour cette entité. Cette mise en correspondance s'effectue à l'aide d'attributs de clé. Un ou plusieurs attributs du groupe d'attributs peuvent être identifiés comme attributs de clé. Ces attributs de clés, lorsqu'ils sont

utilisés conjointement, font la distinction entre une entité surveillée et une autre et ne changent pas d'un échantillon à l'autre lorsqu'il est fait référence à la même entité surveillée.

Les attributs de débit et delta sont calculés à l'aide de la comparaison de l'échantillon en cours à l'échantillon précédent, et les attributs de clé identiques garantissent que l'agent compare les valeurs pour la même entité surveillée. De même, Summarization and Pruning Agent fait la synthèse des échantillons qui comportent des attributs de clé identiques. De plus, vous pouvez également utiliser tout attribut défini en tant qu'attribut de clé comme "élément d'affichage" dans une situation.

Les détails relatifs à votre nouvelle source de données doivent être spécifiés sur la page **Source de données initiale de l'agent**. Si la source de données sélectionnée peut renvoyer plusieurs lignes de données, Agent Builder peut parfois identifier les attributs de clé. Sinon, il vous demande de les sélectionner.

Procédure

- Sur la page **Sélectionner les attributs clés**, effectuez l'une des actions suivantes :
  - Cliquez dans la liste sur un ou plusieurs attributs correspondant aux attributs de clé de cette entité. Pour sélectionner plusieurs attributs, maintenez la touche Ctrl enfoncée.
  - Si ce groupe d'attributs renvoie une seule ligne, sélectionnez **Génère une ligne de données unique**. Si cette option est sélectionnée, aucun attribut de clé n'est nécessaire car une seule entité surveillée est signalée dans ce groupe d'attributs.

Utilisation de l'éditeur d'agent pour modifier l'agent

L'éditeur d'agent permet de modifier, de sauvegarder et de valider une version de votre agent.

Vous pouvez créer un agent dans Agent Builder ; pour plus d'informations, voir «Création d'un agent», à la page 1204. Après avoir créé un agent, vous pouvez le modifier à l'aide de l'éditeur d'agent.

Pour ouvrir un agent créé dans Agent Builder, dans le panneau de l'**explorateur de projet** de l'éditeur d'agent, localisez le nom de l'agent et développez-le. Sous le nom de l'agent, cliquez deux fois sur **Définition d'agent**. Vous pouvez également cliquer deux fois sur le nom de fichier `itm_toolkit_agent.xml`.

L'éditeur d'agent est un éditeur Eclipse multipage qui vous permet de modifier les propriétés d'un agent existant. Chaque page de l'éditeur correspond à une fonction caractéristique de l'agent.

La liste des pages disponibles s'affiche dans la vue Structure sous le noeud **Définition d'agent**. Vous pouvez aisément passer d'une page à l'autre en cliquant sur un noeud dans la vue Structure. Si la vue Structure ne s'affiche pas ou est masquée par une autre vue, vous pouvez réinitialiser la perspective de définition d'agent. Pour cela, sélectionnez **Fenêtre** > **Réinitialiser la perspective**. Sinon, vous pouvez cliquer avec le bouton droit de la souris sur l'onglet **Définition d'agent** et sélectionner **Réinitialiser** dans le menu.

Remarque : Pour des informations détaillées et des procédures pour créer un agent, voir «Création d'un agent», à la page 1204.

Les pages suivantes sont incluses dans l'éditeur d'agent :

- «Page Informations sur l'agent», à la page 1208
- Page Définition de la source de données
- Page Informations sur la configuration d'exécution
- Page de l'éditeur XML d'agent (itm_toolkit_agent.xml)

Remarque : Lorsque vous affichez une page de l'éditeur, vous pouvez également basculer vers une autre page en cliquant sur l'onglet de la page. Certaines pages n'affichent des onglets que si elles sont sélectionnées dans la vue Structure. Vous pouvez forcer l'affichage d'un onglet sur une page même lorsqu'elle n'est pas sélectionnée en cliquant sur l'icône d'épingle dans l'angle supérieur droit pour que l'épingle pointe vers la page.

Page Informations sur l'agent

La page **Informations sur l'agent** est la page principale de l'éditeur d'agent.

La page **Informations sur l'agent** contient les informations suivantes :

- informations générales sur l'agent, y compris le nom de service d'agent et le code produit. Vous pouvez cliquer sur **Avancé** pour définir des noms différents en fonction de l'utilisation mais ce paramètre n'est normalement pas nécessaire.
- Informations sur le contenu d'agent
  - Lien vers les **systèmes d'exploitation par défaut**
  - Lien vers l'**agent autodescriptif**
  - Lien vers les **variables d'environnement**
  - Lien vers les **informations sur le programme de surveillance**
  - Lien vers les **informations Cognos**
  - Lien vers les **sources de données**
  - Lien vers la **configuration d'exécution**
  - Lien **Ressources**
  - Lien vers les **tableaux de bord**
- Lien vers le **test de l'agent**
- Lien vers l'**assistant de génération d'agent**
- Lien vers la **validation de la version de l'agent**

Configuration de la durée d'affichage des messages d'erreur transitoires

L'éditeur d'agent affiche parfois des messages d'erreur transitoires. Un message apparaît pendant un court instant (3 secondes par défaut) dans l'en-tête de l'assistant. Vous pouvez configurer la durée d'affichage de ces messages. Pour modifier ce paramètre :

1. Sélectionnez **Fenêtre** > **Préférences** dans la barre de menus d'Agent Builder. La fenêtre **Préférences** s'ouvre.
2. Sélectionnez **Agent Builder**.
3. Définissez le paramètre **Durée (en secondes) pendant laquelle les messages d'erreur transitoires s'affichent**.
4. Cliquez sur **OK**.

Systèmes d'exploitation par défaut

Utilisez la page **Systèmes d'exploitation par défaut** pour modifier les systèmes d'exploitation pour lesquels votre agent sera créé.

Procédure

- Pour ouvrir la page **Systèmes d'exploitation par défaut**, cliquez sur **Systèmes d'exploitation par défaut** dans la section **Contenu d'agent** de la page **Informations sur l'agent** ou sur le noeud **Systèmes d'exploitation par défaut** de la vue Structure.
- Sur la page **Systèmes d'exploitation par défaut**, sélectionnez les systèmes d'exploitation que votre agent doit prendre en charge.

  Lorsque vous générez un module d'installation pour l'agent, Agent Builder ajoute des fichiers au module pour les systèmes d'exploitation sélectionnés. Les sources de données que vous ajoutez à votre agent et qui ne sont pas spécifiques au système d'exploitation Windows sont disponibles sur tous les systèmes d'exploitation sélectionnés. Les systèmes d'exploitation sur lesquels une source de données spécifique est disponible peuvent être modifiés à partir de cette sélection par défaut. Pour modifier les systèmes d'exploitation disponibles pour une source de données spécifique, utilisez le

panneau **Systèmes d'exploitation** de la page **Définition de la source de données**. Si aucun système d'exploitation par défaut n'est sélectionné, des systèmes d'exploitation doivent être sélectionnés pour chaque source de données spécifique sur la page **Définition de la source de données**.

Important : Pour exécuter un test complet de l'agent dans Agent Builder (pour obtenir des instructions, voir «Test complet de l'agent», à la page 1424), vérifiez que :

- Si vous exécutez Agent Builder sous Windows, la version 32 bits du système d'exploitation est installée.
- Si vous exécutez Agent Builder sous Linux, la version 64 bits du système d'exploitation est installée.

Important : Dans certains cas, il se pourrait que vous deviez installer votre agent sur un système 64 bits où seul un agent de système d'exploitation 32 bits est installé. Dans ce cas, vérifiez que la version 64 bits du système d'exploitation n'est pas sélectionnée et que la version 32 bits est sélectionnée.

Agent autodescriptif

Pour l'environnement IBM Tivoli Monitoring, utilisez la page **Agent autodescriptif** pour indiquer si les fichiers de prise en charge de l'agent sont fournis avec l'agent. Pour l'environnement IBM Cloud Application Performance Management, vous devez laisser l'agent autodescriptif activé.

Procédure

- Pour ouvrir la page **Agent autodescriptif**, cliquez sur **Agent autodescriptif** dans la section **Contenu d'agent** de la page **Informations sur l'agent** ou sur le noeud **Agent autodescriptif** dans la vue Structure.

  L'autodescription est activée par défaut pour tous les nouveaux agents créés avec Agent Builder 6.2.3 ou version ultérieure. Si l'agent est destiné à être utilisé dans l'environnement IBM Cloud Application Performance Management, l'autodescription doit être activée.

  Lorsque l'autodescription est activée pour un agent, les packages de prise en charge d'application sont inclus dans l'image de l'agent. Cette inclusion permet à l'agent de rechercher les fichiers de support du serveur Tivoli Enterprise Monitoring Server, du serveur Tivoli Enterprise Portal Server et du navigateur Tivoli Enterprise Portal. Pour plus d'informations sur les agents autodescriptifs, voir *IBM Tivoli Monitoring - Guide d'installation et de configuration* et *IBM Tivoli Monitoring - Guide d'administration*. Dans un environnement IBM Cloud Application Performance Management, l'autodescription permet à l'agent de distribuer les fichiers de support sur le serveur Cloud APM ; le processus de distribution est une étape obligatoire dans l'environnement.

  Remarque : Dans un environnement IBM Tivoli Monitoring, Tivoli Monitoring version 6.2.3 ou ultérieure doit être installé pour que la fonction de l'agent autodescriptif soit active, et l'autodescription doit être activée dans Tivoli Monitoring. Par défaut, l'autodescription est désactivée dans Tivoli Monitoring.

  Remarque : Si vous cochez la case **Activer l'autodescription pour cet agent**, votre agent peut tout de même s'exécuter sur des versions antérieures de Tivoli Monitoring.

Variables d'environnement

Utilisez la page **Variables d'environnement** pour afficher et modifier les variables d'environnement disponibles pour votre agent lors de son exécution.

Avant de commencer

Pour plus d'informations sur l'**éditeur d'agent** et sur la page **Informations sur l'agent**, voir «Utilisation de l'éditeur d'agent pour modifier l'agent», à la page 1207.

Pourquoi et quand exécuter cette tâche

Les variables d'environnement peuvent être des variables que vous définissez pour accéder à l'intérieur d'un script, ou des variables prédéfinies qui déterminent le comportement de l'agent. Pour obtenir la liste des variables prédéfinies, voir le «Liste des variables d'environnement», à la page 1210.

Procédure

1. Pour ouvrir la page **Variables d'environnement**, cliquez sur **Variables d'environnement** dans la section **Contenu d'agent** de la page **Informations sur L'agent**. Sinon, cliquez sur le noeud **Variables d'environnement** dans la vue **Structure**.
2. Sur la page **Variables d'environnement**, cliquez sur **Ajouter** pour ajouter une nouvelle variable. Sinon, pour éditer une variable existante, sélectionnez-la et cliquez sur **Editer**.
3. Dans la fenêtre **Informations sur les variables d'environnement**, définissez les valeurs suivantes :
   - Dans la zone **Nom**, entrez un nom de variable ou sélectionnez un nom prédéfini dans la liste.
   - Dans la zone **Valeur**, entrez une valeur pour la variable si vous souhaitez définir une variable pour l'agent. Si vous ne spécifiez pas de valeur, l'agent propage une valeur pour la variable existante.
   - Dans la zone **Description**, entrez une description de la variable ou conservez la description existante d'une variable prédéfinie.

   a) Cliquez sur **OK**.

   La nouvelle variable apparaît dans le tableau de la page **Informations sur L'agent**.

Liste des variables d'environnement

Les variables d'environnement permettent de contrôler le comportement de l'agent au moment de l'exécution.

Les variables d'environnement peuvent être générées dans l'agent à l'aide de la page **Variables d'environnement**. Sur les systèmes Windows, ces variables sont définies dans le fichier K*XX*ENV de l'agent. Sur les systèmes UNIX et Linux, elles peuvent être définies dans le fichier `$CANDLEHOME/config/`*`XX`*`.ini` de l'agent. *XX* correspond au code produit à deux lettres. L'agent doit être redémarré pour que les nouveaux paramètres soient appliqués.

Remarque : Les variables d'environnement ne sont pas définies correctement sur un système distant exécutant un interpréteur de commandes C. Si vous devez utiliser des variables d'environnement, utilisez un interpréteur de commandes différent.

Tableau 259. Variables d'environnement. Tableau répertoriant les variables d'environnement, leurs valeurs par défaut, les plages de valeurs valides et les descriptions de chaque variable.

Variable d'environnement	Valeur par défaut	Valeurs admises	Description
`CDP_`*`ATTRIBUTE_GROUP`*`_INTERVALLE_ACTUALISATION`	Non applicable	Tout entier non négatif	Fréquence, en secondes, à laquelle un groupe d'attributs particulier indiqué est mis à jour en arrière-plan. Cette variable fonctionne de la même manière que `CDP_DP_REFRESH_INTERVAL`, à ceci près qu'elle ne vise que le groupe d'attributs indiqué. Le nom de groupe d'attributs dans le nom de variable doit être en majuscules, même si le nom de groupe d'attributs réel ne l'est pas.

Tableau 259. Variables d'environnement. Tableau répertoriant les variables d'environnement, leurs valeurs par défaut, les plages de valeurs valides et les descriptions de chaque variable. *(suite)*

Variable d'environnement	Valeur par défaut	Valeurs admises	Description
CDP_DP_CACHE_TTL	55	Tout entier supérieur ou égal à 1.	Nombre de secondes pendant lequel les données collectées pour un groupe d'attributs sont mises en cache. Pendant cette durée, lorsque plusieurs demandes sont effectuées pour les mêmes données, elles reçoivent une copie en cache de ces données. Cette valeur s'applique à tous les groupes d'attribut de l'agent.
CDP_*GROUPE_ATTRIBUTS*_CACHE_TTL	Valeur de CDP_DP_CACHE_TTL	Tout entier supérieur ou égal à 1.	Nombre de secondes pendant lesquelles les données collectées pour le groupe d'attributs spécifié sont mises en cache. Pendant cette durée, lorsque plusieurs demandes sont effectuées pour les mêmes données, elles reçoivent une copie en cache de ces données. Cette valeur se substitue à CDP_DP_CACHE_TTL pour le groupe spécifié. Le nom de groupe d'attributs dans le nom de variable doit être en majuscules, même si le nom de groupe d'attributs réel ne l'est pas.
CDP_DP_IMPATIENT_COLLECTOR_TIMEOUT	5 si des sous-noeuds sont définis ; dans le cas contraire, elle n'est pas définie.	Tout entier positif	Délai d'attente (en secondes) d'une collecte de données avant expiration et renvoi des données mises en cache, même si les données mises en cache sont périmées. (Les données mises en cache sont périmées si elles sont plus anciennes queCDP_DP_CACHE_TTL secondes). Si cette variable n'est pas définie, l'agent attend la fin de la collecte de données. Il arrive parfois que Tivoli Enterprise Portal ignore le délai d'attente. Si aucun pool d'unités d'exécution n'est configuré, cette variable est ignorée et la collecte de données est exécutée de façon synchrone.

Tableau 259. Variables d'environnement. Tableau répertoriant les variables d'environnement, leurs valeurs par défaut, les plages de valeurs valides et les descriptions de chaque variable. *(suite)*

Variable d'environnement	Valeur par défaut	Valeurs admises	Description
CDP_DP_REFRESH_INTERVAL	60 si des sous-noeuds sont définis ; dans le cas contraire, elle n'est pas définie.	Tout entier non négatif	Fréquence, en secondes, à laquelle les groupes d'attributs sont mis à jour en arrière-plan. Si cette variable n'est pas définie ou qu'elle a pour valeur 0, les mises à jour en arrière-plan sont désactivées. Si un pool d'unités d'exécution est configuré (voir la variable CDP_DP_THREAD_POOL_SIZE), les groupes d'attributs peuvent être régénérés en parallèle. S'il n'y a aucun pool d'unités d'exécution, les mises à jour se font en série, ce qui peut prendre un temps considérable. Cela équivaut logiquement à une taille de pool d'unités d'exécution de 1.
CDP_DP_THREAD_POOL_SIZE	15 si des sous-noeuds sont définis ; dans le cas contraire, elle n'est pas définie.	Tout entier non négatif	Nombre d'unités d'exécution créées pour exécuter des collectes de données en arrière-plan à une fréquence définie par CDP_DP_REFRESH_INTERVAL. Si cette variable n'est pas définie ou qu'elle a pour valeur 0, cela signifie qu'il n'y a aucun pool d'unités d'exécution. Si CDP_DP_THREAD_POOL_SIZE est définie sur une valeur supérieure à 1 et que CDP_DP_REFRESH_INTERVAL est définie sur 0, la valeur de CDP_DP_THREAD_POOL_SIZE est ignorée et la collecte de données est lancée à la demande. Le groupe d'attributs Statut du pool d'unités d'exécution présente le mode de fonctionnement. Il vous permet d'ajuster la taille du pool d'unités d'exécution et la fréquence de régénération pour améliorer les résultats. Par défaut, la requête de ce groupe d'attributs ne s'affiche pas dans l'arborescence de navigation de l'agent. Vous risquez de ne pas vous souvenir d'inclure la requête dans un espace de travail personnalisé pour l'agent. Cependant, vous pouvez aisément la visualiser en affectant la requête Statut du pool d'unités d'exécution à une vue d'espace de travail au niveau de l'agent.

Tableau 259. Variables d'environnement. Tableau répertoriant les variables d'environnement, leurs valeurs par défaut, les plages de valeurs valides et les descriptions de chaque variable. *(suite)*

Variable d'environnement	Valeur par défaut	Valeurs admises	Description
CDP_JDBC_MAX_ROWS	1000	Tout entier positif	Nombre maximal de lignes de données que le fournisseur de données JDBC renvoie. Un ensemble de résultats contenant un nombre supérieur à ce nombre de lignes n'est traité que jusqu'à cette valeur maximale. Des requêtes peuvent être développées pour empêcher qu'une quantité excessive de données soit renvoyée à IBM Tivoli Monitoring.
CDP_NT_EVENT_LOG_GET_ALL_ENTRIES_FIRST_TIME	NO	YES, NO	Si cette variable est définie sur YES, l'agent envoie un événement pour chaque enregistrement dans le journal des événements Windows. Si elle est définie sur NO, seuls les nouveaux événements du journal Windows sont envoyés.
CDP_NT_EVENT_LOG_CACHE_TIMEOUT	3600	Tout entier supérieur ou égal à 300.	Nombre de secondes pendant lequel les événements du journal des événements Windows sont mis en cache par l'agent. Tous les événements mis en cache sont renvoyés lorsqu'une requête est effectuée sur le groupe d'attributs Journal des événements. **Remarque :** Cette variable n'est plus utilisée. Utilisez la variable CDP_PURE_EVENT_CACHE_SIZE.
CDP_PURE_EVENT_CACHE_SIZE	100	Tout entier positif supérieur ou égal à 1.	Nombre maximal d'événements à mettre en cache lorsqu'une source de données de fichier journal est configurée pour traiter de nouveaux enregistrements, pour le groupe d'attributs Journal des événements Windows. Et aussi pour les moniteurs et les notifications JMX. Chaque nouvel enregistrement du journal provoque l'envoi d'un événement. Cette variable d'environnement définit le nombre d'événements placés dans la mémoire cache par l'agent. Les valeurs mises en cache sont renvoyées lorsqu'une requête est effectuée sur le groupe d'attributs.
CDP_DP_ACTION_TIMEOUT	20 secondes	Tout entier positif supérieur ou égal à 1.	Délai d'attente en secondes avant que l'agent n'ait effectué le traitement de la commande Action.

Tableau 259. Variables d'environnement. Tableau répertoriant les variables d'environnement, leurs valeurs par défaut, les plages de valeurs valides et les descriptions de chaque variable. *(suite)*

Variable d'environnement	Valeur par défaut	Valeurs admises	Description
CDP_DP_SCRIPT_TIMEOUT	30 secondes	Tout entier positif supérieur ou égal à 10.	Délai d'attente en secondes, avant que le programme lancé par un groupe d'attributs basé sur des scripts soit terminé.
CDP_DP_PING_TIMEOUT	30 secondes	Tout entier positif supérieur ou égal à 10.	Délai d'attente en secondes, avant que le programme lancé par un code de retour de commande soit terminé. **Remarque :** Cette variable ne concerne pas le fournisseur de données de Ping ICMP.
CDP_SNMP_MAX_RETRIES	2	Tout entier positif	Nombre de nouvelles tentatives d'envoi de la demande SNMP. Le nombre total de demandes envoyées à l'agent SNMP correspond à cette valeur plus un, si aucune réponse n'est reçue.
CDP_SNMP_RESPONSE_TIMEOUT	2 secondes	Tout entier positif	Délai d'expiration, en secondes, de chaque demande SNMP. Chaque ligne d'un groupe d'attributs correspond à une demande distincte. Cette valeur de délai d'expiration correspond au délai d'attente, en secondes, d'une réponse avant une nouvelle tentative. Le délai d'expiration total pour une ligne de données unique est (CDP_SNMP_MAX_RETRIES + 1) * CDP_SNMP_RESPONSE_TIMEOUT. Le délai d'expiration total par défaut est (2+1) * 2 = 6 secondes.
CDP_DP_HOSTNAME	Nom de la première interface réseau installée	Une adresse IP ou un nom d'hôte	Définit le nom d'hôte préféré (interface réseau) sur un système comportant plusieurs interfaces. Utilisez cette variable d'environnement si l'agent connecte ses ports d'écoute à une adresse d'interface réseau autre que celle par défaut. Utilisé par le fournisseur de données SNMP. Pour les sources de données personnalisées et de socket, cette variable s'applique si la variable CDP_DP_ALLOW_REMOTE est également définie.

Tableau 259. Variables d'environnement. Tableau répertoriant les variables d'environnement, leurs valeurs par défaut, les plages de valeurs valides et les descriptions de chaque variable. *(suite)*

Variable d'environnement	Valeur par défaut	Valeurs admises	Description
CDP_SNMP_ALLOW_ DECREASING_OIDS	NO	YES, NO	Si cette variable a pour valeur YES, les fournisseurs de données SNMP ne vérifient pas si les ID objet renvoyés sont en cours d'augmentation. Affectez la valeur YES avec prudence car il se peut que l'agent surveillé ait des problèmes que cette vérification peut généralement intercepter.
KUMP_DP_COPY_MODE_SAMPLE_I NTERVAL	60	Délai d'attente (secondes)	Pour un fournisseur de données de fichier journal, indique le délai d'attente avant la relecture du contenu d'un fichier lorsque l'agent est défini sur **Traiter tous les enregistrements lorsque le fichier est échantillonné**. La durée est exprimée en secondes.
KUMP_MAXPROCESS	100%	5-100%	Pour un fournisseur de données de fichier journal, spécifie l'utilisation maximale du processeur pour traiter le fichier de données. Les valeurs sont comprises entre 5 et 100%. La valeur par défaut est de 100%.
KUMP_DP_SAMPLE_FACTOR	5	Tout entier non négatif	Pour un fournisseur de données de fichier journal, définit le facteur d'échantillonnage lorsque l'option **Traiter tous les enregistrements lorsque le fichier est échantillonné** est sélectionnée. Ce temps d'attente garantit que les modèles qui couvrent plusieurs enregistrements sont totalement écrits avant consignation des balayages du modèle.
KUMP_DP_EVENT	5	Tout entier non négatif	Pour un fournisseur de données de fichier journal, définit la fréquence d'échantillonnage des données d'événement, en secondes.
KUMP_DP_FILE_EXIST_WAIT	YES	YES, NO	Pour un fournisseur de données de fichier journal, indique que l'unité d'exécution de surveillance de fichier continue de s'exécuter si elle détecte que le fichier surveillé est absent ou vide. L'unité d'exécution attend que le fichier existe, re-vérifie toutes les quelques secondes, puis démarre ou redémarre la surveillance une fois que le fichier est disponible.

Tableau 259. Variables d'environnement. Tableau répertoriant les variables d'environnement, leurs valeurs par défaut, les plages de valeurs valides et les descriptions de chaque variable. *(suite)*

Variable d'environnement	Valeur par défaut	Valeurs admises	Description
KUMP_DP_FILE_SWITCH_ CHECK_INTERVAL	600	Tout entier non négatif	Indique la fréquence, en secondes, à laquelle le fournisseur de données de fichier journal recherche un fichier de surveillance différent sur lequel basculer lors de l'utilisation de la prise en charge de nom de fichier dynamique.
KUMP_DP_FILE_ROW_ PAUSE_INCREMENT	Aucun	Tout entier non négatif	Pour un fournisseur de données de fichier journal, indique le nombre d'enregistrements de fichier lus avant que l'unité d'exécution de surveillance de fichier s'interrompe. La pause permet le traitement des mises à jour précédentes. Utilisez cette variable d'environnement uniquement si le fichier surveillé reçoit des rafales volumineuses de nouveaux enregistrements et que certaines mises à jour d'enregistrement risquent d'être perdues.
CDP_COLLECTION_TIMEOUT	60 secondes	Tout entier positif	Délai en secondes durant lequel l'agent attend une réponse d'un collecteur de données qui a été lancé dans un autre processus. Les collecteurs de données JMX, JDBC, HTTP et SOAP en sont des exemples.
CDP_SSH_TEMP_DIRECTORY	. (point)	Toute chaîne de chemin valide sur le système distant	Pour un fournisseur de données de script compatible SSH, spécifie un emplacement sur le système distant. Les fichiers script qui sont fournis avec l'agent doivent être téléchargés à cet emplacement. Le terme d'emplacement relatif désigne un emplacement par rapport au répertoire de base de l'utilisateur. La valeur par défaut de . (point) indique le répertoire de base de l'utilisateur.
CDP_SSH_DEL_COMMAND	rm -Rf	Toute chaîne de commande de suppression valide sur le système distant	Pour un fournisseur de données de script compatible SSH, spécifie la commande appelée pour supprimer les fichiers scripts téléchargés, fournis avec l'agent.

Tableau 259. Variables d'environnement. Tableau répertoriant les variables d'environnement, leurs valeurs par défaut, les plages de valeurs valides et les descriptions de chaque variable. *(suite)*

Variable d'environnement	Valeur par défaut	Valeurs admises	Description
CDP_SNMP_SEND_DELAY_ FACTOR	0 millisecondes	Tout entier positif	L'envoi SNMP initial est retardé de 0 au nombre de millisecondes indiqué. Cette variable n'est activée que si le pool d'unités d'exécution est activé aussi. Le délai ne s'applique pas à tous les envois, mais seulement au premier envoi effectué par un groupe d'attributs. Cette variable est utile lorsque le périphérique surveillé a des difficultés à répondre lorsqu'il reçoit plusieurs demandes à la fois.
CDP_ICMP_PING_REFRESH_ INTERVAL	60 secondes	Tout entier supérieur ou égal à 1.	Intervalle auquel sont "pingués" les systèmes répertoriés dans un fichier listant les unités. Si les pings consomment trop de temps, il y a toujours un délai d'au moins CDP_PING_MIN_INTERVAL_DELAY secondes avant que la commande ne soit réémise. Les données ne sont pas actualisées plus fréquemment que ne l'indique ce paramètre. Elles peuvent l'être moins fréquemment, selon le nombre d'entrées contenues dans le fichier liste de périphériques et la durée nécessaire à la réception des réponses.
CDP_ICMP_PING_MIN_ INTERVAL_DELAY	30 secondes	Tout entier supérieur ou égal à 1 et inférieur à la fréquence de régénération des pings CDP	Après émission d'une commande PING sur les périphériques d'un fichier liste, le prochain intervalle de régénération des pings ne doit pas débuter avant que ce délai, exprimé en secondes, ne soit écoulé.
CDP_ICMP_PING_BURST	10	Tout entier supérieur ou égal à 0.	Nombre de commandes Ping qui seront envoyées avant l'interruption de l'agent spécifiée par la variable CDP_ICMP_PING_BURST_DELAY. La valeur zéro désactive cette fonction.
CDP_ICMP_PING_BURST_DELAY	10	Tout entier supérieur ou égal à 0.	Délai d'attente en millisecondes après envoi du nombre de commandes Ping défini par la variable CDP_ICMP_PING_BURST. La valeur zéro désactive cette fonction.

Tableau 259. Variables d'environnement. Tableau répertoriant les variables d'environnement, leurs valeurs par défaut, les plages de valeurs valides et les descriptions de chaque variable. *(suite)*

Variable d'environnement	Valeur par défaut	Valeurs admises	Description
CDP_ICMP_PING_TIMEOUT	2000 millisecondes	Tout entier supérieur ou égal à 1.	Délai d'attente, en millisecondes, d'une réponse à une commande Ping. Ce paramètre s'applique à chaque tentative de commande PING effectuée. Trois tentatives de commande PING sont effectuées pour chaque hôte. Si aucune réponse n'est reçue suite aux 3 tentatives, la durée totale d'attente d'une réponse est CDP_ICMP_PING_TIMEOUT multiplié par 3. Par défaut, cette valeur est de 6000 millisecondes. Si vous modifiez la valeur de CDP_ICMP_PING_TIMEOUT, l'énumération TIMEOUT par défaut de l'attribut Temps de réponse actuel ne s'applique plus. Vous devez définir l'énumération TIMEOUT sur la nouvelle valeur de CDP_ICMP_PING_TIMEOUT multipliée par 3.
CDP_JDBC_CONNECTIONLESS	false	true, false	Si la valeur est true, les connexions JDBC sont fermées après chaque tentative de collecte de données, c'est-à-dire que tous les groupes d'attributs tentent de créer leur propre connexion chaque fois que des données sont collectées. Les connexions ne sont pas réutilisées si cette variable est activée. Si la valeur est false, une connexion est établie avec la base de données et cette connexion est partagée par les groupes d'attributs.
CDP_SSH_EXCLUDED_ ENVIRONMENT_VARIABLES	Aucun	Liste séparée par des virgules de noms de variables d'environnement	Pour un fournisseur de données de script compatible SSH, spécifie l'ensemble de variables d'environnement local qui ne doivent pas être définies dans l'environnement du système distant.

Tableau 259. Variables d'environnement. Tableau répertoriant les variables d'environnement, leurs valeurs par défaut, les plages de valeurs valides et les descriptions de chaque variable. *(suite)*

Variable d'environnement	Valeur par défaut	Valeurs admises	Description
CDP_DP_EVENT_LOG_MAX_BACKLOG_TIME	0 secondes	0, 1 ou tout entier supérieur à 1	Si cette valeur est définie sur 0 et que la variable CDP_DP_EVENT_LOG_MAX_BACKLOG_EVENTS n'a pas été définie sur 1 ou sur tout entier supérieur à 1, le programme ne traite pas les événements générés pendant que l'agent est arrêté. 0 est la valeur par défaut. Si cette valeur est définie sur 1 et que la variable CDP_DP_EVENT_LOG_MAX_BACKLOG_EVENTS n'a pas été définie sur un entier supérieur à 1, le programme traite tous les événements générés pendant que l'agent est arrêté. Si cette valeur est supérieure à 1 et que la variable CDP_DP_EVENT_LOG_MAX_BACKLOG_EVENTS n'a pas été définie sur un entier supérieur à 1, le programme traite les événements générés pendant ce délai en secondes par rapport à l'heure actuelle de l'ordinateur. Par exemple, si la valeur est définie sur 300, l'agent traite tous les événements générés à moins de 300 secondes de l'heure actuelle de l'ordinateur. Lorsqu'une valeur supérieure à 1 est entrée pour les variables CDP_DP_EVENT_LOG_MAX_BACKLOG_TIME et CDP_DP_EVENT_LOG_MAX_BACKLOG_EVENTS, l'intervalle de temps des événements ou le nombre d'événements est traité. La variable choisie dépend de celle qui correspond en premier.
CDP_DP_EVENT_LOG_*journal_événements_Windows*_MAX_BACKLOG_TIME	0 seconde (ne traitez pas d'événements omis pendant que l'agent est arrêté)	0, 1 ou tout entier supérieur à 1	Si la valeur est

Tableau 259. Variables d'environnement. Tableau répertoriant les variables d'environnement, leurs valeurs par défaut, les plages de valeurs valides et les descriptions de chaque variable. *(suite)*

Variable d'environnement	Valeur par défaut	Valeurs admises	Description
CDP_DP_EVENT_LOG_ MAX_BACKLOG_EVENTS	0 événements	0, 1 ou tout entier supérieur à 1	Si elle est définie sur 0 et que la variable CDP_DP_EVENT_LOG_MAX_BACKLOG _TIME n'est pas définie sur 1 ou un entier supérieur, le programme ne traite pas les événements générés lorsque l'agent est arrêté. 0 est la valeur par défaut. Si elle est définie sur 1 et que la variable CDP_DP_EVENT_LOG_MAX_BACKLOG _TIME n'est pas définie sur un entier supérieur à 1, le programme traite tous les événements générés lorsque l'agent est arrêté. Si elle est supérieure à 1 et que la variable CDP_DP_EVENT_LOG_MAX_BACKLOG _TIME n'est pas supérieure à 1, le programme traite au plus les événements générés lorsque l'agent est arrêté. Par exemple, si la valeur est définie sur 200, au démarrage de l'agent, le programme traite les 200 événements générés directement avant le démarrage. Lorsqu'une valeur supérieure à 1 est entrée pour les variables CDP_DP_EVENT_LOG_MAX_BACKLOG _EVENTS et CDP_DP_EVENT_LOG_MAX_BACKLOG _BACKLOG_TIME, l'intervalle de temps des événements ou le nombre d'événements est traité. La variable choisie dépend de celle qui correspond en premier.
CDP_DP_EVENT_LOG_ *journal_événements_Windows* _MAX_BACKLOG_ EVENTS	0 événement (ne traitez pas d'événement omis pendant que l'agent est arrêté)	0 ou tout entier supérieur ou égal à 1	Si la valeur est
CDP_HTTP_READ_TIMEOUT	10	Tout entier positif	Temps en secondes d'attente d'une réponse à une requête HTTP.
CDP_JAT_THREAD_POOL_SIZE	15	Tout entier positif	Nombre d'unités d'exécution utilisées par les fournisseurs Java pour la gestion des demandes de collecte de données. Les fournisseurs de données JMX, JDBC, HTTP et SOAP sont ceux qui peuvent bénéficier de ce pool d'unités d'exécution.

Tableau 259. Variables d'environnement. Tableau répertoriant les variables d'environnement, leurs valeurs par défaut, les plages de valeurs valides et les descriptions de chaque variable. *(suite)*

Variable d'environnement	Valeur par défaut	Valeurs admises	Description
CDP_HTML_OBJECTS_THREAD_POOL_SIZE	10	Tout entier positif	Nombre d'unités d'exécution utilisées pour le téléchargement d'objets de page trouvés dans les URL surveillées par le fournisseur de données HTTP.
CDP_HTTP_SOAP_MAX_ROWS	500	Tout entier positif	Nombre maximal de lignes renvoyées par le fournisseur de données HTTP SOAP.
CDP_DP_ALLOW_REMOTE	NO	YES, NO	Si cette variable est paramétrée sur Yes, l'agent autorise les connexions socket distantes. Si elle est paramétrée sur Non, l'agent n'autorise que les connexions socket à partir du système hôte local. Il s'agit de la valeur par défaut.
CDP_DP_INITIAL_COLLECTION_DELAY	varie	Tout entier positif	Nombre de secondes, après le démarrage de l'agent, avant que le pool d'unités d'exécution ne commence ses collectes de données planifiées.

Informations sur le programme de surveillance

Utilisez la page **Informations sur le programme de surveillance** pour indiquer des informations de configuration pour le programme de surveillance de l'agent.

Pourquoi et quand exécuter cette tâche

Pour ouvrir la page **Informations sur le programme de surveillance**, cliquez sur **Informations sur le programme de surveillance** dans la section **Contenu d'agent** de la page **Informations sur l'agent**. Vous pouvez également sélectionner le noeud **Informations sur le programme de surveillance** dans la vue Structure.

Vous pouvez spécifier les informations de configuration suivantes pour le programme de surveillance de l'agent :

- **Surveiller cet agent par défaut**

  Cochez cette case pour que l'agent soit placé sous la surveillance d'Agent Management Services lors de son installation. Un programme de surveillance vérifie toute défaillance ou tout arrêt anormal de l'agent et le redémarre.

- **Fréquence de vérification (secondes)**

  Indique la fréquence à laquelle le programme de surveillance vérifie toute défaillance ou tout arrêt anormal du processus d'agent. Valeur par défaut : toutes les 180 secondes.

- **Nombre maximal de redémarrages**

  Indique le nombre de redémarrages de l'agent par le programme de surveillance en cas de défaillance ou d'arrêt anormal, sur une période de 24 heures, avant de prévenir l'administrateur de l'incident. La période commence à minuit chaque jour. Par conséquent, la première période à partir du moment où l'agent est démarré peut être "courte".

  Un redémarrage a lieu si l'agent tombe en panne pour quelque raison que ce soit. Le programme de surveillance arrête et redémarre aussi l'agent si celui-ci ne répond pas, est défectueux, ou si le seuil de mémoire est franchi. La valeur par défaut correspond à quatre redémarrages dans une période de 24 heures, la période étant mesurée de minuit à 23:59. A minuit, le nombre de redémarrages quotidiens de l'agent repasse automatiquement à 0.

- **Informations sur le seuil de mémoire**

  Taille (en mégaoctet) que le processus d'agent peut atteindre avant que le programme de surveillance ne le considère comme défaillant. Il y a une valeur distincte pour Windows, Linux, et UNIX. Si le processus d'agent augmente au-delà du seuil, le programme de surveillance arrête le processus puis le redémarre. Il n'y a pas de valeurs par défaut pour ces propriétés. Si aucune valeur n'est spécifiée, le programme de surveillance ne surveille pas la taille du processus. Cette mesure utilise la taille de la partie active d'un programme sous Windows et la mémoire utilisateur sous UNIX et Linux.

Si le programme de surveillance arrête l'agent et que le nombre maximal de redémarrages a été atteint, le programme de surveillance envoie une alerte indiquant que l'agent a dépassé son nombre de redémarrages, puis cesse d'effectuer des redémarrages automatiques. Le programme de surveillance signale néanmoins si l'agent est actif ou inactif, supposant qu'il est démarré d'une autre manière, par exemple via Tivoli Enterprise Portal.

Vous devez redémarrer manuellement l'agent à l'aide de la commande Action AMS Start Agent de sorte que le nombre de redémarrages ne se réinitialise pas.

Le nombre est réinitialisé de l'une des manières suivantes (le programme de surveillance continue de fonctionner et de signaler l'état mais n'effectue pas de redémarrages automatiques) :

- L'horloge sonne à minuit.
- L'utilisateur emploie la commande Action AMS Start Agent qui comporte un paramètre d'entrée appelé **resetRestartCount**. Si vous entrez une valeur de 1 (signifiant "true" ou "oui"), le nombre de redémarrages quotidiens est réinitialisé à 0.

Pour plus d'informations, voir les sections suivantes sections suivantes dans *IBM Tivoli Monitoring - Guide d'administration* :

- Pour les agents Tivoli System Monitor

  Configuration des services de gestion des agents sur les agents Tivoli System Monitor
- Pour les agents Tivoli Enterprise

  Installation et configuration de Tivoli Agent Management Services

Informations Cognos

Utilisez la page **Informations Cognos** pour indiquer les informations utilisées lorsqu'un modèle de données Cognos est généré pour votre agent. Ces informations ne sont utilisées que pour l'environnement IBM Tivoli Monitoring.

Procédure

1. Pour ouvrir la page **Informations Cognos**, cliquez sur **Informations Cognos** dans la section **Contenu d'agent** de la page **Informations sur l'agent** ou sur le noeud **Informations Cognos** dans la vue Structure.
2. Dans la zone **Source de données**, entrez le nom de la source de données qui relie Tivoli Common Reporting à IBM Tivoli Data Warehouse.

   La valeur par défaut est `TDW`.
3. Dans la zone **Schéma**, entrez le nom du schéma de base de données utilisé pour Tivoli Data Warehouse, qui permet de qualifier dans leur intégralité les noms de table dans les rapports Cognos.

   La valeur par défaut est `ITMUSER`. Vous pouvez modifier cette valeur dans Framework Manager lorsque le modèle généré Cognos est chargé dans Framework Manager.

   La case à cocher **Ajouter ce groupe d'attributs à une catégorie de rapports** dans la page **Définition de la source de données** détermine l'emplacement du groupe d'attributs dans le modèle Cognos. Si la case n'est pas cochée, le groupe d'attributs est placé dans le dossier attributs étendus dans le modèle Cognos. Si cette option est cochée, le groupe d'attributs est placé dans le sous-dossier sélectionné (disponibilité ou performance) du dossier Métriques de la clé. Pour plus d'informations sur les zones de source de données, voir Tableau 260, à la page 1227.

Que faire ensuite

Vous pouvez utiliser le modèle de données Cognos afin de créer des rapports Tivoli Common Reporting pour votre agent (voir «Génération d'un modèle de données Cognos», à la page 1519).

Lien vers l'assistant de génération d'agent

Lorsque vous avez fini de créer ou de modifier le nouvel agent, utilisez l'Assistant Générer un agent pour préparer l'installation.

Procédure

- Lorsque vous avez fini de créer ou de modifier le nouvel agent, cliquez sur le lien **Assistant Générer un agent** dans la page **Informations sur l'agent** de l'**éditeur d'agent**.

  Cet assistant permet de :

  – Générer les fichiers d'agent avec une installation Tivoli Monitoring locale. Pour plus d'informations, voir «Installation en local d'un agent», à la page 1430.

  – Créer un package afin que l'agent puisse être installé sur d'autres systèmes. Pour plus d'informations, voir «Création du package d'agent», à la page 1432.

Page Définition de la source de données

La page **Définition de la source de données** permet de manipuler les sources de données.

Pourquoi et quand exécuter cette tâche

La page **Définition de la source de données** répertorie les sources de données configurées pour l'agent. Lorsque vous sélectionnez une source de données ou un attribut dans l'arborescence, la page est mise à jour pour afficher les propriétés de l'objet sélectionné. Utilisez les zones pour modifier les propriétés de la source de données ou de l'attribut sélectionné.

Remarque : Pour obtenir des instructions détaillées sur la création de sources de données associées à différents fournisseurs de données, voir «Définition et test de sources de données», à la page 1255.

Procédure

- Pour ouvrir la page **Définition de la source de données**, cliquez sur **Sources de données** dans la section **Contenu d'agent** de la page **Informations sur l'agent** ou sur le noeud **Sources de données** dans la vue **Structure**.
- Vous pouvez ajouter d'autres sources de données en cliquant sur **Ajouter à la sélection** ou en cliquant avec le bouton droit de la souris dans l'arborescence de navigation et en sélectionnant l'une des options.
- Vous pouvez supprimer des sources de données et des attributs en cliquant dessus avec le bouton droit de la souris et en sélectionnant **Supprimer**.
- Vous pouvez ajouter, modifier et supprimer des attributs. Pour obtenir des instructions, voir «Modification des propriétés de sources de données et d'attributs», à la page 1227

Copie de sources de données à l'aide de la page Définition de la source de données
Utilisez la page **Définition de la source de données** pour copier des sources de données.

Avant de commencer

Accédez à la page **Définition de la source de données**. Pour plus d'informations, voir «Page Définition de la source de données», à la page 1223.

Pourquoi et quand exécuter cette tâche

Les sources de données correspondant à des groupes d'attributs peuvent être copiées dans le presse-papiers et reportées dans cet agent ou un autre agent. Les sources de données qui ne correspondent pas à des groupes d'attributs sont les sources de données Disponibilité et Journal des événements Windows.

Procédure

1. Sélectionnez les groupes d'attributs que vous souhaitez copier.
2. Coupez ou copiez le groupe d'attributs en effectuant l'une des actions suivantes :
   - Cliquez sur **Editer** > **Couper** > **Editer** > **Copier** dans la barre de menus.
   - Cliquez avec le bouton droit de la souris sur l'un des éléments sélectionnés, puis cliquez sur **Couper** ou **Copier** dans le menu.
   - Utilisez l'un des raccourcis clavier du système d'exploitation ou d'Eclipse qui correspond à l'action Couper ou Copier. Par exemple, sur les systèmes Windows, la combinaison de touches **Ctrl-C** correspond à la commande Copier.

   Pour supprimer des sources de données de leur emplacement existant et les placer dans le presse-papiers, utilisez **Couper**. Pour laisser des sources de données en place et les copier au presse-papiers, utilisez **Copier**.
3. Sélectionnez le parent d'un groupe d'attributs (l'agent, un sous-noeud ou un groupe de navigation) ou sélectionnez un groupe d'attributs existant.
4. Collez la sélection en effectuant l'une des actions suivantes :
   - Sélectionnez **Editer** > **Coller** dans la barre de menus.
   - Cliquez avec le bouton droit de la souris sur le noeud dans lequel vous souhaitez coller la sélection dans l'arborescence, puis cliquez sur **Coller** dans le menu.
   - Utilisez l'un des raccourcis clavier du système d'exploitation ou d'Eclipse qui correspond à l'action Coller. Par exemple, sur les systèmes Windows, la combinaison de touches **Ctrl-V** correspond à la commande Coller.

Résultats

Les groupes d'attributs du presse-papiers sont placés dans le parent sélectionné. Si un groupe d'attributs est sélectionné, les groupes d'attributs sont placés dans le parent de ce groupe.

En cas de conflit de nom avec un autre groupe d'attributs lors du Copier-Coller, le nom du groupe d'attributs collé est légèrement modifié pour éviter le conflit.

Page Informations sur la configuration d'exécution

La page **Informations sur la configuration d'exécution** contient les variables configurables de l'agent. Vous pouvez définir les valeurs des variables lorsque vous installez l'agent sur un hôte surveillé.

Ces valeurs sont transmises aux codes retour de commande et aux scripts via l'environnement. Pour ouvrir la page **Informations sur la configuration d'exécution**, cliquez sur **Configuration de l'exécution** dans la section **Contenu d'agent** de la page **Informations sur l'agent** ou du noeud **Configuration d'exécution** dans la vue Structure. Agent Builder construit automatiquement le nom de la variable d'environnement à partir du code produit et du libellé.

Vous pouvez ajouter et modifier les propriétés de configuration et fournir des valeurs par défaut à l'aide de la page **Informations sur la configuration d'exécution**.

Page Editeur XML d'agent

La page **Editeur XML d'agent** affiche les données XML de la définition d'agent.

Le code XML de définition d'agent inclut les informations qui s'affichent dans les autres zones d'Agent Builder. Si vous modifiez le code XML, les informations qui s'affichent dans Agent Builder répercutent le changement.

Avertissement : N'apportez aucun changement au code XML. Un éventuel changement peut provoquer des erreurs qui pourraient vous empêcher de générer l'agent ou affecter de manière négative le fonctionnement de l'agent.

Enregistrement de vos modifications

Les modifications que vous apportez à l'éditeur ne sont pas stockées tant que vous ne les enregistrez pas.

Procédure

- Effectuez un enregistrement à l'aide d'une des opérations suivantes :
  - Sélectionnez **Fichier** > **Sauvegarder** en sélectionnant l'icône d'enregistrement (disquette).
  - Appuyez sur **Ctrl+S**

  Lors de l'enregistrement, une validation est effectuée pour vérifier que les informations sont bien complètes. Si des problèmes se produisent, des informations sur l'erreur s'affichent dans la vue **Incidents** d'Eclipse. Si cette vue n'est pas visible, sélectionnez **Fenêtre** > **Afficher la vue** > **Incidents**. Si vous essayez de générer un agent qui comporte des erreurs, un message d'erreur s'affiche.

  Remarque : Vous devez corriger toutes les erreurs et sauvegarder vos modifications pour pouvoir générer et installer l'agent.

Validation d'une version de l'agent

Lorsque vous êtes certain que vous avez terminé de développer cette version de l'agent et que vous êtes prêt à le livrer, validez votre agent.

Pourquoi et quand exécuter cette tâche

Les systèmes IBM Tivoli Monitoring exigent que les nouvelles versions d'un agent incluent toutes les informations contenues dans les précédentes versions de cet agent utilisées dans l'environnement de surveillance. Le fait d'inclure toutes les informations des précédentes versions est nécessaire pour que les espaces de travail, les situations et les requêtes continuent de fonctionner si le nouvel agent est installé sur certains hôtes surveillés, alors que l'ancien agent reste sur les autres.

Après avoir terminé la mise au point et le test d'un agent, vous devez le valider en tant que version finale pour un certain numéro de version. Agent Builder garantit qu'aucune information n'est supprimée une fois l'agent validé. Les versions ultérieures de l'agent ont un nouveau numéro de version.

La limite est de 1024 versions.

A faire : Si vous apportez des modifications à un agent qui doit être testé et exécuté dans un environnement IBM Cloud Application Performance Management, vous devez modifier la version de l'agent.

Procédure

1. Ouvrez la fenêtre de l'**éditeur d'agent**, puis la page **Informations sur l'agent**.
2. Dans la zone **Valider la version d'agent**, cliquez sur l'option de **validation de ce niveau**.
3. Sauvegardez l'agent validé ou enregistrez-le dans votre système de contrôle des versions.

Que faire ensuite

Lorsque vous validez un agent, toutes les modifications supplémentaires apportées à l'agent font partie d'une nouvelle version. Vous devez entrer le nouveau numéro de version pour que les modifications supplémentaires puissent être sauvegardées. Les modifications apportées à la nouvelle version ne doivent pas rompre la compatibilité avec les précédentes versions de l'agent.

Après avoir validé l'agent, vous ne pouvez pas effectuer ces actions sur des objets ayant existé avant la validation de l'agent :

- Suppression d'attributs d'un groupe d'attributs.

- Suppression de groupes d'attributs.
- Réorganisation des attributs existants d'un groupe d'attributs.
- Réorganisation des groupes d'attributs existants (à l'aide d'éléments du navigateur).
- Déplacement des groupes d'attributs ou des groupes de navigation vers ou hors des sous-noeuds.
- Changement de nom des groupes d'attributs.
- Changement de nom des attributs.
- Modification des types de données des attributs existants.
- Modification d'un nom ou type de sous-noeud s'il contient un groupe d'attributs ayant existé avant la validation de l'agent.
- Modification d'un identificateur de société ou d'un identificateur d'agent pour l'agent.
- Modification du code produit de l'agent. Pour plus d'informations, voir «Modification du code produit», à la page 1226.

Après avoir validé l'agent, vous pouvez effectuer les opérations suivantes :

- Ajout de nouveaux attributs dans des groupes d'attributs existants.
- Ajout de nouveaux groupes d'attributs.
- Réorganisation des nouveaux attributs.
- Organisation des nouveaux groupes d'attributs à l'aide d'éléments du navigateur.
- Création de types de sous-noeud.
- Ajout de nouvelles requêtes.
- Ajout de nouvelles situations.
- Ajout de nouveaux espaces de travail.

Définition d'un nouveau numéro de version pour votre agent

Pour sauvegarder les modifications apportées à un agent validé, vous devez saisir un nouveau numéro de version.

Procédure

1. Ouvrez la fenêtre de l'**éditeur d'agent**, puis la page **Informations sur l'agent**.
2. Entrez une version, un chemin d'accès de correctif ou un niveau de module de correction supérieur au niveau actuel après l'invite de version.
3. Apportez les modifications à votre agent.

   Conseil : Si vous validez un agent et que vous oubliez de modifier sa version, vous êtes invité à indiquer la nouvelle version lorsque vous enregistrez l'une de vos modifications.

Modification du code produit

Si vous modifiez le code produit, l'agent devient incompatible avec toutes ses versions précédentes. Tous les enregistrements des précédentes actions de validation sont perdus et vous développez un nouvel agent.

Tout fichier, situation, commande Action ou espace de travail que vous avez exporté de IBM Tivoli Monitoring et importé dans l'agent, est supprimé de l'agent.

Si vous essayez de modifier le code produit d'un agent validé, Agent Builder affiche un avertissement et vous demande si vous voulez continuer.

Si vous cliquez sur **Oui** dans la fenêtre **Code produit de l'agent**, vous êtes averti que le contenu des fichiers de prise en charge de l'agent n'est plus valide. Vous êtes également informé que les fichiers seront supprimés lors de la prochaine sauvegarde de l'agent.

Modification des propriétés de sources de données et d'attributs

Lorsque vous ajoutez des sources de données à votre agent, Agent Builder crée des ensembles de données correspondants. Vous pouvez éditer les ensembles de données et les attributs qu'ils contiennent pour fournir les informations de surveillance nécessaires.

Procédure

Pour éditer ou supprimer les informations d'un ensemble de données (groupe d'attributs) :

1. Dans la zone **Contenu d'agent** de la page **Informations sur l'agent**, cliquez sur **Sources de données**.
   La page **Définition de la source de données** s'affiche.
2. Sélectionnez l'ensemble de données (groupe d'attributs).

   La zone d'informations de groupe d'attributs de la page est mise à jour pour afficher les propriétés de l'ensemble de données sélectionné.

   Remarque : Sinon, si vous vous trouvez sur la dernière page de l'assistant d'**agent**, vous pouvez cliquer deux fois sur la source de données pour ouvrir la fenêtre **Informations sur le groupe d'attributs**. Cette fenêtre contient les mêmes informations que la zone d'informations du groupe d'attributs de la page **Définition de la source de données**.

   Le (Tableau 260, à la page 1227) décrit les informations de zone applicables à toutes les sources de données. Utilisez les zones pour modifier les propriétés de la source de données ou de l'attribut sélectionné.

Tableau 260. Zones pour l'édition des sources de données

Nom de la zone	Description	Valeurs admissibles et exemples
Nom du groupe d'attributs	Nom de la source de données tel qu'il s'affiche dans Tivoli Enterprise Portal ou dans la console IBM Cloud Application Performance Management	Valeurs admissibles : chaîne descriptive comportant au maximum 32 caractères. Elle doit être unique dans l'agent. Le premier caractère doit correspondre à une lettre et les autres caractères peuvent être des lettres, des nombres ou des traites de soulignement. Un trait de soulignement apparaît sous la forme d'un espace. N'utilisez pas d'espaces ou de caractères spéciaux.
Texte d'aide	Texte d'aide pour la source de données	Valeurs admissibles : chaîne comportant jusqu'à 256 caractères.
Génère une ligne de données unique	La source de données renvoie 1 ligne de données. Modifiable dans toutes les sources de données échantillonnées.	Exemple : si vous surveillez la mémoire système physique, choisissez une seule ligne. Un système gère généralement l'intégralité de sa mémoire dans un pool unique ; par conséquent, une seule ligne de données peut être renvoyée.

Tableau 260. Zones pour l'édition des sources de données (suite)		
Nom de la zone	**Description**	**Valeurs admissibles et exemples**
Peut générer plusieurs lignes de données	La source de données peut renvoyer n'importe quel nombre de lignes de données. Modifiable dans toutes les sources de données échantillonnées.	Exemple : si vous surveillez des unités de disque, choisissez plusieurs lignes, car un système peut contenir plusieurs disques. Pour les clés, choisissez les attributs faisant la distinction entre les disques. Dans le cas d'un disque, l'attribut de clé est le numéro de disque, la lettre d'unité, le label de volume ou tout élément approprié de votre environnement.
Génère des événements	La source de données renvoie les données d'événement, en générant une ligne de données par événement.	Exemple : une source de données basée sur des événements SNMP envoie des notifications (alertes) lors du franchissement des seuils de performances. **Remarque :** Toutes les sources de données peuvent générer des événements.
Ajoutez ce groupe d'attributs à une catégorie de rapport	Catégorie dans le modèle généré Cognos à laquelle sont affectés les attributs de ce groupe d'attributs.	Cochez la case pour placer le groupe d'attributs dans le sous-dossier sélectionné (disponibilité ou performance). Si la case n'est pas cochée, le groupe d'attributs est placé dans le dossier **Mesures étendues** dans le modèle de données Cognos.
Catégorie mesure	Catégorie à laquelle seront affectés les attributs de ce groupe d'attributs.	Sélectionnez **Performance** ou **Disponibilité**.

Remarque :

a. Les zones **Génère une ligne de données unique** et **Peut générer plusieurs lignes de données** n'ont pas d'incidence sur les données d'une source de données d'événement.

b. Pour plus d'informations sur les données échantillonnées et les types de données d'événement, voir («Types de données», à la page 1249).

c. Pour plus d'informations sur les zones d'une source de données spécifique, voir les informations de fournisseur de données applicables dans «Définition et test de sources de données», à la page 1255.

Création, modification et suppression d'attributs

Vous pouvez créer, modifier ou supprimer des attributs dans un ensemble de données (groupe d'attributs).

Pour utiliser des attributs, ouvrez la page **Définition de la source de données**. Pour plus d'informations, voir «Page Définition de la source de données», à la page 1223.

Création d'attributs

Vous pouvez ajouter de nouveaux attributs à un ensemble de données.

Procédure

1. Cliquez avec le bouton droit de la source de données et sélectionnez **Ajouter un attribut** dans le menu.

   La page **Information d'attribut** s'ouvre.

   Remarque : La page qui s'affiche dépend de la source de données de l'attribut.
2. Indiquez vos options pour le nouvel attribut sur la page **Informations d'attribut**.

   Voir «Zones et options de définition des attributs», à la page 1232 pour plus d'informations sur les zones et les options.
3. Pour ajouter d'autres attributs, sélectionnez **Ajouter des attributs supplémentaires** et cliquez sur **Suivant**.
4. Une fois que vous avez fini d'ajouter des attributs, cliquez sur **Terminer**.

Copie d'attributs

Vous pouvez copier des attributs à partir de la page **Définition de la source de données**.

Procédure

1. Sur la page **Définition de la source de données** de l'éditeur d'agent, cliquez avec le bouton droit de la souris sur l'attribut que vous souhaitez copier, puis cliquez sur **Copier un attribut**.
2. Dans la fenêtre **Copier un attribut**, entrez le nom du nouvel attribut dans la zone **Nom**, puis cliquez sur **OK**.

Modification des attributs

Vous pouvez modifier les informations d'attribut à l'aide de la page **Définition de la source de données**.

Procédure

1. Sélectionnez l'attribut que vous souhaitez modifier.

   Le panneau **Information d'attribut** est mis à jour pour afficher les propriétés de l'attribut sélectionné.
2. Définissez vos choix pour les nouvelles informations d'attribut.

   Remarque : Sur la dernière page de l'assistant d'**agent** (page **Définition de la source de données**), vous pouvez cliquer deux fois sur l'attribut pour ouvrir la fenêtre **Informations d'attribut**. Cette fenêtre contient les mêmes informations que le panneau d'informations sur l'attribut de la page **Définition de la source de données**.

Création d'attributs dérivés

Vous pouvez créer un attribut qui dérive sa valeur d'autres attributs, au lieu de les dériver directement de la source de données.

Pourquoi et quand exécuter cette tâche

Dans l'attribut dérivé, vous pouvez effectuer des opérations sur les valeurs des attributs source. Par exemple, vous pouvez effectuer des opérations arithmétiques de base sur des attributs numériques ou la concaténation de chaînes sur des attributs de chaîne.

La syntaxe d'expression de base utilisée pour les expressions dérivées contient des fonctions. Ces dernières utilisent une manipulation plus compliquée des données, qui comprend l'agrégation à court terme, la conversion de chaîne en entier et l'accès aux propriétés de configuration et aux variables d'environnement. En outre, un éditeur vous aide à visualiser l'expression pendant sa génération.

Procédure

1. Sur la page **Définition de la source de données**, cliquez avec le bouton droit de la souris sur la source de données, puis cliquez sur **Ajouter un attribut**.
2. Sur la page **Informations d'attribut**, entrez un nom d'attribut et le texte d'aide.
3. Sélectionnez **Dérivé d'autres valeurs d'attribut**.
4. Dans la zone **Formule**, entrez le texte de la formule ou cliquez sur **Editer** pour entrer la formule via un éditeur graphique.

   Pour plus d'informations sur les opérateurs et les fonctions pouvant être utilisés dans la formule, voir «Opérateurs et fonctions de formule», à la page 1242.

   Remarque : Lorsque vous cliquez sur **Editer**, l'éditeur de formules s'ouvre. Pour plus d'informations sur la modification d'attributs dérivés, voir «Modification des attributs dérivés», à la page 1231.
5. Facultatif : Sélectionnez ou décochez la case **Calculs des intervalles spécifiques** pour déterminer quelles sont les valeurs d'exemple d'attribut qui sont utilisées lorsque la fonction est calculée.

   Utilisez cette option lorsque votre formule utilise les fonctions `taux` ou `delta`. Pour plus d'informations sur **Calculs des intervalles spécifiques**, voir «Calculs des intervalles spécifiques», à la page 1230. Pour plus d'informations sur les fonctions `débit` et `delta`, voir «Opérateurs et fonctions de formule», à la page 1242.
6. Dans la zone **Type d'attribut**, cliquez sur le type d'attribut.
7. Cliquez sur **OK**.

   La page **Définition de la source de données** s'affiche de nouveau avec la source de données indiquée comme auparavant.
8. Cliquez sur **Terminer**.

   Important : Si vous créez un attribut dérivé qui fait référence à un autre attribut dérivé, assurez-vous que l'attribut référencé est répertorié avant le nouvel attribut. Si un attribut fait référence à un autre attribut dérivé qui se trouve plus loin dans la liste, l'agent ne peut pas afficher la valeur de cet attribut. Si vous créez un tel attribut, Agent Builder affiche un avertissement.

Calculs des intervalles spécifiques

Vous pouvez choisir **Calculs des intervalles spécifiques** lorsque vous définissez un attribut dérivé basé sur les fonctions `taux` ou `delta`.

Vous devez sélectionner **Calculs des intervalles spécifiques** dans l'onglet **Détails de l'attribut dérivé** de la page **Informations d'attribut**. Pour plus d'informations, voir «Création d'attributs dérivés», à la page 1229.

Lorsque vous choisissez **Calculs des intervalles spécifiques**, il est important de comprendre le principe d'un delta ou d'une différence entre les valeurs d'attribut. Le delta correspond à la différence entre la valeur la plus récente de l'attribut et une valeur précédente de celui-ci. Le delta est renvoyé directement par la fonction `delta` et est utilisé par la fonction `rate` pour calculer un résultat.

La fonction `delta` ou `rate` doit toujours avoir la fonction `dernière` comme argument unique. La fonction`dernière` indique quelles valeurs d'un attribut sont utilisées pour déterminer le delta. Si **Calculs des intervalles spécifiques** n'est pas sélectionné, la valeur précédente utilisée correspond toujours à la deuxième valeur la plus récente. Si **Calculs des intervalles spécifiques** est sélectionné, la valeur précédente utilisée correspond à la valeur dont l'ancienneté (par rapport à la valeur la plus récente) est égale à l'intervalle de collecte du demandeur.

Par exemple, supposons que `CDP_DP_REFRESH_INTERVAL` est défini sur 120 secondes et que `Affecter A` contient les valeurs échantillonnées suivantes :

Date et heure	**Valeur échantillonnée**
En cours	`2800`
il y a 2 minutes (120 secondes)	`2600`
il y a 4 minutes (240 secondes)	`2499`

Date et heure	Valeur échantillonnée
il y a 6 minutes (360 secondes)	1500
il y a 8 minutes (480 secondes)	1200
il y a 10 minutes (600 secondes)	1000

Si **Calculs des intervalles spécifiques** n'est pas sélectionné, la fonction delta renvoie toujours 200, à savoir la différence entre les deux valeurs les plus récentes, 2800 - 2600. La même valeur est renvoyée si la valeur s'affiche sur Tivoli Enterprise Portal ou dans la console IBM Cloud Application Performance Management, utilisée dans une situation ou une collecte d'historique.

Lorsque **Calculs des intervalles spécifiques** est sélectionné, la fonction delta renvoie une valeur qui dépend de l'intervalle de collecte défini par le demandeur.

Si un attribut dérivé comportant la fonction delta est utilisé dans une situation avec un intervalle de collecte 4 minutes, la valeur renvoyée par la fonction delta est 301, à savoir la différence entre la valeur la plus récente et la valeur obtenue 4 minutes avant, 2800 - 2499.

Si un attribut dérivé comportant la fonction rate est utilisé dans une situation avec un intervalle de collecte de 10 minutes (600 secondes), la valeur renvoyée par la fonction rate est 3, à savoir la différence entre la valeur la plus récente et la valeur obtenue 10 minutes avant, divisée par le nombre de secondes dans l'intervalle (2800 à 1000)/600.

Remarque : Tivoli Enterprise Portal ne présente aucun intervalle de collecte inhérent, ce qui signifie que les calculs de delta et de débit pour les requêtes de Tivoli Enterprise Portal utilisent toujours la valeur d'attribut la plus récente et la deuxième valeur la plus récente, le même résultat, que **Calculs spécifiques à un intervalle** soit sélectionné ou non.

Pour que delta ou débit fonctionnent correctement avec les **Calculs des intervalles spécifiques**,

- l'agent doit collecter les données périodiquement en arrière-plan et non à la demande (CDP_DP_THREAD_POOL_SIZE doit être supérieure à 0).
- Chaque situation ou intervalle de collecte d'historique dans lequel l'attribut est utilisé doit être un multiple de l'intervalle d'actualisation d'arrière-plan (CDP_DP_REFRESH_INTERVAL).
- Le nombre (le deuxième argument de la dernière fonction) doit être suffisant pour contenir le plus grand intervalle de collecte d'une situation ou d'une collecte d'historique. Par exemple, si l'agent doit prendre en charge la collecte d'historique de 10 minutes (600 secondes) et que CDP_DP_REFRESH_INTERVAL est de 120 secondes, le nombre doit être au moins 6, 1+(600/120). Un nombre de valeurs correspondant à 6 garantit que la fonction dernière renvoie l'échantillon le plus récent et échantillonne jusqu'à 600 secondes.

Remarque : Si ces conditions ne sont pas remplies, les valeurs en entrée ne sont probablement pas valides et le résultat 0 est renvoyé.

Modification des attributs dérivés
Utilisez l'éditeur de formule pour modifier les attributs dérivés.

L'éditeur de formules est disponible sur la page **Information d'attribut** pour un attribut dérivé, comme décrit dans «Création d'attributs dérivés», à la page 1229. Pour plus d'informations sur l'éditeur de formule, voir «Editeur de formule», à la page 1237.

Suppression d'attributs
Vous pouvez supprimer un ou plusieurs attributs d'un ensemble de données à l'aide de la page **Définition de la source de données**.

Procédure

- Pour supprimer un ou plusieurs attributs, cliquez avec le bouton droit de la souris sur le ou les attributs, puis sélectionnez **Supprimer** dans le menu qui s'affiche.

Remarque : Vous ne pouvez pas supprimer un attribut qui est utilisé par un attribut dérivé. Vous devez d'abord supprimer la référence à l'attribut dérivé à l'attribut que vous supprimez.

Zones et options de définition des attributs
Description des informations de zone et des options de la page **Informations d'attribut** qui sont applicables à toutes les sources de données

Pour plus de détails sur les informations de zone caractéristiques de chacune des sources de données, consultez la documentation correspondante pour chaque source de données.

Tableau 261. Zones et options de définition des attributs

Noms/options de zone	Description	Valeurs admises
Nom de l'attribut	Nom de l'attribut tel qu'il s'affiche dans Tivoli Enterprise Portal ou dans la console IBM Cloud Application Performance Management	Chaîne comportant les caractères suivants : • A-Z • _ • a-z • 0-9 **Remarque :** Le nom doit commencer par A-Z ou a-z. Le nom d'attribut est limité à 63 caractères et le nom du groupe d'attributs à 63 caractères
Texte d'aide	Texte d'aide pour l'attribut	Chaîne
Masqué - ne peut être utilisé que dans un attribut dérivé	S'il est sélectionné, l'attribut ne s'affiche pas dans Tivoli Enterprise Portal ou dans la console IBM Cloud Application Performance Management. Voir la remarque à la dernière ligne.	Non applicable
Dérivé d'autres valeurs d'attribut	La valeur de l'attribut doit être calculée à partir des valeurs des autres attributs	Non applicable
Attribut de clé	L'attribut est une clé de la table. Indique si cet attribut aide à définir de façon unique l'objet sur lequel un rapport est en cours de génération. Si les données sont entreposées et récapitulées, les attributs de clé sont utilisés pour cumuler des données dans les tables récapitulatives.	Cette option n'est pas disponible pour les attributs Perfmon.

Tableau 261. Zones et options de définition des attributs (suite)		
Noms/options de zone	**Description**	**Valeurs admises**
Sous-fenêtre **Informations d'attribut**	Le contenu de cet onglet est fonction du type de source de données dont fait partie cet attribut. Pour plus de détails, consultez les informations du chapitre relatif à la source de données à surveiller. Pour un attribut dérivé, dans la zone **Formule**, entrez une formule pour calculer la valeur de l'attribut en fonction d'autres attributs ou constantes. Vous pouvez taper la formule dans la zone **Formule** ou cliquer sur **Modifier** pour utiliser l'éditeur de formules graphique. Voir «Editeur de formule», à la page 1237.	
Type d'attribut	Décrit la manière dont l'attribut s'affiche dans Tivoli Enterprise Portal ou dans la console IBM Cloud Application Performance Management. Il existe trois types d'attributs : • Chaîne • Numérique • Horodatage «Types d'attribut», à la page 1233 contient des informations détaillées sur les types d'attribut.	Le Tableau 262, à la page 1234 contient des descriptions des valeurs de type d'attribut numériques.
Enumérations	Il peut s'agir d'une valeur d'échelle zéro numérique ou d'une valeur de chaîne.	Ajoutez vos énumérations dans le tableau à l'aide de la procédure décrite dans «Spécification d'une énumération pour un attribut», à la page 1236. Le nom de l'énumération s'affiche dans Tivoli Enterprise Portal ou dans la console IBM Cloud Application Performance Management lorsque la valeur correspondante est reçue dans l'attribut à partir de l'agent. Cet attribut est utilisé pour un ensemble de valeurs caractéristiques avec des significations (par exemple, 1=UP, 2=DOWN).
Remarque : Dans les cas où l'attribut est utilisé dans des calculs avec d'autres attributs, il y a des raisons pour ne pas afficher la valeur de base. Par exemple, un nombre qui représente un comptage d'octet boucle tellement rapidement qu'il est peu utile.		

Types d'attribut
Il existe trois types d'attributs

Ces trois types sont :

- Chaîne
- Numérique

- Horodatage

Attributs de chaîne

Lorsque vous sélectionnez **Chaîne**, utilisez la zone **Taille maximale** pour indiquer la longueur maximale de la chaîne en octets. La taille par défaut est de 64 octets.

Valeur de chaîne pouvant comporter tout caractère UTF-8. La taille maximale est la longueur totale, en octets, de la mémoire tampon attribuée pour contenir la chaîne. Certains caractères UTF-8 non ASCII occupent plus d'un octet ; vous devez donc en tenir compte lorsque vous sélectionnez une taille maximale. Le regroupement de données dans l'entrepôt de données affiche la dernière valeur collectée pendant la période.

Numérique

Lorsque vous indiquez **Numérique**, vous pouvez définir un certain nombre d'options. Pour plus d'informations sur ces options, voir Tableau 262, à la page 1234.

Horodatage

Un attribut Horodatage est un attribut Chaîne au format `SAAMMJJHHMMSSmmm` (où S=1 pour le 21e siècle). Tous les 16 caractères doivent être utilisés pour des scripts ou des clients de socket. Lorsqu'il est affiché dans Tivoli Enterprise Portal ou dans la console IBM Cloud Application Performance Management, un type d'attribut horodatage s'affiche dans le format approprié à l'environnement local.

Lorsque vous utilisez la fonction Parcourir pour WMI, Agent Builder marque automatiquement en tant qu'horodatages les attributs dont le modèle CIM est `CIM_DATETIME`. Le fournisseur de données convertit automatiquement les attributs WMI vers ce format.

Aspects numériques des attributs
Descriptions des aspects de taille, objectif,échelle et plage des attributs.

Lorsque vous indiquez un attribut numérique, vous devez spécifier la taille, le but, l'échelle et la plage de l'attribut. Pour plus d'informations, voir Tableau 262, à la page 1234.

Tableau 262. Options d'attribut numérique

Aspects numériques	Options et zones	Description
Taille	**32 bits** **64 bits**	La valeur des nombres 32 bits peut être comprise entre `-2147483648` et `2147483647` (soit environ `-2 000 000 000` à `2 000 000 000`). La valeur des nombres 64 bits peut être comprise entre `-9223372036854775808` et `9223372036854775807` (soit environ $-9x10^{18}$ à $9x10^{18}$)

Tableau 262. Options d'attribut numérique (suite)

Aspects numériques	Options et zones	Description
Objet	**Jauge**	Valeurs entières lorsque les valeurs brutes renvoyées sont supérieures ou inférieures aux valeurs précédentes. Les valeurs négatives sont prises en charge. Ce type est le type par défaut pour les entiers. Le regroupement de données dans l'entrepôt de données produit les valeurs minimum, maximum et moyenne.
	Compteur	Valeur entière positive contenant des valeurs brutes qui augmentent généralement au fil du temps. Le regroupement de données dans l'entrepôt de données affiche les valeurs totale, supérieure, inférieure et delta la plus récente. Dans l'exemple ci-après de calculs basés sur un delta, où les valeurs de données détaillées en une heure sont 9, 15, 12, 20 et 22, le traitement basé sur un delta respecte les règles suivantes : • Si la valeur courante est supérieure ou égale à la valeur précédente, la sortie est égale à la valeur précédente moins la valeur courante • Si la valeur courante est inférieure à la valeur précédente, la sortie est égale à la valeur courante • 15 étant supérieur à 9, la sortie égale 6 • 12 étant inférieur à 15, la sortie égale 12 • 20 étant supérieur à 12, la sortie égale 8 • 22 étant supérieur à 20, la sortie égale 2 • La valeur TOT_ est 28, qui correspond au total des sorties • La valeur LOW_ est 2, qui correspond au minimum de sorties • a valeur HI_ est 12, qui correspond au maximum de sorties
	Propriété	Propriété de l'objet qui ne change pas fréquemment. Le regroupement de données dans l'entrepôt de données affiche la dernière valeur collectée pendant la période.
	Delta	Valeur entière représentant la différence entre la valeur actuelle et la valeur précédente de cet attribut. Cet attribut étant représenté sous forme d'une jauge dans l'entrepôt de données, le regroupement de données dans l'entrepôt de données produit les valeurs minimum, maximum et moyenne.
	Modification en pourcentage	Une valeur entière qui représente le pourcentage de modification entre la valeur actuelle et la valeur précédente. Ce type est calculé selon la formule : `((nouvelle - précédente)*100)/précédente`. Cet attribut étant représenté sous forme d'une jauge dans l'entrepôt de données, le regroupement de données dans l'entrepôt de données produit les valeurs minimum, maximum et moyennes.
	Fréquence de modification	Valeur entière représentant la différence entre la valeur actuelle et la valeur précédente, divisée par le nombre de secondes entre les échantillons. Convertit une valeur (telle que des octets) en valeur par seconde (octets par seconde). Cet attribut étant représenté sous forme d'une jauge dans l'entrepôt de données, le regroupement de données dans l'entrepôt de données produit les valeurs minimum, maximum et moyennes.

Tableau 262. Options d'attribut numérique (suite)		
Aspects numériques	**Options et zones**	**Description**
Echelle	**Ajustement décimal**	L'échelle détermine la quantité de décimales figurant dans le nombre. Chaque décimale réduit la plage mentionnée ci-dessus d'un facteur de 10. Par exemple, un ajustement décimal de 2 affiche deux décimales et, dans un nombre 32 bits, la plage admissible devient -21474836.48 à 21474836.47. Lorsqu'un ajustement décimal différent de zéro est indiqué, le nombre est manipulé en interne sous la forme d'un nombre en virgule flottante. Par conséquent, il se peut que la précision des nombres 64 bits élevés soit réduite.
Plage	**Minimum** **Maximum**	La plage indique la plage attendue de la valeur. Si aucune plage minimale ou maximale n'est indiquée, les valeurs maximales décrites ci-dessus sont utilisées. La plage sert à générer une vue initiale plus utile dans certaines vues d'espace de travail Tivoli Monitoring graphiques.

Spécification d'une énumération pour un attribut
Spécifiez une énumération de valeurs à l'aide de la page **Informations d'attribut** .

Pourquoi et quand exécuter cette tâche
La spécification d'une énumération pour un attribut nécessite une procédure courte. Lorsqu'est rencontrée une valeur pour laquelle une énumération a été définie, le nom de l'énumération s'affiche dans Tivoli Enterprise Portal ou dans la console IBM Cloud Application Performance Management au lieu de la valeur.

Procédure

1. Dans la zone **Type d'attribut** de la page **Informations d'attribut**, cliquez sur **Numérique**.
2. Dans la zone **Enumérations**, cliquez sur une énumération puis sur **Ajouter**.
   La fenêtre **Définition d'énumération** s'affiche.
3. Entrez le nom et la valeur de l'énumération dans les zones de la fenêtre.
4. Cliquez sur **OK**.
   Vous pouvez ensuite ajouter des énumérations.

Spécification de la gravité pour un attribut utilisé comme indicateur de statut
Dans un environnement IBM Cloud Application Performance Management, un tableau de bord récapitulatif doit afficher un statut. Vous devez utiliser un attribut pour indiquer la valeur du statut. Pour cet attribut, vous devez spécifier des valeurs qui indiquent une gravité de statut spécifique.

Pourquoi et quand exécuter cette tâche
L'attribut utilisé pour indiquer le statut doit être de type numérique. Sélectionnez cet attribut dans l'assistant de **Configuration du tableau de bord** ; pour obtenir des instructions sur l'utilisation de cet assistant, voir «Préparation de l'agent pour Cloud APM», à la page 1417.

Vous pouvez spécifier des valeurs pour l'attribut qui correspondent à la gravité Normale, Avertissement et Critique. Toute autre valeur indique un statut de gravité "Inconnu" ; vous pouvez également définir de manière explicite certaines valeurs comme "Non défini", le statut "Inconnu" s'affiche alors pour ces valeurs.

Procédure

1. Sélectionnez l'attribut que vous souhaitez modifier.

Le panneau Informations sur l'attribut est mise à jour pour afficher les propriétés de l'attribut sélectionné.

2. Dans le panneau des informations d'attribut, cliquez sur l'onglet **Gravité**.
3. Sélectionnez la gravité requise (Normale, Avertissement, Critique ou Non défini) et cliquez sur **Editer**.
4. Sélectionnez **Plage** ou **Nombre unique**, entrez la plage de valeurs ou une valeur numérique unique, puis cliquez sur **Ok**.
5. Facultatif : Si vous devez ajouter une autre valeur pour la même gravité (par exemple : 2 et 25 indiquent un avertissement), cliquez sur **Ajouter**, sélectionnez la gravité, entrez la valeur et cliquez sur **OK**.

Filtrage des groupes d'attributs

Vous pouvez créer un filtre pour limiter les données renvoyées depuis un groupe d'attributs qui renvoie des données échantillonnées.

Avant de commencer

Si le groupe d'attributs existe déjà, ouvrez la page **Définition de la source de données**. Pour plus d'informations, voir «Page Définition de la source de données», à la page 1223.

Si vous souhaitez créer un groupe d'attributs, suivez la procédure décrite dans «Définition de sources de données initiales», à la page 1206, puis cliquez sur **Avancé** dans la page d'informations de la source de données initiale.

Procédure

1. Pour commencer à créer le filtre, choisissez l'une des opérations suivantes :
   - Si vous créez un groupe d'attributs, cliquez sur **Avancé** dans la page d'informations de la source de données initiale.
   - Si le groupe d'attributs existe, sélectionnez-le dans la page **Définition de la source de données** et cliquez sur **Avancé** dans la page **Définition de la source de données**.
2. Dans la page **Propriétés avancées de la source de données**, entrez une formule de sélection. La formule de sélection entrée doit donner un résultat booléen, à savoir vrai ou faux.

   Dans la page **Propriétés avancées de la source de données**, vous pouvez cliquer sur **Modifier** pour entrer ou modifier la formule à l'aide de l'éditeur de formule. Pour plus d'informations sur l'éditeur de formule, voir «Editeur de formule», à la page 1237.
3. Après avoir entré la formule de sélection de filtre, cliquez sur **OK** jusqu'à ce que vous reveniez à la page **Définition de la source de données**.

   Lorsque le filtre est créé, l'agent l'utilise pour évaluer chaque ligne de données. Lorsque le filtre donne la valeur *vrai* pour une ligne de données, les données sont envoyées à IBM Tivoli Monitoring ou IBM Cloud Application Performance Management. Lorsque le filtre a pour résultat *faux*, la ligne de données n'est pas envoyée et elle est supprimée.

Que faire ensuite

Vous pouvez confirmer que le filtre effectue la tâche prévue à l'aide de la fonction de test du groupe d'attributs. Pour plus d'informations sur le test des groupes d'attributs, voir «Test des groupes d'attributs», à la page 1420.

Editeur de formule

L'éditeur de formule permet de créer et modifier des formules dans Agent Builder.

L'éditeur de formule, qui consiste en un outil graphique, s'affiche lors de l'exécution de l'une des tâches suivantes :

1. Création ou modification d'attributs dérivés, voir «Création d'attributs dérivés», à la page 1229 et «Modification des attributs dérivés», à la page 1231

2. Création de groupes d'attributs filtrés, voir «Création d'un groupe d'attributs filtré», à la page 1383
3. Filtrage des données à partir de groupes d'attributs, voir «Filtrage des groupes d'attributs», à la page 1237

Avertissement :

- Lorsque vous créez des attributs dérivés, la formule créée doit donner un type de données qui correspond au type de l'attribut. Par exemple, si le type d'attribut dérivé est un nombre, la formule créée doit donner un résultat numérique.
- Lors de la création de groupes d'attributs filtrés ou du filtrage de données à partir de groupes d'attributs, la formule créée doit donner une valeur booléenne, à savoir "vrai" ou "faux".

Remarque : Dans les vues suivantes, l'éditeur de formule affiche la création de formules pour les attributs dérivés. Les vues sont identiques lors de l'utilisation de l'éditeur de formule avec des groupes d'attributs filtrés ou pour filtrer les données des groupes d'attributs. Les vues affichent l'en-tête **Editeur de formule dérivée** ou **Editeur de formule filtrée** en fonction de l'utilisation.

Lorsque l'éditeur de formule s'affiche, la formule en cours est chargée dans l'éditeur. Si aucune formule n'existe, vous pouvez en entrer une en la tapant directement dans l'espace de formule dans la fenêtre de **l'éditeur de formule**. Sinon, vous pouvez cliquer sur **Insérer** pour commencer à entrer une formule à l'aide des options du menu de l'éditeur. L'éditeur contient deux vues de la formule dans la fenêtre par défaut, ainsi qu'une option pour une troisième vue :

Vue de composant (par défaut)
Les composants de la formule en cours d'édition sont affichés dans les zones **opérande** et **Opérateur**. L'opérateur et ses deux opérandes peuvent être modifiés à l'aide des menus de sélection.

Vue de formule (par défaut)
La formule complète se trouve dans la zone de formule dans la fenêtre. Vous pouvez modifier la formule en complétant cette case.

Vue de l'arborescence hiérarchique des formules (option)
L'arborescence hiérarchique des formules s'affiche en cochant la case **Afficher la hiérarchie des formules**. L'état de la case à cocher est mémorisé dans les appels ultérieurs de l'éditeur de formule.

Modification de la vue de composant Editeur de formule

Modifiez la vue de composant de l'éditeur de formule.

Pourquoi et quand exécuter cette tâche

Le composant affiché dans la vue de composant peut être modifié à l'aide des méthodes suivantes :

Procédure

- Déplacez le curseur dans le texte de la formule.
- Sélectionnez un noeud différent dans l'arborescence hiérarchique des formules.
- Cliquez sur **Monter d'un niveau** ou sur l'un des boutons Modifier.

Types de composant

Vous pouvez utiliser l'éditeur de formule pour modifier le composant en cours et tous les opérandes ou arguments de fonction de ce composant. Lorsqu'ils sont sélectionnés, certains composants peuvent s'afficher différemment dans l'éditeur de formule.

Composant Attribut de l'éditeur de formule

Utilisez le composant Attribut de l'éditeur de formule pour sélectionner et manipuler les attributs dans des formules.

Pourquoi et quand exécuter cette tâche

Vous pouvez sélectionner un attribut dans une liste d'attributs pour le groupe d'attributs dans la vue de composant de l'éditeur de formule.

Procédure

1. Pour travailler avec un attribut spécifique, sélectionnez cet attribut dans la liste et cliquez sur **Editer**.
   La fenêtre **Modifier l'attribut sélectionné** s'ouvre.
2. Vous pouvez manipuler l'attribut sélectionné des manières suivantes :
   - Vous pouvez remplacer l'attribut par une chaîne ou un nombre en sélectionnant **Chaîne** ou **Nombre**. La liste d'attributs est remplacée par une zone d'entrée et le contenu n'est plus comparé à la liste des noms d'attributs valides.
   - Vous pouvez remplacer l'attribut par une fonction en cliquant sur **Fonction**. Des parenthèses sont ajoutées après le nom et la liste contient des noms de fonction valides que vous pouvez sélectionner.
   - Vous pouvez taper un nom d'attribut au lieu d'en sélectionner un. Cela est utile si vous n'avez pas encore défini tous les attributs de ce groupe d'attributs.
     – Un avertissement s'affiche s'il n'existe aucun attribut portant le nom entré.
     – Une erreur s'affiche si des caractères ne pouvant pas faire partie d'un nom d'attribut sont entrés.
     – Le bouton **OK** est désactivé tant que l'avertissement ou l'erreur n'est pas corrigé(e).
   - Les attributs ne sont pas filtrés en fonction du type. Si un attribut (ou une valeur) du type incorrect est sélectionné ou entré, un message d'avertissement s'affiche.

Composants Littéraux de l'éditeur de formule

Utilisez les composants chaîne et nombre de l'éditeur de formule pour manipuler les littéraux dans des formules.

Pourquoi et quand exécuter cette tâche

Un littéral correspond à toute valeur entrée directement dans la formule qui ne provient pas d'une valeur d'attribut ou d'une fonction. Une valeur littérale peut être soit une chaîne ou un nombre.

Procédure

- Vous pouvez remplacer une chaîne ou un nombre littéral par un attribut en cliquant sur **Attribut**. Un nom d'attribut valide doit être sélectionné ou entré sans guillemets.
- Vous pouvez remplacer une chaîne ou un nombre littéral par une fonction en cliquant sur **Fonction**. Des parenthèses sont ajoutées après le nom et la liste de sélection contient des noms de fonction valides que vous pouvez sélectionner.
  – Un avertissement s'affiche si un nombre est entré dans un emplacement où une chaîne est attendue, ou vice versa.
  – Si **Nombre** est sélectionné, un message d'erreur s'affiche si le contenu de la zone n'est pas un nombre. Le bouton **OK** est désactivé tant que l'erreur n'est pas corrigée.

Composant Opérateur de l'éditeur de formule

Utilisez le composant Opérateur de l'éditeur de formule pour manipuler les opérateurs dans les formules.

Pourquoi et quand exécuter cette tâche

Un composant Opérateur affiche un opérateur et ses opérandes.

Procédure

- Dans la vue du composant Editeur de formule, sélectionnez l'opérateur à partir de la liste **Opérateur** entre les deux opérandes. L'opérateur (%) multiple le premier opérande par 100, puis le divise par le second opérande.
- Sélectionnez l'opérateur (`+ - * / ou %`).
  – La section **Opérande de gauche** de la page est située avant l'opérateur.

- La section **Opérande de droite** est située après l'opérateur.
- Les opérandes simples (attributs et littéraux) peuvent être modifiés sans qu'il soit nécessaire de remplacer le composant sélectionné par l'opérande, comme décrit dans «Composant Attribut de l'éditeur de formule», à la page 1238 et «Composants Littéraux de l'éditeur de formule», à la page 1239.
- Vous pouvez modifier les opérandes complexes, qui sont constitués d'autres opérateurs ou fonctions, en cliquant sur **Modifier**. Cette action sélectionne le composant opérande au lieu de l'opérateur tout entier.

Composant Expression conditionnelle dans l'éditeur de formule

Le composant Expression conditionnelle associe une condition à une valeur à renvoyer si la condition est vraie, et à une valeur à renvoyer si la condition est fausse.

- L'expression de la section **Condition** doit s'évaluer par rapport aux critères Vrai ou Faux. Les opérateurs `(==)`, `(!=)`, `(<)`, `(<=)`, `(>)`, `(>=)`, `(&&)`, `(||)`, `(!)` sont disponibles pour former des expressions qui renvoient Vrai ou Faux.
- Les opérandes simples (attributs et littéraux) peuvent être modifiés sans qu'il soit nécessaire de remplacer le composant sélectionné par l'opérande, comme décrit dans «Composant Attribut de l'éditeur de formule», à la page 1238 et «Composants Littéraux de l'éditeur de formule», à la page 1239.
- Vous pouvez modifier des opérandes complexes, qui sont constitués d'autres opérateurs ou fonctions, en cliquant sur Modifier. Cette action sélectionne le composant opérande au lieu de l'expression conditionnelle tout entière.
- Voir «Options communes de l'éditeur de formule», à la page 1241 pour obtenir des informations sur l'utilisation des options suivantes : **Insérer**, **Supprimer**, **Monter d'un niveau** et **Modifier**.

Concepts associés

«Editeur de formule», à la page 1237
L'éditeur de formule permet de créer et modifier des formules dans Agent Builder.

Composant Fonction de l'éditeur de formule
Utilisez le composant Fonction de l'éditeur de formule pour sélectionner et manipuler les composants Fonction dans des formules.

Pourquoi et quand exécuter cette tâche

Le composant Fonction affiche la fonction et ses arguments.

Procédure

- Pour utiliser les fonctions, sélectionnez le **nom de la fonction** dans la liste de l'éditeur de formule.
  - La description de la fonction sélectionnée apparaît après la fonction.
  - Les sections **Argument de fonction** s'affichent sous le nom de la fonction. Le nombre approprié d'arguments pour la fonction sélectionnée est affiché. La description de la fonction est affichée.
  - Les arguments simples (attributs et littéraux) peuvent être modifiés sans qu'il soit nécessaire de remplacer le composant sélectionné par l'opérande, comme décrit dans «Composant Attribut de l'éditeur de formule», à la page 1238 et «Composants Littéraux de l'éditeur de formule», à la page 1239.
  - Vous pouvez modifier les arguments complexes, qui sont constitués d'opérateurs ou d'autres fonctions, en cliquant sur **Modifier**. Cette action sélectionne le composant argument au lieu de la fonction tout entière.
- Pour les fonctions qui utilisent un nombre variable d'arguments, ajoutez des arguments en cliquant sur **Insérer** ou supprimez des arguments en cliquant sur **Supprimer** en sus des actions décrites dans «Options communes de l'éditeur de formule», à la page 1241.

- Pour la fonction `getenv`, vous pouvez choisir une propriété de configuration en cliquant sur **Insérer**. Si vous sélectionnez l'option de propriété de configuration, la fenêtre **Propriétés de configuration** s'affiche.

Options communes de l'éditeur de formule
Vous pouvez utiliser certaines options dans toutes les vues de l'éditeur de formule

Les options communes dans l'éditeur de formule sont les suivantes :

- **Insertion**
- **Supprimer**
- **Monter d'un niveau**
- **Modifier**

Insertion

Insérer permet d'insérer un opérateur ou une fonction au-dessus du composant. Le composant est rétrogradé à l'un des opérandes de l'opérateur ou à l'un des arguments de la fonction. Par exemple, si vous cliquez sur **Insérer** avant la fonction `sqrt(attr2)`, vous êtes invité à indiquer ce que vous voulez insérer et les choix suivants s'affichent :

- **Un opérateur dont l'un des opérandes est sqrt(attr2)**
- **Une fonction dont le premier argument est sqrt(attr2)**
- **Une expression conditionnelle avec sqrt(attr2) comme valeur Vraie ou Fausse**

Si vous cliquez sur **Insérer** avant la fonction `getenv`, vous êtes invité à indiquer ce que vous voulez insérer et les choix suivants s'affichent :

- **Configuration property** : utilisez cette option pour récupérer la valeur d'une propriété de configuration que vous avez configurée pour l'agent, ou la valeur de n'importe quelle variable d'environnement (par exemple, `JAVA_HOME`) sur l'hôte qui exécute l'agent.
- **Un opérateur dont l'un des opérandes est attr2**
- **Une fonction dont le premier argument est attr2**
- **Une expression conditionnelle avec attr2 comme valeur Vraie ou Fausse.**

Supprimer

Supprimer n'est disponible que pour les opérateurs et les fonctions, et correspond à l'inverse de l'option **Insérer**. Lorsque vous cliquez sur **Supprimer**, vous êtes invité à indiquer l'élément devant remplacer l'opérateur ou la fonction supprimée. Par exemple, **Supprimer** avant la fonction `sqrt(attr2)` affiche les options suivantes :

- **L'actuel argument 1, attr2**
- **Une nouvelle chaîne, un nouveau nombre ou une nouvelle référence d'attribut**

Sélectionnez **Une nouvelle chaîne, un nouveau nombre ou une nouvelle référence d'attribut** pour éliminer l'ensemble de l'arborescence après le point à supprimer et remplacez-le par une nouvelle valeur d'attribut ou littérale.

Cliquez sur **L'argument en cours** pour promouvoir l'opérande ou l'argument sélectionné pour remplacer l'opérateur ou la fonction supprimés. Vous pouvez cliquer sur les choix suivants s'il existe plusieurs arguments ou opérandes. Tous les autres opérandes ou arguments sont ignorés.

Monter d'un niveau

Cliquez sur **Monter d'un niveau** pour remonter dans l'arborescence.

Modifier

Cliquez sur **Modifier** avant un opérande ou un argument complexe pour le définir comme composant à modifier.

Cliquez sur **Monter d'un niveau** après avoir cliqué sur **Modifier** pour restaurer le composant en cours. Le composant retrouve l'état dans lequel il était avant que vous ne cliquiez sur **Modifier**.

Editeur de formule - Erreurs de formule
Elimination des erreurs de formule dans l'**éditeur de formule**

La vue de composant est différente lorsqu'elle ne contient aucune formule ou que la formule entrée ne peut pas être analysée. Elle n'affiche pas d'arborescence de formules, mais un message d'erreur.

Vous pouvez corriger une formule comportant des erreurs d'analyse syntaxique, en complétant directement la zone de formule, ou en la remplaçant par une nouvelle formule en cliquant sur **Insérer**. Dans ce cas, **Insérer** présente les choix suivants :

- **Un attribut**
- **Une chaîne**
- **Un nombre**
- **Un opérateur**
- **Une expression conditionnelle**
- **Une fonction**

Concepts associés

«Editeur de formule», à la page 1237
L'éditeur de formule permet de créer et modifier des formules dans Agent Builder.

Opérateurs et fonctions de formule

Référence d'opérateurs et de fonctions de formule (avec des exemples) utilisés dans l'éditeur de formule.

La valeur d'un attribut dérivé est le résultat de l'évaluation d'une expression en fonction de constantes et des valeurs d'autres attributs dans la même source de données. Les règles grammaticales d'expression sont l'expression mathématique normale - opérande opérateur opérande, en utilisant les parenthèses pour les regroupements. Les attributs numériques peuvent être regroupés avec d'autres attributs ou constantes numériques à l'aide des opérateurs mathématiques normaux : `+ - * /, et %`, qui multiplient **l'opérande de gauche** par 100 et divisent **l'opérande de droite**. Les attributs de chaîne peuvent être regroupés avec d'autres attributs ou constantes de chaîne à l'aide de +. Vous pouvez également utiliser les fonctions suivantes. Les fonctions sont entrées dans le format `function_name(argument_1, argument_2, argument_3)`.

Un attribut est représenté par son nom (le même nom que vous voyez dans l'arborescence Informations sur la **source de données**). Les constantes de type entier sont indiquées sous forme de nombres. Les constantes de chaîne sont placées entre apostrophes.

Vous pouvez utiliser les fonctions suivantes dans une formule :

abs
Renvoie la valeur absolue d'un nombre.

atof
Convertit une chaîne en valeur en virgule flottante.

atoi
Convertit une chaîne en valeur entière. Elle fonctionne de la même façon que la fonction **C atoi** normale : elle s'arrête au premier caractère non décimal.

average
Renvoie une valeur unique correspondant à la moyenne d'un ensemble de valeurs. Ce dernier est issu des arguments de la fonction. Plusieurs valeurs individuelles peuvent être fournies (par exemple, des noms d'attribut ou des constantes), chacune dans un argument distinct. Par ailleurs, la dernière

fonction peut être le seul argument de cette fonction (pour calculer la moyenne des valeurs les plus récentes d'un attribut).

Exemples de cette fonction utilisée :

```
average (Attr_A, AttrB, Attr_C)
```

```
average (last (Attr_A, 10))
```

Plafond
Renvoie le plus petit entier qui n'est pas inférieur à l'argument.

Par exemple, quand `attribute_a = 12.4`, `ceiling(attribute_a)` renvoie la valeur 13. Et quand `attribute_a = -12.4`, `ceiling(attribute_a)` renvoie la valeur -12.

delta
La différence entre la valeur la plus récente d'un attribut et une valeur précédemment collectée de cet attribut. L'argument unique de delta doit être la `dernière` fonction, laquelle extrait les valeurs en cours et antérieures d'un attribut. Une utilisation normale ressemble à :

```
delta (last(OtherAttribute, 2))
```

Pour plus d'informations sur les valeurs d'attribut issues de la dernière fonction qui sont utilisées pour calculer le delta, voir «Calculs des intervalles spécifiques», à la page 1230. Cette fonction est applicable uniquement pour les attributs dérivés, et non pour les filtres de groupes d'attributs.

floor
Renvoie le plus grand entier qui n'est pas supérieur à l'argument.

Par exemple, quand `attribute_a = 12,4`, `floor(attribute_a)` renvoie la valeur 12. Et quand `attribute_a = -12.4`, `floor(attribute_a)` renvoie la valeur -13.

getenv
Renvoie la valeur de la variable d'environnement fournie ou de la "variable de configuration".

ipAddressToName
Convertit une adresse IP en nom d'hôte. Cette fonction requiert un argument, à savoir une chaîne d'adresse IP en notation décimale avec point. Si l'adresse ne peut pas être résolue, alors l'adresse IP est renvoyée.

itoa
Convertit un entier en chaîne. Cette fonction est très utile lorsque vous voulez concaténer une valeur numérique dans une chaîne. La chaîne dérivée plus la fonction n'utilise que deux arguments de chaîne.

last
Renvoie une liste de valeurs à utiliser par les fonctions `min`, `max`, `average`, `stddev`, `rate` et `delta`. Elle admet deux arguments : l'attribut à collecter et le nombre de valeurs à utiliser dans le calcul. Si l'attribut requis est une valeur intégrale dans un attribut de chaîne, le premier argument peut contenir la fonction `atoi`, telle que `atoi(numericalStringAttribute)`. Le second argument doit être un nombre. Il peut être codé en dur sous la forme d'une constante ou peut être le résultat d'une expression `atoi(getenv("ENV_VAR"))`. Il ne peut pas référencer une valeur d'attribut.

Exemples de cette fonction utilisée :

```
average (last (Attr_A, 10))
```

```
last (Attribute_A, ${K01_NUM_COLLECTIONS}))
```

Restriction : Vous ne pouvez utiliser la fonction `last` qu'une seule fois dans une formule spécifique.

matches
Renvoie une valeur booléenne, à savoir true ou false, indiquant si une expression régulière correspond ou non à une valeur. Deux arguments sont pris en charge : une chaîne source et une

expression régulière dont le résultat de la chaîne est comparé. Cette fonction est utile pour filtrer des groupes d'attributs.

max
Renvoie une valeur unique correspondant à la valeur maximale d'un ensemble de valeurs. Ce dernier est issu des arguments de la fonction. Plusieurs valeurs individuelles peuvent être fournies (par exemple, des noms d'attribut ou des constantes), chacune dans un argument distinct. Par ailleurs, la dernière fonction peut être le seul argument de cette fonction (pour calculer la moyenne des valeurs les plus récentes d'un attribut).

min
Renvoie une valeur unique correspondant à la valeur minimale d'un ensemble de valeurs. Ce dernier est issu des arguments de la fonction. Plusieurs valeurs individuelles peuvent être fournies (par exemple, des noms d'attribut ou des constantes), chacune dans un argument distinct. Par ailleurs, la dernière fonction peut être le seul argument de cette fonction (pour calculer la moyenne des valeurs les plus récentes d'un attribut).

nameToIpAddress
Convertit un nom d'hôte en adresse IP. Cette fonction requiert un argument, une chaîne de nom d'hôte. Si l'adresse ne peut pas être résolue, le nom d'hôte est renvoyé.

NetWareTimeToTivoliTimestamp
Convertit une valeur temporelle Novell NetWare au format hexadécimal en horodatage Tivoli Monitoring. Cette fonction requiert un argument, à savoir une valeur temporelle hexadécimale spécifique à NetWare. L'attribut est de type horodatage.

taux
Taux de variation (par seconde) entre la valeur la plus récente d'un attribut et une valeur précédemment collectée du même attribut. L'argument unique du taux doit être la `dernière` fonction, laquelle extrait les valeurs en cours et antérieures d'un attribut. Une utilisation normale ressemble à :

```
rate (last(OtherAttribute, 2))
```

Pour plus d'informations sur les valeurs d'attribut issues de la dernière fonction qui sont utilisées pour calculer le débit, voir «Calculs des intervalles spécifiques», à la page 1230. Cette fonction est applicable uniquement pour les attributs dérivés, et non pour les filtres de groupes d'attributs.

replaceFirst
Remplace la première occurrence d'une sous-chaîne correspondant à une expression régulière par une chaîne de remplacement. Cette fonction utilise trois arguments. Premier argument : Chaîne d'entrée. Deuxième argument : Expression régulière utilisée pour trouver une sous-chaîne de la chaîne d'entrée. Troisième argument : Chaîne de remplacement. Voir («Expressions régulières ICU», à la page 1534) pour plus d'informations sur les expressions régulières et les valeurs de substitution autorisées dans la chaîne de remplacement.

replaceAll
Remplace toutes les occurrences des sous-chaînes correspondant à une expression régulière par une chaîne de remplacement. Cette fonction utilise trois arguments. Premier argument : Chaîne d'entrée. Deuxième argument : Expression régulière utilisée pour trouver une sous-chaîne de la chaîne d'entrée. Troisième argument : Chaîne de remplacement. Voir («Expressions régulières ICU», à la page 1534) pour plus d'informations sur les expressions régulières et les valeurs de substitution autorisées dans la chaîne de remplacement.

round
Arrondit la valeur au nombre entier le plus proche.

sqrt
Retourne la racine carrée d'un nombre

stddev
Renvoie une valeur unique correspondant à l'écart standard d'un ensemble de valeurs. Ce dernier est issu des arguments de la fonction. Plusieurs valeurs individuelles peuvent être fournies (par exemple, des noms d'attribut ou des constantes), chacune dans un argument distinct. Par ailleurs, la dernière

fonction peut être le seul argument de cette fonction (pour calculer la moyenne des valeurs les plus récentes d'un attribut).

StringToTivoliTimestamp

Convertit une chaîne de date et d'heure en horodatage Tivoli Monitoring. Cette fonction requiert deux arguments. Le premier argument est une représentation de chaîne à structure libre de l'horodatage. Le deuxième argument est une chaîne de format qui détermine comment analyser la représentation de chaîne à structure libre d'un horodatage. Le (Tableau 263, à la page 1245) décrit les paramètres de format valides. L'attribut est de type horodatage.

Tableau 263. Paramètres de format valides pour StringToTivoliTimestamp

Symbole	Signification	Format	Exemple
y	Année	yy yyyy	*96* *1996*
M	Mois **Remarque :** Seules les chaînes de mois en langue anglaise sont prises en charge.	M ou MM MMM MMMM	*09* *Sept* *September*
d	jour	d dd	*2* *02*
E	Jour de la semaine **Remarque :** Seules les chaînes de jour de la semaine en langue anglaise sont prises en charge.	EE EEE EEEE	*Sa* *Sam* *Samedi*
h	Heure sur une journée (0-23)	hh	*07*
H	Heure de la journée (0-23)	HH	*00*
m	Minute dans une heure	mm	*04*
s	Seconde dans une minute	ss	*05*
S	Milliseconde	S SS SSS	*2* *24* *245*
a	marqueur AM ou PM	a or aa	*am*

Tableau 263. Paramètres de format valides pour StringToTivoliTimestamp (suite)			
Symbole	**Signification**	**Format**	**Exemple**
Tout autre caractère ASCII	ignorer ce caractère	- (trait d'union) (espace) / (barre oblique) : (deux-points) * (astérisque) , (virgule)	

Le Tableau 264, à la page 1246 fournit des exemples de représentations de chaîne d'horodatage et de chaînes de format utilisées pour les analyser.

Tableau 264. Exemples de la fonction StringToTivoliTimestamp. Tableau répertoriant et expliquant quelques exemples de représentations de chaîne d'horodatage.	
Représentation de la chaîne d'horodatage	**Chaîne de format**
96.07.10 at 15:08:56	`yy.MM.dd ** HH:mm:ss`
Wed, August 10, 2010 12:08 pm	`EEE, MMMM dd, yyyy hh:mm a`
Thu 21/01/2010 14:10:33.17	`EEE dd/MM/yyyy HH:mm:ss.SS`

sum
Renvoie une valeur unique correspondant à la somme d'un ensemble de valeurs. Ce dernier est issu des arguments de la fonction. Plusieurs valeurs individuelles peuvent être fournies (par exemple, des noms d'attribut ou des constantes), chacune dans un argument distinct. Par ailleurs, la dernière fonction peut être le seul argument de cette fonction (pour calculer la moyenne des valeurs les plus récentes d'un attribut).

TivoliLogTimeToTivoliTimestamp
Convertit un horodatage de fichier journal Tivoli en horodatage Tivoli Monitoring. Cette fonction requiert un argument, à savoir la chaîne d'horodatage d'un fichier journal Tivoli. L'attribut est de type horodatage.

tokenize
Jeton d'une chaîne segmentée. Cette fonction requiert trois arguments. Le premier argument est une chaîne à fractionner en jetons. Le deuxième argument indique un ou plusieurs caractères de la chaîne qui sépare un jeton d'un autre. Toute occurrence de l'un des caractères de cet argument est utilisée pour identifier et séparer des jetons du premier argument. Le troisième argument correspond à l'indice du jeton à renvoyer comme résultat de cette fonction. Le premier jeton a pour indice 0, le deuxième pour indice 1, etc. Cet argument peut être également la chaîne LAST qui renvoie le dernier jeton.

UTCtoGMT
Convertit des valeurs au format GMT en horodatage Tivoli Monitoring. Cette fonction requiert un argument, à savoir la valeur entière time_t. L'attribut est de type horodatage.

UTCtoLocalTime
Convertit des valeurs au format UTC en horodatage Tivoli Monitoring. Cette fonction requiert un argument, à savoir la valeur entière time_t. L'attribut est de type horodatage.

Les fonctions suivantes ne prennent pas d'arguments et renvoient uniquement un nombre.

count
Présente un compteur qui démarre à 1 lorsqu'il est appelé pour la première fois, puis augmente par incréments de 1 à chaque appel ultérieur. Si vous l'utilisez dans une expression qui utilise également

`last`, il fait corresponde le nombre d'éléments stockés par `last()`, mais uniquement jusqu'à ce que `last()` atteigne sa valeur maximale. A ce stade, `last()` commence à supprimer la valeur la plus ancienne pour chaque nouvelle valeur, conservant ainsi le même nombre de valeurs totales, alors que `count()` continue d'augmenter indéfiniment.

cumulativeSum
Renvoie la somme des valeurs d'argument des événements en double représentés par un événement du récapitulatif du contrôle de flux. Ou renvoie l'argument s'il s'agit d'un événement unique d'une source de données. Elle utilise un argument numérique unique. Cette fonction ne s'applique qu'aux groupes d'attributs d'événements dont l'option de `filtrage et de récapitulatif des événements` est activée.

eventThreshold
Renvoie la valeur de seuil configurée pour le groupe d'attributs qui a généré l'événement. Un nombre, avec trois énumérations :

- `SEND_ALL (-3)`
- `SEND_FIRST (-2)`
- `SEND_NONE (-1)`

Le nombre entre parenthèses est la valeur brute mais Agent Builder définit les énumérations. Par défaut, la version textuelle est donc visible dans Tivoli Enterprise Portal ou dans la console IBM Cloud Application Performance Management. Si vous indiquez un seuil numérique réel sans utiliser l'une des options prédéfinies, ce nombre est renvoyé par cette fonction. La valeur est un entier > 0. Cette fonction ne s'applique qu'aux groupes d'attributs d'événements dont l'option de `filtrage et de récapitulatif des événements` est activée.

isSummaryEvent
Renvoie 0 s'il s'agit d'un événement unique de la source de données ou 1 si l'événement est un événement du récapitulatif du contrôle de flux. Les valeurs affichées sont Evénement ou Evénement du récapitulatif si vous utilisez l'attribut par défaut de la fonction. Si vous créez l'attribut manuellement, les valeurs affichées sont 0 et 1, sauf si vous définissez les noms en tant qu'énumération. Cette fonction ne s'applique qu'aux groupes d'attributs d'événements dont l'option de `filtrage et de récapitulatif des événements` est activée.

occurrenceCount
Le nombre d'événements concordants représentés par un événement du récapitulatif du contrôle de flux, ou 1 s'il s'agit d'un événement unique d'une source de données. (Un événement du récapitulatif du contrôle de flux inclut le premier événement). Cette fonction ne s'applique qu'aux groupes d'attributs d'événements dont l'option de `filtrage et de récapitulatif des événements` est activée.

summaryInterval
Renvoie l'intervalle de récapitulatif configuré pour le groupe d'attributs qui a généré l'événement, en secondes. Cette fonction ne s'applique qu'aux groupes d'attributs d'événements dont l'option de `filtrage et de récapitulatif des événements` est activée.

Exemples

Exemples d'utilisation d'opérateurs et de fonctions de formule pour créer des attributs dérivés et filtrés

Exemple 1 : Attributs dérivés

Si vous disposez d'une source de données qui définit le type d'attribut suivant :

Nom	Chaîne
xBytes	Numérique
yBytes	Numérique
Taille_virtuelle	Numérique

Vous pouvez définir :

- un attribut `totalBytes` qui doit être la somme de `xBytes` et de `yBytes`. Vous entrez la formule `xBytes + yBytes`.
- Un attribut `yPercent` qui doit être un pourcentage du total d'octets qui est `yBytes`, peut être défini sous la forme `yBytes % (xBytes + yBytes)` ou`yBytes % totalBytes`.

Exemple 2 : Attributs dérivés

Cette formule renvoie le maximum des valeurs récemment collectées pour l'attribut `Virtual_Size`. Le nombre d'échantillons collectés est la valeur de la variable de configuration, *K4P_COLLECTIONS_PER_HISTORY_INTERVAL* (accessible via `getenv`), convertie en nombre (via `atoi`) :

```
max(last(Taille_Virtuelle,atoi(getenv("K4P_COLLECTIONS_PER_HISTORY_INTERVAL"))))
```

Exemple 3 : Attributs dérivés

Cette formule renvoie la racine carrée de la somme des carrés des valeurs d'attribut `xBytes` et `yBytes` :

```
sqrt(xOctets * xOctets + yOctets * yOctets)
```

Exemple 4 : Attributs dérivés

Cette formule retourne la moyenne de l'attribut `xBytes`à partir des 20 échantillons les plus récents du groupe d'attributs. Si moins de 20 échantillons ont été collectés depuis le démarrage de l'agent, elle renvoie la moyenne de l'attribut `xBytes` de tous les échantillons:

```
average(last(xOctets,20))
```

Exemple 5 - Attributs filtrés

Vous disposez d'une source de données qui renvoie :

```
Name    Type  Size  Used  Free
Memory  MEM      8     4     4
Disk1   DISK   300   200   100
Disk2   DISK   500   100   400
```

Vous êtes uniquement intéressé par l'utilisation du disque dur. La solution consiste à créer un filtre pour limiter les données renvoyées. Pour limiter les données renvoyées, créez un filtre simple renvoyant une valeur booléenne, à savoir vrai ou faux, comme suit :

Filtre de disque :

```
Type=="DISK"
```

Maintenant, lorsque la condition du filtre `Type=="DISK"` est vraie, le groupe d'attributs renvoie les données d'utilisation du disque uniquement, par exemple :

```
Name    Type   Size  Used  Free
Disk1   DISK   300   200   100
Disk2   DISK   500   100   400
```

Exemple 6 - Attributs filtrés

Vous disposez d'une source de données qui renvoie :

```
Name   Size  Used  Free
Memory    8     4     4
Disk1   300   200   100
Disk2   500   100   400
```

Les données qui sont renvoyées sont similaires à celles de l'exemple précédent, à ceci près que dans ce cas, aucun attribut Type n'est présent. Ici, vous pouvez utiliser la fonction matches pour trouver des lignes de données avec une valeur d'attribut de nom qui correspond à `"Disque"` suivi d'un nombre.

Filtre de disque :

```
matches(Nom, "Disque[0-9]*")
```

Lorsque le filtre correspond à la chaîne `"Disque"` suivi d'un chiffre dans l'attribut `Nom`, seules les lignes de données d'utilisation des disques sont renvoyées:

```
Name   Size  Used  Free
Disk1   300   200   100
Disk2   500   100   400
```

Spécification des systèmes d'exploitation

Lorsque vous définissez des sources de données qui sont indisponibles sur certains des systèmes d'exploitation pris en charge par l'agent, vous devez spécifier les systèmes d'exploitation sur lesquels la source de données est exécutée.

Pourquoi et quand exécuter cette tâche

Par défaut, la source de données fournit des données sur tous les systèmes d'exploitation définis au niveau de l'agent, comme décrit dans «Systèmes d'exploitation par défaut», à la page 1208. Vous pouvez modifier les systèmes d'exploitation pour chaque source de données.

Procédure

1. Pour ouvrir la section Systèmes d'exploitation, cliquez sur **Systèmes d'exploitation** dans la page **Informations sur la source de données** lors de l'ajout d'une source de données.
2. Sélectionnez les systèmes d'exploitation sur lesquels la source de données doit s'exécuter.

   Sélectionnez des systèmes d'exploitation individuels, tous les systèmes d'exploitation, tous les systèmes d'exploitation d'un type particulier, ou les systèmes d'exploitation associés par défaut à l'agent.

Configuration et optimisation de la collecte de données

Lorsqu'un agent Agent Builder est créé, vous pouvez configurer et régler sa collecte de données pour obtenir les meilleurs résultats.

La procédure de configuration et de réglage de votre agent peut varier selon les agents Agent Builder, voire entre les groupes d'attributs d'un même agent. Les agents Agent Builder peuvent inclure les deux types de données et ils prennent en charge deux méthodes de base de collecte de données pour le type le plus courant de données.

Types de données

Un agent collecte deux types de données :

1. La plupart des groupes d'attributs Tivoli Monitoring représentent des instantanés de données. Les données demandées par un utilisateur sont extraites. Les agents utilisent ce type de données pour représenter les informations de configuration, les attributs de performances, le statut et les autres informations où un ensemble de données collectées simultanément est utile. Ces données sont appelées *données échantillonnées*.
2. Certaines données Tivoli Monitoring représentent des événements. Dans ce cas, un événement se produit et l'agent doit transférer les données à Tivoli Monitoring. Les alertes SNMP, les entrées du journal des événements Windows et les nouveaux enregistrements écrits dans un fichier journal sont des exemples d'événements. Pour des raisons de simplicité, ces types de données sont regroupés et appelés *données d'événement*.

Données échantillonnées

Lorsque des données échantillonnées sont requises, une demande de groupe d'attributs particulier est envoyée à l'agent. La requête peut être lancée en cliquant sur un espace de travail dans Tivoli Enterprise Portal. Elle peut également être lancée sur une situation en cours, sur une collecte de données pour l'entrepôt ou sur une requête SOAP. Lorsque l'agent reçoit la demande, il renvoie les données en cours concernant ce groupe d'attributs. Les demandes Tivoli Enterprise Portal ciblent un groupe d'attributs spécifique dans un nom de système géré en particulier. Les situations et les demandes d'historique sont plus intéressantes, notamment pour un agent comportant des sous-noeuds. Lorsqu'une situation nécessite des données sur un groupe d'attributs d'un sous-noeud, l'agent reçoit une demande unique avec une liste des sous-noeuds ciblés. L'agent doit répondre en renvoyant toutes les données sur le groupe d'attributs demandé pour tous les sous-noeuds avant que Tivoli Monitoring puisse traiter la demande suivante.

Pour un agent, la méthode la plus simple de répondre à une demande consiste à collecter des données à chaque demande de Tivoli Monitoring. Les agents Agent Builder ne collectent pas de données à chaque fois. Cette opération prend souvent un certain temps ou consomme des ressources et les mêmes données sont dans bien des cas demandées à de nombreuses reprises dans une période courte. Par exemple, un utilisateur peut définir plusieurs situations qui s'exécutent dans le même intervalle sur un groupe d'attributs ; les situations peuvent signaler plusieurs conditions différentes. Chaque situation se traduit par l'envoi d'une requête à l'agent, mais il se peut que vous préfériez cette solution pour afficher les mêmes données. Il est probable que les mêmes données apparaissent pour chaque situation. Ainsi, vous obtiendrez probablement des résultats plus homogènes et minimiserez la demande en ressources système de la part de l'agent de surveillance.

Le développeur d'agent peut configurer les agents de sorte à optimiser la collecte de données en choisissant d'exécuter la collecte dans l'un des deux modes suivants :

1. **Collecte à la demande** : l'agent collecte et renvoie les données lorsqu'il reçoit une demande.
2. **Collecte planifiée** : l'agent collecte les données en arrière-plan à des intervalles planifiés et renvoie les dernières données collectées lorsqu'il reçoit une demande.

L'agent utilise une mémoire cache à court terme dans ces deux modes. Si une autre requête de données est reçue alors que la mémoire cache est valide, l'agent renvoie des données à partir de la mémoire cache sans collecter de nouvelles données pour chaque demande. L'utilisation de données cache résout le problème généré par plusieurs situations simultanées et par d'autres types de demandes. Des variables d'environnement permettent de définir la durée de validité des données, l'intervalle de collecte planifiée, le nombre d'unités d'exécution utilisées pour la collecte et si l'agent s'exécute à la demande ou de manière planifiée. Ces variables d'environnement permettent d'optimiser le fonctionnement de chaque agent pour son environnement.

Consultez les exemples ci-après illustrant le fonctionnement de l'agent dans les deux modes :

- Agent 1 (collecte *à la demande*) : agent simple qui collecte une quantité relativement réduite de données généralement accessibles aux situations ou rarement dans Tivoli Enterprise Portal. La collecte de données est relativement rapide, mais peut utiliser les ressources informatiques et du réseau. Cet agent est normalement défini pour s'exécuter à la demande. Si aucune situation n'est en cours d'exécution ou que personne ne clique sur Tivoli Enterprise Portal, l'agent n'exécute aucune action. Les données requises sont collectées et renvoyées. Elles sont placées dans le cache à court terme, si bien que les demandes supplémentaires effectuées environ à la même heure renvoient les mêmes données. Ce type de collecte est probablement la manière la plus efficace d'exécuter cet agent, car il ne collecte des données que si elles sont demandées.
- Agent 2 (collecte *planifiée*) : agent complexe incluant des sous-noeuds et collectant des données de plusieurs copies de la ressource surveillée. Plusieurs copies de la ressource peuvent être gérées par un seul agent. Il est normal d'exécuter des situations sur les données assez fréquemment pour surveiller le statut et les performances de la ressource surveillée. Cet agent est défini pour exécuter une *collecte planifiée*. Cette collecte *planifiée* est due entre autres au mode d'évaluation des situations par les agents Tivoli Monitoring. Comme les situations se produisent sur les groupes d'attributs des sous-noeuds, l'agent reçoit une demande unique concernant les données de tous les sous-noeuds à la fois. Il ne peut pas répondre aux autres demandes jusqu'à ce que toutes les données sur une situation soient

renvoyées. Si l'agent collectait toutes les données dès l'arrivée de la demande, il se bloquerait à chaque clic sur un de ses espaces de travail dans Tivoli Enterprise Portal. Afin d'éviter tout blocage de l'agent, Agent Builder définit automatiquement tous les agents de sous-noeuds de manière à ce qu'ils exécutent une collecte planifiée. Le développeur d'agent ajuste le nombre d'unités d'exécution et la fréquence de régénération pour collecter les données à un intervalle raisonnable pour le type de données. Par exemple, l'intervalle d'actualisation peut être une fois par minute ou toutes les 5 minutes.

Variables d'environnement

Un agent détermine le mode à utiliser et la façon dont la collecte de données planifiée s'exécute en fonction des valeurs d'un ensemble de variables d'environnement. Ces variables d'environnement peuvent être réglées dans la définition de l'agent sur le panneau **Variables d'environnement**. Chaque variable d'environnement figure dans le menu avec les valeurs par défaut. Vous pouvez également définir ou modifier les variables d'environnement pour un agent installé en modifiant son fichier d'environnement (`env`) sous Windows ou d'initialisation (`ini`) sous UNIX. Les variables d'environnement qui contrôlent les collectes de données pour les groupes d'attributs échantillonnés sont les suivantes :

- `CDP_DP_CACHE_TTL=<période de validité pour les données mises en cache - valeur par défaut de 55 secondes>`
- `CDP_DP_THREAD_POOL_SIZE=<nombre d'unités d'exécution à utiliser pour la collecte simultanée - valeur par défaut égale à 15 pour les agents de sous-noeud>`
- `CDP_DP_REFRESH_INTERVAL=<nombre de secondes entre les collectes - la valeur par défaut est de 60 secondes pour les agents de sous-noeud>`
- `CDP_DP_IMPATIENT_COLLECTOR_TIMEOUT=< durée d'attente des nouvelles données après l'expiration de la période de validité - valeur par défaut : 5 secondes>`

Les variables les plus importantes sont `CDP_DP_CACHE_TTL, CDP_DP_REFRESH_INTERVAL` et `CDP_DP_THREAD_POOL_SIZE`.

Si `CDP_DP_THREAD_POOL_SIZE` a une valeur supérieure ou égale à 1 ou que l'agent inclut des sous-noeuds, l'agent exécute une collecte *planifiée*. Si la valeur `CDP_DP_THREAD_POOL_SIZE` n'est pas définie ou qu'elle est égale à 0, l'agent exécute une collecte *à la demande*.

Si l'agent s'exécute en mode *planifié*, il collecte automatiquement les données de tous les groupes d'attributs toutes les `CDP_DP_REFRESH_INTERVAL` secondes. Il utilise un ensemble d'unités d'exécution d'arrière-plan pour effectuer la collecte. Le nombre d'unités d'exécution est défini à l'aide de `CDP_DP_THREAD_POOL_SIZE`. La valeur correcte de `CDP_DP_THREAD_POOL_SIZE` varie en fonction de l'action de l'agent. Par exemple :

- Si l'agent collecte des données de systèmes distants via le protocole SNMP, il est préférable que `CDP_DP_THREAD_POOL_SIZE` soit identique au nombre de systèmes distants surveillés. Une taille de pool définie sur une valeur identique au nombre de systèmes distants surveillés permet à l'agent de collecter les données en parallèle, mais limite la charge simultanée sur ces systèmes. Les démons SNMP ont tendance à refuser les requêtes lorsqu'ils sont occupés. Ce processus met l'agent en mode de nouvelle tentative et la collecte des données finit par prendre davantage de temps et de ressources.
- Si l'agent inclut un certain nombre de groupes d'attributs dont la collecte prend un certain temps, utilisez une quantité suffisante d'unités d'exécution pour que les collectes de données longues puissent s'exécuter en parallèle, en prévoyant éventuellement quelques-unes de plus pour le reste des groupes d'attributs. Utilisez les unités d'exécution de cette manière si la ressource cible peut le gérer. Par exemple, la collecte des groupes d'attributs peut nécessiter beaucoup de temps si l'exécution du script ou une requête JDBC prend beaucoup de temps.

Si le pool d'unités d'exécution est plus volumineux, l'agent utilise plus de mémoire (principalement pour la pile allouée pour chaque unité d'exécution). Cependant, cette action n'entraîne pas d'augmentation notable de l'utilisation de l'unité centrale par le processus ou de la taille réelle de la partie active de ce dernier. L'agent est plus efficace lorsque la taille du pool d'unités d'exécution convient à la charge de travail. Cette taille peut être optimisée pour générer le comportement désiré d'un agent en particulier dans un environnement donné.

Les données collectées sont placées dans le cache interne. Ce cache permet de répondre à des demandes supplémentaires jusqu'à la collecte de nouvelles données. La période de validité de la mémoire cache est contrôlée par CDP_DP_CACHE_TTL. Par défaut, la période de validité est définie sur 55 secondes. Lorsqu'un agent s'exécute en mode planifié, il est préférable de définir la période de validité sur la valeur correspondant à CDP_DP_REFRESH_INTERVAL. Définissez-la légèrement supérieure si la collecte de données nécessite plus de temps. Lorsque vous définissez la période de validité de cette manière, les données sont considérées comme valides jusqu'à la prochaine collecte planifiée.

La dernière variable est CDP_DP_IMPATIENT_COLLECTOR_TIMEOUT. Elle n'est utilisée que lorsque CDP_DP_CACHE_TTL arrive à expiration avant la collecte de nouvelles données. Lorsque la mémoire cache expire avant la collecte de nouvelles données, l'agent planifie immédiatement une autre collecte de données. Il attend ensuite que cette collecte se termine au bout de CDP_DP_IMPATIENT_COLLECTOR_TIMEOUT secondes. Si la nouvelle collecte se termine, la mémoire cache est mise à jour et de nouvelles données sont renvoyées. Dans le cas contraire, les données existantes sont renvoyées. Pour éviter que ne se produise le même problème qu'avec Universal Agent, l'agent n'efface pas la mémoire cache à l'issue du traitement de CDP_DP_CACHE_TTL. En effet, Universal Agent efface toujours le cache de données lorsque la période de validité se termine. Si Universal Agent efface son cache de données avant la fin de la prochaine collecte, le cache est vide pour ce groupe d'attributs et ne renvoie aucune donnée avant que la collecte ne se termine. L'absence de données renvoyées pose problème en cas d'exécution de situations. Toute situation qui s'exécute entre l'effacement du cache et la fin de la collecte suivante n'identifie pas les données et les situations qui se déclenchent sont effacées. Par conséquent, d'innombrables événements se déclenchent et s'effacent tout simplement parce que la collecte de données est légèrement lente. Avec les agents Agent Builder, ce problème n'a pas lieu. Si les "anciennes" données entraînent le déclenchement d'une situation, les mêmes données ne modifient pas l'état de la situation. Une fois la collecte suivante terminée, la situation récupère les nouvelles données, puis se déclenche ou s'efface en fonction des données valides.

Groupes d'attributs

Les agents Agent Builder comprennent deux groupes d'attributs qui vous permettent de contrôler le fonctionnement de la collecte de données et d'optimiser l'agent pour votre environnement. Les groupes d'attributs s'appellent Statut de l'objet de performances et Statut du pool d'unités d'exécution. Lorsque ces groupes d'attributs sont utilisées pour optimiser la performance de la collecte de données, les données les plus utiles sont les suivantes :

- Attribut `Statut de l'objet de performance`, `Durée moyenne de la collecte`. Cet attribut affiche la durée nécessaire à chaque groupe d'attributs pour la collecte de données. Souvent, un faible pourcentage des groupes d'attributs représente la plus grande partie de l'utilisation de l'unité centrale ou du temps utilisé par l'agent. Vous pouvez peut-être optimiser la collecte pour un ou plusieurs de ces groupes d'attributs. Sinon, vous pouvez modifier l'intervalle de collecte pour un ou plusieurs d'entre eux si l'actualisation peut être moins fréquente que pour d'autres données. Pour plus d'informations, voir «Exemples et optimisation avancée», à la page 1254.
- Attribut `Statut de l'objet de performance`, `Intervalles ignorés`. Cet attribut indique le nombre de tentatives, par l'agent, de planification d'une nouvelle collecte pour le groupe d'attributs et a permis de détecter que la collecte précédente était toujours en attente ou en cours d'exécution. Dans un agent au comportement normal, cette valeur d'attribut est nulle pour tous les groupes d'attributs. Si ce nombre augmente, personnalisez la collecte de données. Pour ce faire, ajoutez des unités d'exécution, augmentez l'intervalle entre collectes ou optimisez la collecte.
- Attribut `Statut du pool d'unités d'exécution`, `Nombre moyen d'unités d'exécution actives du pool d'unités d'exécution`. Vous pouvez comparer cette valeur au groupe d'attributs Taille du pool d'unités d'exécution pour vérifier l'état d'utilisation de votre pool d'unités d'exécution. Ainsi, une taille de pool d'unités d'exécution réglée sur 100 unités aura pour effet de gaspiller la mémoire si 5 unités d'exécution s'exécutent en moyenne.
- Attributs `Statut du pool d'unités d'exécution, Délai d'attente moyen des travaux du pool d'unités d'exécution et Longueur de la file d'attente moyenne du pool d'unités d'exécution.` Ces attributs représentent le temps d'attente d'une collecte de données moyenne pour une unité d'exécution et le nombre moyen de collectes dans la file d'attente. En raison de la manière dont ces données sont collectées, un système même inactif indique une moyenne d'un

travail présent dans la file d'attente. Lorsqu'un plus grand nombre de travaux sont en attente ou que le temps moyen est plus longs, cela indique que des collectes sont réduites. Vous pouvez envisager d'ajouter des unités d'exécution, de rallonger l'intervalle entre deux collectes ou d'optimiser la collecte pour un ou plusieurs groupes d'attributs.

Données d'événement

Les agents Agent Builder peuvent exposer plusieurs types de données d'événement. Toutes les données d'événement possèdent des éléments de comportement en commun. L'agent reçoit chaque nouvel événement en tant que ligne séparée de données. Aussitôt reçues, les lignes de données sont immédiatement envoyées à Tivoli Monitoring pour traitement et ajoutées à un cache interne dans l'agent. Les situations sont générées et les collectes d'historique sont exécutées par Tivoli Monitoring dès réception de chaque ligne. Le cache permet de répondre aux demandes de données de Tivoli Enterprise Portal ou de requêtes SOAP et l'agent peut l'utiliser pour effectuer une détection, un filtrage et un récapitulatif en double s'il est défini pour le groupe d'attributs. La taille du cache d'événements est défini par `CDP_PURE_EVENT_CACHE_SIZE` pour chaque groupe d'attributs. Cette mémoire cache contient les événements `CDP_PURE_EVENT_CACHE_SIZE` les plus récents classés par ordre chronologique décroissant. Chaque groupe d'attributs d'événement possède une mémoire cache séparée. Lorsque la mémoire cache est saturée pour un groupe d'attributs, l'événement le plus ancien est supprimé de la liste.

L'agent Agent Builder peut afficher les événements pour les éléments suivants :

- Entrées du journal des événements Windows
- Alertes ou informations SNMP
- Enregistrements ajoutés aux fichiers journaux
- Notifications MBean JMX
- Contrôleurs JMX
- Evénements d'un fournisseur d'interface de programme d'application Java API ou de socket.
- Groupes d'attributs joints (où l'une des sources de données est une source de données d'événement)

Ces événements sont traités de la manière la plus appropriée pour chacune des sources. Les alertes/informations SNMP, les notifications JMX et les événements de fournisseurs Java API ou de sockets sont reçus de façon asynchrone et transférés immédiatement à Tivoli Monitoring. Il n'est pas nécessaire d'ajuster ces collecteurs. L'agent s'abonne pour recevoir les entrées du journal des événements Windows du système d'exploitation à l'aide de l'interface de programme d'application correspondante. Si l'agent utilise l'interface de programme d'application de consignation des événements plus ancienne, il recherche les nouveaux événements dans le système à l'aide des paramètres de pool d'unités d'exécution. Dans le cas des groupes d'attributs joints où l'une des sources de données est une source de données d'événement, aucun réglage n'est nécessaire pour ces groupes, bien que les ajustages appliqués au groupe de sources d'événements leur soient utiles.

La surveillance de fichier est plus complexe. L'agent doit surveiller l'existence des fichiers et le moment où de nouveaux enregistrements sont ajoutés aux fichiers. L'agent peut être configuré pour surveiller les fichiers à l'aide de modèles de nom de fichier ou d'un nom statique. Puisque l'ensemble de fichiers correspondant aux modèles peut changer avec le temps, l'agent recherche les fichiers nouveaux ou modifiés toutes les `KUMP_DP_FILE_SWITCH_CHECK_INTERVAL` secondes. Cette variable globale d'environnement régit la surveillance des fichiers dans une instance d'agent. Lorsque l'agent détermine les fichiers appropriés à surveiller, il doit déterminer leurs dates et heures de changement. Sous Windows, l'agent utilise les interfaces de programme d'application pour écouter ces changements. Il est informé dès que les fichiers sont mis à jour et les traite alors immédiatement. Sur les systèmes UNIX, l'agent recherche les changements de fichier toutes les `KUMP_DP_EVENT` secondes. Cette variable globale d'environnement régit la surveillance des fichiers dans une instance d'agent. Lorsqu'un agent remarque qu'un fichier a changé, il traite toutes les nouvelles données de ce fichier, puis attend le changement suivant.

Exemples et optimisation avancée

Exemple

Les variables d'environnement utilisées pour une optimisation plus avancée sont définies au niveau de l'agent. Il suffit de définir une fois les variables suivantes pour qu'elles s'appliquent à tous les groupes d'attribut de l'agent :

- CDP_DP_CACHE_TTL
- CDP_DP_IMPATIENT_COLLECTOR_TIMEOUT
- KUMP_DP_FILE_SWITCH_CHECK_INTERVAL
- KUMP_DP_EVENT

Vous pouvez choisir d'appliquer les variables suivantes à des groupes d'attributs pris séparément. Elles présentent encore toujours un paramètre global qui s'applique à tous les autres groupes d'attribut de l'agent :

- CDP_DP_REFRESH_INTERVAL
- CDP_PURE_EVENT_CACHE_SIZE

Si vous avez défini un agent pour inclure les six groupes d'attributs suivants :

- EventDataOne
- EventDataTwo
- EventDataThree
- SampledDataOne
- SampledDataTwo
- SampledDataThree

Vous pouvez définir les variables par défaut suivantes :

- CDP_DP_CACHE_TTL=55
- CDP_DP_IMPATIENT_COLLECTOR_TIMEOUT=2
- CDP_DP_REFRESH_INTERVAL=60
- CDP_PURE_EVENT_CACHE_SIZE=100

Par conséquent, tous les groupes d'attributs qui contiennent des données échantillonnées (SampledDataOne, SampledDataTwo et SampledDataThree) seront collectées toutes les 60 secondes. Chacun des groupes d'attributs d'événements (EventDataOne, EventDataTwo et EventDataThree) stockera les 100 derniers événements dans sa mémoire cache.

Ces paramètres peuvent fonctionner parfaitement ou certaines raisons peuvent vous contraindre à les contrôler de manière plus précise. Par exemple, que se passe-t-il si EventDataOne reçoit régulièrement 10 fois plus d'événements que EventDataTwo et EventDataThree ? Pour compliquer les choses davantage, nous dirons qu'il existe un lien entre EventDataOne et EventDataTwo. Lorsqu'un événement est reçu pour EventDataTwo, il existe toujours plusieurs événements pour EventDataOne et les utilisateurs doivent tous les corréler. Il n'y a pas un paramètre correct unique pour la taille du cache. Il est souhaitable que EventDataOne stocke plus d'événements et EventDataTwo moins d'événements. Pour cela, nous réglons CDP_PURE_EVENT_CACHE_SIZE sur la taille la plus adéquate pour la plupart des groupes d'attributs d'événements (100 semble être une bonne valeur). Ensuite, vous pouvez régler CDP_EVENTDATAONE_PURE_EVENT_CACHE_SIZE sur 1000. Ainsi, tous les événements correspondants sont visibles dans Tivoli Enterprise Portal.

La même opération peut être effectuée avec CDP_DP_REFRESH_INTERVAL. Définissez une valeur par défaut compatible avec le plus grand nombre de groupes d'attributs de l'agent, ensuite, définissez CDP_*nom groupe attributs*_REFRESH_INTERVAL pour les groupes d'attributs qui nécessitent une collecte différente. Pour optimiser la collecte, définissez la valeur par défaut CDP_DP_REFRESH_INTERVAL afin qu'elle corresponde à la valeur CDP_DP_CACHE_TTL .

CDP_DP_CACHE_TTL est une valeur globale. Par conséquent, si elle est définie sur une valeur inférieure à un intervalle d'actualisation, des collectes inattendues peuvent se produire.

Définition et test de sources de données

Agent Builder prend en charge plusieurs fournisseurs de données. Vous pouvez créer des sources de données à partir de chaque fournisseur de données. La procédure de création et test de sources de données est différente pour chaque fournisseur de données.

Pour la plupart des fournisseurs de données, lorsque vous créez une source de données, un ensemble de données (groupe d'attributs) est ajouté à l'agent. L'ensemble de données contient les informations qui sont recueillies par cette source de données.

Une source de données avec un fournisseur de données de processus, de service Windows ou de code retour de programme utilise l'ensemble de données spécial de disponibilité. Un seul ensemble de données de disponibilité peut être créé dans un agent. Il contient les informations recueillies par toutes les sources de données avec un fournisseur de données de processus, de service Windows ou de code retour de programme dans l'agent.

Toutes les sources de données de journal Windows d'un agent ou d'un sous-noeud placent les informations liées aux événements dans un ensemble de données de journal des événements.

Configuration d'une source de données pour Cloud APM

Dans Cloud APM, vous pouvez utiliser des données issues de tous les ensembles de données dans le tableau de bord Détails et pour définir des seuils à l'aide du gestionnaire de seuils. Si vous souhaitez utiliser les informations d'un ensemble de données dans le tableau de bord récapitulatif pour l'agent ou le sous-noeud, notamment l'indicateur de statut, ainsi que les informations de ressources (nom du service, adresse et port), l'ensemble de données doit générer une seule ligne.

Pour la plupart des fournisseurs de données, vous pouvez sélectionner **Génère une ligne de données unique** dans la configuration de jeu de données. Si les informations collectées doivent inclure plusieurs lignes, vous pouvez cliquer sur **Avancé** pour configurer un filtre qui garantit que la ligne correcte est générée (pour plus d'instructions, voir «Filtrage des groupes d'attributs», à la page 1237). Vous pouvez tester votre source de données de manière à vous assurer que les informations recueillies génèrent la ligne souhaitée.

Pour certains fournisseurs de données, l'ensemble de données doit générer plusieurs lignes. De plus, les sources de données de code retour de commande, de service Windows et de processus placent les données dans un ensemble de données Disponibilité unique, qui produit plusieurs lignes. Dans ce cas, vous devez créer un ensemble de données filtré qui produit une seule ligne. Pour obtenir des instructions sur la création d'un ensemble de données filtré (groupe d'attributs), voir «Création d'un groupe d'attributs filtré», à la page 1383.

D'autres fournisseurs de données produisent des données d'événement ; une ligne est incluse pour chaque nouvel événement. Ne les utilisez pas pour les informations de ressource ou de récapitulatif dans Cloud APM.

Les fournisseurs de données suivants doivent produire un ensemble de données incluant plusieurs lignes :

- Processus (utilise l'ensemble de données Disponibilité)
- Service Windows (utilise l'ensemble de données Disponibilité)
- Code retour de programme (utilise l'ensemble de données Disponibilité)
- Pour certains types de données, SNMP et JMX
- Selon l'application, socket et API Java

Les fournisseurs de données suivants produisent des données d'événement :

- Evénement SNMP

- Fichier journal
- Journal binaire AIX
- Journal des événements Windows
- Selon l'application, socket et API Java

L'un des attributs de l'ensemble de données doit produire une valeur de statut dont se servira Cloud APM pour l'indicateur de statut global. Si la ligne ne comprend aucun attribut pouvant être utilisé comme indicateur de statut, vous pouvez créer un attribut dérivé pour calculer le statut. Vous devez configurer les valeurs de gravité du statut ; pour obtenir des instructions, voir «Spécification de la gravité pour un attribut utilisé comme indicateur de statut», à la page 1236.

Surveillance d'un processus

Vous pouvez définir une source de données qui surveille un processus ou plusieurs processus qui s'exécutent sur un serveur. Les processus doivent s'exécuter sur le même hôte que l'agent. Pour chaque processus, la source de données ajoute une ligne à l'ensemble de données de disponibilité.

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, cliquez sur **Un processus** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **Un processus**.
3. Cliquez sur **Suivant**.
4. Sur la page **Contrôleur de processus**, dans la zone **Informations sur le processus**, fournissez le nom affiché et le nom de processus. Vous pouvez entrer le nom du processus manuellement ou l'obtenir en cliquant sur **Parcourir**. Vous pouvez aussi cliquer sur **Parcourir** pour afficher la liste des processus en cours d'exécution sur le système local ou sur un système distant.

   Vous pouvez également distinguer les processus en sélectionnant les options **Utiliser la correspondance d'argument** et **Correspondance complète de ligne de commande**. Par exemple, si plusieurs instances du même processus sont en cours d'exécution sur le système, une instance peut être distinguée d'une autre à l'aide de ces options.

*Tableau 265. Zones de la page **Contrôleur de processus**.* Tableau répertoriant les zones de la page **Contrôleur de processus** et leurs descriptions

Nom de la zone	Description	Valeurs admises
Nom affiché	Nom descriptif du composant de l'application implémenté par le processus tel qu'il est affiché dans Tivoli Enterprise Portal ou dans la console IBM Cloud Application Performance Management	Chaîne descriptive
Nom du processus	Nom du processus surveillé	Nom de fichier exécutable valide
Utiliser la correspondance d'arguments	Sélectionnez cette option si vous voulez un filtrage d'après les arguments du processus.	Activé ou Désactivé

*Tableau 265. Zones de la page **Contrôleur de processus**.* Tableau répertoriant les zones de la page **Contrôleur de processus** et leurs descriptions *(suite)*		
Nom de la zone	**Description**	**Valeurs admises**
Argument	Chaîne d'argument d'après laquelle établir la correspondance. La correspondance d'argument recherche la chaîne fournie en tant que sous-chaîne des arguments. La correspondance aboutira si vous fournissez n'importe quelle partie des arguments sous la forme de la chaîne en entrée.	Chaîne
Ligne de commande correspondance complète	Spécifiez le nom complet du fichier exécutable, qui peut aussi inclure le chemin	Activé ou Désactivé
Ligne de commande	Fait correspondre la chaîne fournie au nom de commande complet qualifié utilisé pour démarrer le processus. Les arguments de commande ne sont pas inclus. "Complet" signifie que le chemin d'accès de la commande doit être inclus.	Chaîne
Systèmes d'exploitation	Sélectionnez les systèmes d'exploitation sur lesquels vous voulez exécuter le processus	Toute sélection

5. Si vous cliquez sur **Parcourir**, la fenêtre **Afficheur de processus** s'affiche. Cette fenêtre contient, à l'origine, des informations détaillées sur chaque processus du système Agent Builder. Les informations inclut l'ID, le nom de processus et la ligne de commande complète du processus. Sélectionnez un ou plusieurs processus ou gérez la liste dans la fenêtre **Afficheur de processus** à l'aide d'une ou de plusieurs des actions suivantes :
   a) Pour trier la liste des processus, cliquez sur l'en-tête de colonne.
   b) Pour régénérer les informations dans la fenêtre, cliquez sur l'icône **Régénérer** (éclair).
   c) Pour rechercher des processus particuliers, cliquez sur l'icône **Rechercher** (jumelles).

      Vous pouvez entrer une phrase de recherche et sélectionner la section d'options pour effectuer une recherche par identificateur de processus, nom et ligne de commande.
   d) Pour afficher les processus d'un système différent, sélectionnez un système défini précédemment dans la liste **Nom de connexion**. Vous pouvez également cliquer sur **Ajouter** pour entrer les informations relatives au nouveau système.

      Pour plus d'informations, voir «Définition des connexions pour l'exploration des processus», à la page 1259. Vous pouvez charger en même temps des processus issus de plusieurs systèmes et passer d'une connexion à l'autre alors que les processus se chargent via une ou plusieurs connexions.

      Remarque : Lorsque vous explorez des systèmes distants, les détails de ligne de commande ne sont disponibles que si vous utilisez un Tivoli Enterprise Portal Server.

Dans l'exemple suivant, lorsque vous sélectionnez `svchost.exe`, il s'affiche dans la zone **Nom de processus** de la page **Contrôleur de processus** (Figure 31, à la page 1258).

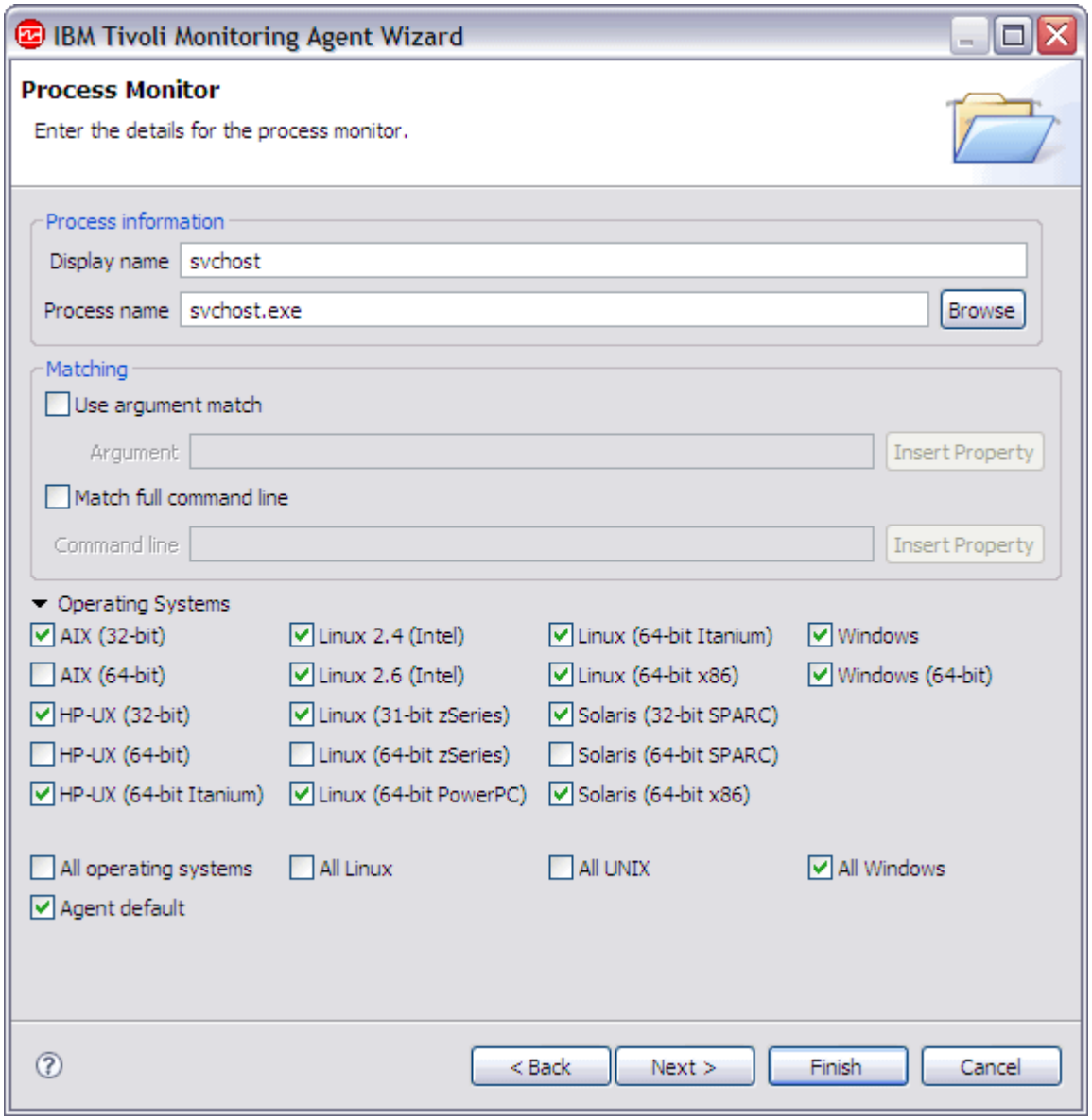


Figure 31. Exemple de page Contrôleur de processus

6. Complétez la page **Contrôleur de processus** à l'aide des informations figurant dans le (Tableau 265, à la page 1256).

   Remarque : Si le processus que vous avez décrit dans ce contrôleur n'est applicable qu'à certains des systèmes d'exploitation sur lesquels votre application s'exécute, vous pouvez vouloir créer un ou plusieurs contrôleurs de processus supplémentaires avec le même nom d'affichage pour couvrir les autres systèmes d'exploitation. Ajoutez les moniteurs de processus un par un. Veillez à ce que le nom d'affichage soit le même pour chaque contrôleur, et que le nom du processus existe sur les systèmes d'exploitation vérifiés.

7. Effectuez l'une des opérations suivantes :

   - Si vous utilisez l'assistant d'**agent**, cliquez sur **Suivant**.
   - Cliquez sur **Terminer** pour sauvegarder la source de données et ouvrir l'éditeur d'agent.

Que faire ensuite

Si vous souhaitez utiliser les données issues de cette source de données dans le tableau de bord récapitulatif pour IBM Cloud Application Performance Management, vous devez créer un ensemble de données filtré (un groupe d'attributs) basé sur l'ensemble de données Disponibilité et le configurer comme fournissant une ligne unique. Sélectionnez la ligne pour votre processus à l'aide de la zone NAME.

Vous pouvez utiliser la zone Statut pour connaître le statut ; DOWN signifie que le processus n'est pas en cours d'exécution, tandis que UP signifie qu'il l'est. Dans le nouveau groupe d'attributs filtré, sélectionnez la zone Statut et indiquez les valeurs de gravité associées.

Si plusieurs copies du processus sont en cours d'exécution, plusieurs lignes ayant ce nom de processus sont présentes dans l'ensemble de données Disponibilité et l'ensemble d'entre elles incluent le statut UP. Votre ensemble de données filtré doit être configuré pour renvoyer une seule ligne. Ainsi, n'importe laquelle de ces lignes peut être renvoyée mais la valeur Statut est valide dans tous les cas.

Pour des instructions, voir :

- «Création d'un groupe d'attributs filtré», à la page 1383
- «Spécification de la gravité pour un attribut utilisé comme indicateur de statut», à la page 1236
- «Préparation de l'agent pour Cloud APM», à la page 1417

Définition des connexions pour l'exploration des processus
Lorsque vous définissez une source de données de processus, vous pouvez visualiser et sélectionner les processus d'autres systèmes. Toutefois, lorsque l'agent s'exécute, il surveille les processus qui s'exécutent sur le même système que l'agent.

Pourquoi et quand exécuter cette tâche
Vous devez disposer de droits d'accès pour les autres systèmes ou ils doivent être surveillés par un agent de système d'exploitation Tivoli Monitoring.

Procédure

1. Pour définir une connexion, cliquez sur **Ajouter** dans la fenêtre **Afficheur de processus**.

   Vous pouvez sélectionner un type de connexion (Secure Shell (SSH), Windows ou système géré Tivoli Enterprise Portal Server), ou bien sélectionner une connexion existante à utiliser comme modèle.

   Pour ajouter une connexion de système géré, vous avez besoin du nom d'hôte Tivoli Enterprise Server, du nom d'utilisateur et du mot de passe Tivoli. Le nom du système géré de la connexion à distance est également nécessaire. Lorsqu'un système géré est sélectionné, la table affiche la liste des processus sur le système distant.

   Remarque : L'agent de système d'exploitation doit être en cours d'exécution sur le système que vous tentez d'explorer. L'agent doit également être connecté à un serveur Tivoli Enterprise Monitoring et un serveur Tivoli Enterprise Portal en cours d'exécution.

   Pour ajouter des connexions Secure Shell (SSH) ou Windows, vous avez besoin d'un nom d'hôte, d'un nom d'utilisateur et d'un mot de passe.
2. Lorsque vous ajoutez une connexion, vous pouvez la sélectionner dans la liste **Nom de connexion** de la fenêtre **Afficheur de processus**.

   Si toutes les zones requises pour créer la connexion n'ont pas été sauvegardées (par exemple, le mot de passe), la fenêtre **Propriétés de la connexion** correspondante s'ouvre. Entrez les informations manquantes. Pour les connexions de système géré Tivoli Enterprise Portal Server, vous devez vous connecter à Tivoli Enterprise Portal Server avant d'entrer un système géré.
3. Entrez vos nom d'utilisateur et mot de passe, puis cliquez sur l'icône **Régénérer** (éclair) pour vous connecter avant de sélectionner le système géré.

Que faire ensuite

Pour supprimer une connexion, sélectionnez-la et cliquez sur **Modifier** pour ouvrir la fenêtre **Propriétés de connexion**. Cochez la case **Supprimer cette connexion**, puis cliquez sur **OK**.

Surveillance d'un service Windows

Vous pouvez définir une source de données qui surveille un service ou plusieurs services qui s'exécutent sur un système Windows. Les services doivent s'exécuter sur le même hôte que l'agent. Pour chaque service, la source de données ajoute une ligne à l'ensemble de données de disponibilité.

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, cliquez sur **Un processus** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **Un service Windows**.
3. Cliquez sur **Suivant**.
4. Sur la page **Contrôleur de service**, dans la zone **Nom affiché**, entrez une description. Dans la zone **Nom de service**, entrez le nom de l'application de service. Vous pouvez l'entrer manuellement ou cliquer sur **Parcourir** pour afficher la liste des services en cours d'exécution sur le système local ou sur un système distant.

   Si vous cliquez sur **Parcourir**, la fenêtre **Afficheur de service** s'affiche. Cette fenêtre contient, à l'origine, des informations détaillées sur chaque service du système Agent Builder. Les informations incluent le nom, le nom d'affichage, l'état et la description du service.

   Remarque : Aucun service local n'est affiché lorsqu'Agent Builder ne s'exécute pas sur un système Windows. Un système Windows distant doit être défini ou sélectionné ; voir «Définition des connexions pour l'exploration des services», à la page 1261.

   Remarque : La description du service n'est pas disponible lorsque l'exploration se fait via Tivoli Enterprise Portal Server ou à partir d'un système UNIX ou Linux.
5. Sélectionnez un ou plusieurs services ou exécutez une ou plusieurs des opérations suivantes pour gérer la liste dans la fenêtre **Afficheur de services** :
   - Pour trier la liste des services, cliquez sur l'en-tête de colonne.
   - Pour régénérer les informations dans la fenêtre, cliquez sur l'icône **Régénérer** (éclair).
   - Pour rechercher un service, cliquez sur l'icône **Recherche** (jumelles) pour afficher la fenêtre **Recherche de service**. Vous pouvez effectuer une recherche par nom de service, nom d'affichage et description.
   - Pour afficher les services d'un système différent, sélectionnez un système défini précédemment dans la liste **Nom de connexion** ou cliquez sur **Ajouter** pour entrer les informations relatives au système. Pour plus d'informations, voir «Définition des connexions pour l'exploration des services», à la page 1261. Vous pouvez charger en même temps des services issus de plusieurs systèmes et passer d'une connexion à l'autre alors que les services se chargent via une ou plusieurs connexions.
6. Après avoir sélectionné ou saisi le nom du service, effectuez l'une des actions suivantes :
   - Si vous utilisez l'assistant d'**agent**, cliquez sur **Suivant**.
   - Cliquez sur **Terminer** pour sauvegarder la source de données et ouvrir l'éditeur d'agent.

Que faire ensuite

Si vous souhaitez utiliser les données issues de cette source de données dans le tableau de bord récapitulatif pour IBM Cloud Application Performance Management, vous devez créer un ensemble de données filtré (un groupe d'attributs) basé sur l'ensemble de données Disponibilité et le configurer comme fournissant une ligne unique. Sélectionnez la ligne pour votre processus à l'aide de la zone NAME.

Dans le nouveau groupe d'attributs filtré, sélectionnez la zone Functionality_Test_Status et indiquez les valeurs de gravité associées.

Pour des instructions, voir :

- «Création d'un groupe d'attributs filtré», à la page 1383
- «Spécification de la gravité pour un attribut utilisé comme indicateur de statut», à la page 1236

- «Préparation de l'agent pour Cloud APM», à la page 1417

Définition des connexions pour l'exploration des services
Vous pouvez sélectionner des services du système sur lequel Agent Builder s'exécute, mais également des services d'autres systèmes Windows.

Pourquoi et quand exécuter cette tâche

Pour sélectionner des services d'autres systèmes Windows, vous devez définir une connexion au système distant. Vous devez disposer de droits d'accès à ces systèmes, ou ceux-ci doivent être surveillés par un agent de système d'exploitation Tivoli Monitoring.

Procédure

1. Pour définir une connexion, cliquez sur **Ajouter** dans la fenêtre **Afficheur de service**.

   La fenêtre **Sélectionner un type de connexion** s'affiche. Pour ajouter une connexion de système géré, vous avez besoin du nom d'hôte Tivoli Enterprise Server, du nom d'utilisateur et du mot de passe Tivoli Monitoring ainsi que du nom du système géré. Lorsqu'un système géré est sélectionné, la table affiche la liste des services sur le système distant.

   Remarque : L'agent de système d'exploitation doit être en cours d'exécution sur le système que vous parcourez et être également connecté à un Tivoli Enterprise Monitoring Server et à un Tivoli Enterprise Portal Server en cours d'exécution.

   Pour ajouter une connexion Windows, vous avez besoin d'un nom d'hôte, d'un nom d'utilisateur et d'un mot de passe.
2. Sélectionnez un type de connexion (Windows ou le système géré Tivoli Enterprise Portal Server) ou sélectionnez une connexion existante à utiliser comme modèle.

   La fenêtre **Propriétés de la connexion** s'affiche.
3. Définissez les Propriétés de la connexion.
4. Cliquez sur **Terminer**
5. Lorsque vous ajoutez une connexion, vous pouvez la sélectionner dans la liste **Nom de connexion** de la fenêtre **Navigateur de service**.

   Si toutes les zones requises pour créer la connexion n'ont pas été sauvegardées (par exemple, le mot de passe), la fenêtre **Propriétés de la connexion** correspondante s'ouvre afin que vous puissiez entrer les données manquantes.

   a) Pour les connexions de système géré Tivoli Enterprise Portal Server, vous devez vous connecter à Tivoli Enterprise Portal Server avant d'entrer un système géré. Entrez vos nom d'utilisateur et mot de passe, puis cliquez sur l'icône **Régénérer** (éclair) pour vous connecter avant de sélectionner le système géré.
6. Pour supprimer une connexion, procédez comme suit :
   a) Sélectionnez la connexion dans la fenêtre **Navigateur de service**.
   b) Cliquez sur **Modifier** pour ouvrir la fenêtre **Propriétés de connexion**.
   c) Cochez la case **Supprimer cette connexion**.
   d) Cliquez sur **OK**.

Surveillance de données à partir de Windows Management Instrumentation (WMI)

Vous pouvez définir une source de données pour qu'elle collecte les données de Windows Management Instrumentation (WMI) sur le système sur lequel l'agent s'exécute ou sur un système distant. Une source de données surveille une classe WMI unique et place toutes les valeurs de cette classe dans l'ensemble de données qu'elle produit. Si la classe fournit plusieurs instances, l'ensemble de données comporte plusieurs lignes ; vous pouvez effectuer un filtrage par nom d'instance pour vous assurer que l'ensemble de données comporte une ligne uniquement.

Avant de commencer

Si votre agent collecte des données à partir d'un système distant à l'aide de Windows Management Instrumentation (WMI), il a besoin des droits d'accès aux données WMI sur le système distant. L'agent peut accéder aux données WMI sur un système distant si vous fournissez les données d'identification d'un compte doté des droits d'accès aux données WMI sur le système. Le compte Administrateur possède les droits requis. Dans la procédure suivante, vous pouvez soit utiliser les données d'identification Administrateur ou celles d'un autre utilisateur ayant les droits requis. Pour plus d'informations sur la création d'un compte utilisateur disposant de droits pour parcourir les données WMI, voir «Création d'un utilisateur avec les droits Windows Management Instrumentation (WMI)», à la page 1408.

Pour collecter des mesures via les API Windows, l'agent doit être hébergé sur un système d'exploitation Windows. L'administration des registres à distance doit être activée sur les systèmes distants.

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, cliquez sur **Données d'un serveur** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **WMI**.
3. Cliquez sur **Suivant**.
4. Sur la page **Informations sur Windows Management Instrumentation (WMI)**, effectuez l'une des opérations suivantes :
   - Entrez un nom pour l'espace de nom WMI et un nom pour la classe WMI dans les zones correspondantes. Passez ensuite à l'étape «9», à la page 1262
   - Cliquez sur **Parcourir** pour afficher toutes les classes WMI sur le système.

     Pour parcourir un système distant, sélectionnez un système dans la liste (s'il est défini). Vous pouvez également cliquer sur **Ajouter** pour ajouter le nom d'hôte d'un système Windows. Indiquez les données d'identification d'un compte utilisateur avec les droits nécessaires pour accéder aux données WMI sur un système distant ou bien celles d'un compte Administrateur pour le système distant. La page est mise à jour avec les informations du système distant. L'exploration est disponible uniquement si Agent Builder est en cours d'exécution sur un système Windows ; elle permet de parcourir des systèmes Windows uniquement.

5. Cliquez sur le signe plus (+) en regard d'une classe pour développer cette classe et afficher les attributs.
6. Dans la liste, sélectionnez la classe que vous voulez indiquer avec ses attributs associés, puis cliquez sur le bouton **OK**.

   Remarque : Vous pouvez cliquer sur l'icône **Rechercher** (jumelles) pour rechercher votre sélection dans la liste. Entrez une phrase dans la zone **Rechercher une phrase** ; indiquez votre préférence en cliquant sur l'une des zones **Rechercher par nom**, **Rechercher par description de classe** ou **Rechercher par propriétés de classe** et cliquez sur **OK**. Si vous trouvez l'élément que vous recherchez, sélectionnez-le et cliquez sur le bouton **OK**.

   La page **Informations WMI** de l'assistant s'affiche de nouveau et présente les informations de classe WMI sélectionnées.
7. Facultatif : Vous pouvez tester ce groupe d'attributs en cliquant sur **Tester**. Pour plus d'informations sur le test, voir «Test des groupes d'attributs WMI», à la page 1263.
8. Facultatif : Vous pouvez créer un filtre pour limiter les données renvoyées par ce groupe d'attributs en cliquant sur **Avancé**. Pour plus d'informations sur le filtrage de données à partir d'un groupe d'attributs, voir «Filtrage des groupes d'attributs», à la page 1237.
9. Cliquez sur **Suivant**.

   Remarque : Si vous avez tapé l'espace de nom WMI et le nom de classe WMI manuellement, la page **Informations d'attribut** s'affiche pour que vous puissiez compléter les informations d'attribut. Dans

cette même page, vous pouvez sélectionner **Ajouter des attributs supplémentaires** si vous le souhaitez. Cliquez sur **Terminer** pour valider les ajouts.

10. Sur la page **Sélectionner les attributs clés**, sélectionnez les attributs de clé ou indiquez que la source de données génère uniquement une ligne de données. Pour plus d'informations, voir «Sélection des attributs de clé», à la page 1206.
11. Effectuez l'une des opérations suivantes :
    - Si vous utilisez l'assistant d'**agent**, cliquez sur **Suivant**.
    - Cliquez sur **Terminer** pour sauvegarder la source de données et ouvrir l'éditeur d'agent.
12. Vous pouvez ajouter des attributs et fournir les informations correspondantes. Pour plus d'informations, voir «Création d'attributs», à la page 1229.

    Outre les zones applicables à toutes les sources de données (Tableau 261, à la page 1232), la page **Informations d'attribut** de la source de données WMI contient la zone suivante :

    Nom de mesure
    Nom de propriété de la classe que vous voulez collecter.
13. Si vous voulez définir des options globales pour la source de données, cliquez sur **Options globales**.

    Cochez la case **Include remote Windows configuration properties** si vous souhaitez inclure cette option, puis cliquez sur **OK**.

    Pour plus d'informations sur la configuration des connexions distantes Windows pour les sources de données Windows, voir («Configuration d'une connexion distante Windows», à la page 1407).

Test des groupes d'attributs WMI
Si vous exécutez Agent Builder sur un système Windows, vous pouvez tester un groupe d'attributs WMI dans Agent Builder.

Procédure

1. Vous pouvez démarrer la procédure de test de l'une des manières suivantes :
    - Lors de la création de l'agent, cliquez sur **Tester** sur la page **Informations WMI**.
    - Après la création de l'agent, sélectionnez un groupe d'attributs à la page **Définition de la source de données** de l'éditeur d'agent et cliquez sur **Tester**. Pour plus d'informations sur l'éditeur d'agent, voir «Utilisation de l'éditeur d'agent pour modifier l'agent», à la page 1207.

    Après avoir cliqué sur **Tester** dans l'une des deux étapes précédentes, la fenêtre de **test WMI** s'affiche.
2. Facultatif : Avant de démarrer le test, vous pouvez définir des variables d'environnement et des propriétés de configuration. Pour plus d'informations, voir «Test des groupes d'attributs», à la page 1420.
3. Cliquez sur l'option de **démarrage de l'agent**.

    Une fenêtre indique que l'agent est en cours de démarrage.
4. Pour simuler une demande de données d'agent provenant de l'environnement de surveillance, cliquez sur **Collecter des données**.

    L'agent interroge WMI pour accéder aux données. La fenêtre **Test WMI** collecte et affiche toutes les données du cache de l'agent depuis son dernier démarrage.
5. Facultatif : Cliquez sur **Vérifier les résultats** si les données renvoyées ne sont pas celles que vous attendez.

    La fenêtre **Statut de la collecte de données** affiche des informations supplémentaires sur les données. Les données collectées et affichées dans la fenêtre **Statut de la collecte de données** sont décrites dans «Noeud de statut d'objet de performances», à la page 1466.
6. Arrêtez l'agent en cliquant sur **Arrêter l'agent**.
7. Cliquez sur **OK** ou **Annuler** pour quitter la fenêtre **Test WMI**. Cliquez sur **OK** pour sauvegarder les modifications que vous avez apportées.

Concepts associés

«Test de votre agent dans Agent Builder», à la page 1420
Après avoir utilisé Agent Builder pour créer un agent, vous pouvez tester l'agent dans Agent Builder.

Surveillance d'un Windows Performance Monitor (Perfmon)

Vous pouvez définir une source de données pour qu'elle collecte les données d'un Windows Performance Monitor (Perfmon). Une source de données surveille un objet Perfmon. Les compteurs de l'objet sont placés dans des attributs dans l'ensemble de données obtenu. Si la classe fournit plusieurs instances, l'ensemble de données comporte plusieurs lignes ; vous pouvez effectuer un filtrage par nom d'instance pour vous assurer que l'ensemble de données comporte une ligne uniquement.

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, cliquez sur **Données d'un serveur** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **Perfmon**.
3. Cliquez sur **Suivant**.
4. Sur la page **Informations Perfmon**, effectuez l'une des actions suivantes :
   - Tapez le nom de l'objet dans la zone **Nom d'objet** et cliquez sur **Suivant** pour définir le premier attribut du groupe d'attributs.

     Remarque : Si vous entrez le nom de l'objet Windows Performance Monitor, vous devez entrer le nom anglais.
   - Cliquez sur **Parcourir** pour afficher la liste des objets du Perfmon.

     Lorsque la fenêtre de navigation d'objet du Analyseur de performances (Perfmon) s'ouvre pour la première fois, la fenêtre renseigne les informations à partir du système local. Pour accéder à un système distant, sélectionnez le système dans la liste (si une liste est définie) ou cliquez sur **Ajouter** pour ajouter le nom d'hôte d'un système Windows. Entrez un ID administrateur et un mot de passe. La fenêtre est mise à jour avec les informations du système distant. L'exploration est disponible uniquement si Agent Builder est en cours d'exécution sur un système Windows ; elle permet de parcourir des systèmes Windows uniquement. Par exemple, vous ne pouvez pas ajouter le nom d'hôte d'un système Linux ou Solaris pour effectuer une exploration à distance.
     - Lorsque vous cliquez sur un nom d'objet, les compteurs disponibles dans cet objet sont affichés dans la fenêtre.
       - Pour trier les objets ou compteurs du Windows Performance Monitor, cliquez sur l'en-tête de colonne.
       - Pour régénérer les informations dans la fenêtre, cliquez sur **Régénérer**.
       - Pour rechercher des objets ou compteurs particuliers, cliquez sur l'icône **Rechercher** (jumelles) pour ouvrir la fenêtre **Recherche dans l'Analyseur de performances**. Vous pouvez rechercher des noms d'objet, des noms de compteur ou les deux. La recherche met en correspondance des sous-chaînes et ne différencie pas les majuscules et les minuscules.
       - Sélectionnez un objet et cliquez sur **OK**.
       - La page **Informations Perfmon** s'affiche avec le nom de l'objet sélectionné dans la zone **Nom d'objet**.
   - Si vous voulez définir des options globales pour la source de données, cliquez sur **Options globales**

     Cochez la case **Include remote Windows configuration properties** si vous souhaitez inclure cette option, puis cliquez sur **OK**.

     Pour plus d'informations sur la configuration des connexions distantes Windows pour les sources de données Windows, voir («Configuration d'une connexion distante Windows», à la page 1407).

5. Si l'objet Windows Performance Monitor sélectionné renvoie plusieurs instances et que vous souhaitez filtrer les résultats en fonction du nom d'instance :
   a) Cochez la case **Filtrer par nom d'instance Perfmon** sur la page **Informations Perfmon**.
   b) Dans la zone **Nom d'instance Perfmon**, entrez le nom de l'instance à filtrer ou cliquez sur **Parcourir** pour afficher la liste des instances disponibles.
   c) Pour parcourir un système distant, sélectionnez-en un dans la liste ou cliquez sur **Ajouter** pour ajouter le nom d'hôte d'un système Windows. Après avoir sélectionné un système hôte, entrez un ID administrateur et un mot de passe. La table est mise à jour avec la liste des processus sur le système distant.

   Remarque : Vous pouvez également filtrer par groupe d'attributs, voir l'étape «9», à la page 1265
6. Si l'objet Windows Performance Monitor sélectionné renvoie plusieurs instances et que vous souhaitez que le nom d'instance soit renvoyé, sélectionnez **Renvoyer le nom d'instance** sur la page **Informations Perfmon**.

   Le fait de cocher cette option ajoute un attribut supplémentaire à la source de données qui ne figure pas dans la liste des attributs. Cet attribut contient le nom d'instance.

   Remarque : Si vous avez parcouru l'objet sélectionné et que cet objet est défini comme ayant plusieurs instances, cette case est automatiquement cochée.
7. Si vous n'avez pas coché l'option permettant de renvoyer le nom d'instance, la page Sélectionner les attributs clés s'affiche. Sur cette page, sélectionnez des attributs de clé ou indiquez que cette source de données ne génère qu'une seule ligne de données. Pour plus d'informations, voir «Sélection des attributs de clé», à la page 1206.
8. Facultatif : Vous pouvez tester ce groupe d'attributs en cliquant sur **Tester**. Pour plus d'informations sur le test, voir «Test des groupes d'attributs Perfmon», à la page 1266.
9. Facultatif : Vous pouvez créer un filtre pour limiter les données renvoyées par ce groupe d'attributs en cliquant sur **Avancé**.

   Pour plus d'informations sur le filtrage des données à partir d'un groupe d'attributs, voir l'étape «Filtrage des groupes d'attributs», à la page 1237.

   Remarque : Vous pouvez également effectuer un filtrage par nom d'instance (voir l'étape «5», à la page 1265).
10. Effectuez l'une des opérations suivantes :
    - Si vous utilisez l'assistant de création d'agent, cliquez sur **Suivant**.
    - Cliquez sur **Terminer** pour sauvegarder la source de données et ouvrir l'éditeur d'agent.

      La page **Définition de la source de données** de l'**éditeur d'agent** affiche une liste contenant l'objet et des informations relatives à l'objet.
11. Vous pouvez ajouter des attributs et fournir les informations correspondantes. Pour plus d'informations, voir «Création d'attributs», à la page 1229.

    Outre les zones applicables à toutes les sources de données, la page **Informations d'attribut Perfmon** de la source de données contient la zone suivante :

    Nom de mesure
    Nom du compteur de l'objet spécifique.

Que faire ensuite

Pour plus d'informations sur la configuration des connexions distantes Windows pour les sources de données Perfmon, voir («Configuration d'une connexion distante Windows», à la page 1407).

Test des groupes d'attributs Perfmon

Si vous exécutez Agent Builder sur un système Windows, vous pouvez tester le groupe d'attributs Perfmon que vous avez créé.

Procédure

1. Vous pouvez démarrer la procédure de test de l'une des manières suivantes :
   - Lors de la création de l'agent, cliquez sur **Tester** à la page **Informations Perfmon**.
   - Après la création de l'agent, sélectionnez un groupe d'attributs à la page **Définition de la source de données** de l'éditeur d'agent et cliquez sur **Tester**. Pour plus d'informations sur l'éditeur d'agent, voir «Utilisation de l'éditeur d'agent pour modifier l'agent», à la page 1207.

   Après avoir cliqué sur **Tester** dans l'une des deux étapes précédentes, la fenêtre **Test Perfmon** s'affiche.
2. Facultatif : Avant de démarrer le test, vous pouvez définir des variables d'environnement et des propriétés de configuration. Pour plus d'informations, voir «Test des groupes d'attributs», à la page 1420.
3. Cliquez sur l'option de **démarrage de l'agent**. Une fenêtre indique que l'agent est en cours de démarrage.
4. Pour simuler une demande de données d'agent provenant de l'environnement de surveillance, cliquez sur **Collecter des données**.

   L'agent demande les données à l'Analyseur de performances. La fenêtre **Test Perfmon** collecte et affiche toutes les données du cache de l'agent depuis son dernier démarrage.

   Remarque : Il se peut que des données utiles associées à certains attributs ne s'affichent pas si vous ne cliquez pas une deuxième fois sur l'option de **collecte de données**. Cela est dû au fait que certains attributs Analyseur de performances renvoient des valeurs delta et que le calcul d'une valeur delta nécessite une valeur précédente.
5. Facultatif : Cliquez sur **Vérifier les résultats** si les données renvoyées ne sont pas celles que vous attendez.

   La fenêtre **Statut de la collecte de données** affiche des informations supplémentaires sur les données. Les données collectées et affichées dans la fenêtre **Statut de la collecte de données** sont décrites dans «Noeud de statut d'objet de performances», à la page 1466.
6. Arrêtez l'agent en cliquant sur **Arrêter l'agent**.
7. Cliquez sur **OK** ou **Annuler** pour quitter la fenêtre **Test Perfmon**. Cliquez sur **OK** pour sauvegarder les modifications que vous avez apportées.

Concepts associés

«Test de votre agent dans Agent Builder», à la page 1420
Après avoir utilisé Agent Builder pour créer un agent, vous pouvez tester l'agent dans Agent Builder.

Surveillance de données à partir d'un serveur SNMP (Simple Network Management Protocol)

Vous pouvez définir une source de données pour qu'elle surveille un serveur SNMP. Une source de données surveille toutes les données d'un ID objet SNMP unique et d'un hôte unique. Si vous sélectionnez un élément de l'arborescence d'enregistrement d'identificateur d'objet sous laquelle d'autres objets sont enregistrés, un ensemble de données est créé pour chaque ensemble distinct de valeurs de table ou scalaires. Si un objet renvoie des données scalaires, l'ensemble de données n'a qu'une seule ligne. Si l'objet renvoie des données de table, l'ensemble de données a plusieurs lignes.

Pourquoi et quand exécuter cette tâche

Les protocoles SNMP V1, V2C (il est à noter qu'il s'agit de V2C et non de V2 uniquement) et V3 sont pris en charge par les agents.

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, cliquez sur **Données d'un serveur** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **SNMP**.
3. Cliquez sur **Suivant**.
4. Sur la page Informations sur le protocole SNMP, entrez le nom d'affichage ou cliquez sur **Parcourir** pour afficher l'ensemble des objets sur le système.

   Après avoir défini la source de données, vous pouvez ajouter un attribut. Les ID objet de ces attributs dérivés peuvent être longs et difficiles à entrer correctement. L'option Parcourir est un moyen plus facile pour entrer le bon ID objet.

   Remarque : Le navigateur ne parcourt pas le système en direct, mais lit les définitions et les bases d'informations de gestion (MIB).

   Remarque : L'icône **Régénérer** permet d'effacer la version en mémoire des fichiers MIB analysés et d'effectuer une autre analyse syntaxique des fichiers dans le cache d'espace de travail. Le cache se trouve dans *workspace_directory*`\.metadata\.plugins\com.ibm.tivoli.monitoring.agentkit\mibs`

   Où :

   répertoire_espace_de_travail
   Identifie le répertoire d'espace de travail que vous avez spécifié lorsque vous avez exécuté pour la première fois Agent Builder (voir «Démarrage d'Agent Builder», à la page 1202).

   a) Si la base d'informations de gestion définissant l'objet souhaité n'est pas chargée, cliquez sur le bouton **Gérer les bases d'informations de gestion personnalisées** pour ouvrir la boîte de dialogue de même nom.

   b) Cliquez sur **Ajouter** pour rechercher dans l'arborescence le fichier MIB à ajouter. Pour supprimer du cache un fichier MIB, sélectionnez-le, puis cliquez sur **Supprimer**.

   c) Cliquez sur **OK** pour mettre le cache à jour.

   S'il existe des erreurs lorsque les MIB sont analysées, la boîte de dialogue Gérer les MIB personnalisées reste ouverte. Cette boîte de dialogue permet d'ajouter ou de supprimer des MIB pour éliminer les erreurs.

   Cliquez sur **Annuler** pour restaurer l'état du cache MIB qui existait avant l'ouverture de la boîte de dialogue.

   Agent Builder comprend un ensemble de bases d'informations de gestion :

   - `hostmib.mib`
   - `rfc1213.mib`
   - `rfc1243.mib`
   - `rfc1253.mib`
   - `rfc1271.mib`
   - `rfc1286.mib`
   - `rfc1289.mib`
   - `rfc1315.mib`
   - `rfc1316.mib`
   - `rfc1381.mib`
   - `rfc1382.mib`
   - `rfc1443.mib`
   - `rfc1461.mib`
   - `rfc1471.mib`

- rfc1493.mib
- rfc1512.mib
- rfc1513.mib
- rfc1516.mib
- rfc1525.mib
- rfc1573a.mib
- rfc1595.mib
- rfc1650.mib
- rfc1657.mib
- rfc1659.mib
- rfc1666.mib
- rfc1695.mib
- rfc1747.mib
- rfc1748.mib
- rfc1757.mib
- rfc1903.mib
- rfc1907.mib
- rfc2011.mib
- rfc2021.mib
- rfc2024.mib
- rfc2051.mib
- rfc2127.mib
- rfc2128.mib
- rfc2155.mib
- rfc2206.mib
- rfc2213.mib
- rfc2232.mib
- rfc2233.mib
- rfc2238.mib
- rfc2239.mib
- rfc2320.mib
- rfc3411.mib

Tous ces MIB sont des MIB standard définies par le groupe de travail IETF. Les MIB sont fournies parce qu'elles représentent des définitions courantes qui peuvent être utiles pour la surveillance. En outre, la plupart des MIB sont nécessaires pour que les MIB personnalisées puissent résoudre les symboles qu'elles importent.

d) Sélectionnez un objet dans la liste

Cliquez sur le signe Plus (+) à côté d'un objet pour développer et afficher les modèles.

e) Dans la liste, sélectionnez l'objet que vous voulez indiquer et cliquez sur **OK**.

La nouvelle source de données apparaît alors sur la page **Définition de la source de données**.

Remarque : Si vous sélectionnez un objet qui définit d'autres objets (des objets qui sont imbriqués dans le premier objet), tous ces objets sont transformés en sources de données. Si vous sélectionnez un objet de haut niveau, de nombreuses sources de données sont ajoutées.

5. Sur la page **Informations sur le protocole SNMP**, sélectionnez les systèmes d'exploitation.

6. Facultatif : Vous pouvez tester la ou les sources de données en cliquant sur **Tester** dans la page **Informations sur le protocole SNMP**.

   Pour plus d'informations sur le test, voir «Test des groupes d'attributs SNMP», à la page 1270.
7. Facultatif : Vous pouvez créer un filtre pour limiter les données renvoyées par ce groupe d'attributs en cliquant sur **Avancé**. Pour plus d'informations sur le filtrage de données à partir d'un groupe d'attributs, voir «Filtrage des groupes d'attributs», à la page 1237.
8. Cliquez sur **Suivant**.
9. Sur la page **Informations d'attribut**, indiquez les informations relatives à l'attribut.
10. Effectuez l'une des opérations suivantes :
    - Si vous utilisez l'assistant de création d'agent, cliquez sur **Suivant**.
    - Cliquez sur **Terminer** pour sauvegarder la source de données et ouvrir l'éditeur d'agent.
11. Pour plus d'informations sur l'ajout d'attributs et sur la saisie d'informations sur ces attributs, voir «Création d'attributs», à la page 1229.

    Outre les zones applicables à toutes les sources de données, la page **Informations d'attribut** de la source de données SNMP contient les zones suivantes :

    Nom de mesure
    Chaîne arbitraire

    Identificateur d'objet
    ID complet de l'objet enregistré, hors les valeurs d'index

Que faire ensuite

Utilisez la configuration d'exécution de l'agent pour définir l'hôte surveillé.

Pour permettre à Agent Builder de générer des types de données 64 bits et traiter la valeur maximale des propriétés de base d'informations de gestion non signées 32 bits, voir «Options d'analyse de base d'informations de gestion», à la page 1269.

Erreurs MIB SNMP

Traitement des erreurs dans les MIB SNMP.

Il n'est pas inhabituel de trouver des erreurs lors de l'ajout de MIB SNMP. Cliquez sur **Détails>>** dans la fenêtre d'erreur **Agent Builder** pour identifier l'erreur MIB.

Une des erreurs les plus courantes correspond aux définitions manquantes définies dans d'autres bases d'informations de gestion. Vous pouvez importer plusieurs bases d'informations de gestion (MIB) simultanément pour résoudre le problème ou ajouter des MIB par incréments tant que toutes les définitions manquantes ne sont pas résolues. Agent Builder peut utiliser les définitions résolues. Par conséquent, vous pouvez ignorer une erreur qui n'a d'incidence que sur une partie de la base d'informations de gestion que vous n'envisagez pas d'utiliser. L'ordre des bases d'informations de gestion n'est pas important, car elles sont toutes chargées, puis les références sont résolues.

Options d'analyse de base d'informations de gestion

Définir vos préférences d'analyse MIB SNMP

Procédure

1. Dans Agent Builder, sélectionnez **Fenêtre** > **Préférences** pour ouvrir la fenêtre **Préférences**.
2. Dans la sous-fenêtre de navigation, développez **IBM Agent Builder**.
3. Cliquez sur **Analyse de base d'informations de gestion** pour ouvrir la fenêtre **Analyse de base d'informations de gestion**.

   L'analyseur de base d'informations de gestion utilisé par Agent Builder utilise les règles grammaticales définies par ASN.1 pour analyser les bases d'informations de gestion. Certaines bases d'informations de gestion ne respectent pas correctement les règles grammaticales. L'analyseur syntaxique peut

assouplir certaines règles afin de tolérer les erreurs les plus courantes. L'assouplissement de ces règles vous permet d'analyser les bases d'informations de gestion non conformes.

Autoriser les types à commencer par des lettres minuscules
Autorise les types écrits dans les bases d'informations de gestion, par exemple, des valeurs.

Autoriser les nombres nommés numériques
Autorise les nombres commençant par des lettres majuscules.

Autoriser le trait de soulignement dans les noms de valeur
Autorise les caractères de soulignement.

Autoriser les valeurs à commencer par des lettres majuscules
Autorise les valeurs commençant par des lettres majuscules.

Ignorer les bases d'informations de gestion en double
Désactive l'avertissement concernant les modèles de base d'informations de gestion en double.

4. Facultatif : La sélection de l'option **Créer des attributs 64 bits pour les propriétés de base d'informations de gestion non signés 32 bits** permet à Agent Builder de générer des types de données 64 bits pour traiter la valeur maximale des propriétés de base d'informations de gestion non signées 32 bits. La sélection de cette option ne modifie pas les définitions des zones de l'agent. Vous devez accéder au fichier MIB pour créer des sources de données pour ces propriétés.
5. Une fois que vous avez fini de modifier les préférences, cliquez sur **OK**.

Test des groupes d'attributs SNMP

Vous pouvez tester le groupe d'attributs SNMP que vous avez créé dans Agent Builder.

Procédure

1. Vous pouvez démarrer la procédure de test de l'une des manières suivantes :
   - Lors de la création de l'agent, cliquez sur **Tester** sur la page **Informations sur le protocole SNMP**.

     Remarque :

     Si l'objet SNMP sélectionné contient plusieurs groupes d'attributs, vous devez sélectionner celui que vous voulez tester.
   - Après la création de l'agent, sélectionnez un groupe d'attributs à la page **Définition de la source de données** de l'**éditeur d'agent** et cliquez sur **Tester**. Pour plus d'informations sur l'éditeur d'agent, voir «Utilisation de l'éditeur d'agent pour modifier l'agent», à la page 1207.

   Lorsque vous cliquez sur **Tester** dans l'une des deux étapes précédentes, la fenêtre des paramètres de test SNMP s'ouvre.
2. Sélectionnez une connexion existante dans **Nom de connexion** ou cliquez sur **Ajouter** pour sélectionner un type de connexion. Vous pouvez également sélectionner une connexion existante à utiliser comme modèle, à l'aide de l'**Assistant de création d'une connexion**.
3. Après avoir sélectionné un type de connexion ou une connexion existante, cliquez sur **Suivant** pour compléter les propriétés de la connexion SNMP. Lorsque vous avez terminé, cliquez sur **Terminer** pour revenir à la fenêtre des paramètres de test SNMP.
4. Facultatif : Avant de démarrer le test, vous pouvez définir des variables d'environnement et des propriétés de configuration. Pour plus d'informations, voir «Test des groupes d'attributs», à la page 1420.
5. Cliquez sur l'option de **démarrage de l'agent**. Une fenêtre indique que l'agent est en cours de démarrage.
6. Pour simuler une demande de données d'agent provenant de Tivoli Enterprise Portal ou de SOAP, cliquez sur **Collecte de données**. L'agent interroge la connexion SNMP configurée à la recherche de données.
7. La fenêtre **Paramètres de test** collecte et affiche toutes les données du cache de l'agent depuis son dernier démarrage.
8. Facultatif : Cliquez sur **Vérifier les résultats** si les données renvoyées ne sont pas celles que vous attendez.

La fenêtre **Statut de la collecte de données** affiche des informations supplémentaires sur les données. Les données collectées et affichées dans la fenêtre **Statut de la collecte de données** sont décrites dans «Noeud de statut d'objet de performances», à la page 1466.

9. Arrêtez l'agent en cliquant sur **Arrêter l'agent**.
10. Cliquez sur **OK** ou sur **Annuler** pour quitter la fenêtre **Tester les paramètres**. Cliquez sur **OK** pour sauvegarder les modifications que vous avez apportées.

Concepts associés

«Test de votre agent dans Agent Builder», à la page 1420
Après avoir utilisé Agent Builder pour créer un agent, vous pouvez tester l'agent dans Agent Builder.

Surveillance d'événements à partir d'expéditeurs d'événements SNMP (Simple Network Management Protocol)

Vous pouvez définir une source de données pour qu'elle collecte les données des événements d'alerte et d'information SNMP. Vous devez définir le port dans la configuration d'exécution de l'agent et configurer les serveurs de sorte qu'ils envoient l'événement à l'hôte de l'agent sur ce port. Tous les événements surveillés sont placés sous forme de lignes dans un ensemble de données.

Pourquoi et quand exécuter cette tâche

Simple Network Management Protocol (SNMP) V1, V2C (notez que ce nom de version est V2C et non V2 uniquement) et V3 sont pris en charge par les agents. Les alertes SNMP et les informations peuvent être reçues et traitées par l'agent. Les données reçues par ce fournisseur sont transmises à l'environnement de surveillance en tant qu'événements.

Pour plus d'informations sur les groupes d'attributs relatifs aux événements SNMP, voir («Groupes d'attributs d'événements SNMP», à la page 1492).

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, cliquez sur **Données d'un serveur** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **Evénements SNMP**.
3. Cliquez sur **Suivant**.
4. Dans la fenêtre **Informations sur les événements SNMP**, effectuez l'une des étapes suivantes :
   - Cliquez sur **Tous les événements** pour créer un groupe d'attributs qui envoie un événement lors de la réception de tout événement SNMP.
   - Cliquez sur **Evénements génériques** pour créer un groupe d'attributs qui envoie un événement lors de la réception de tout événement SNMP générique correspondant à l'un des types d'événement générique sélectionnés.
   - Cliquez sur **Evénements personnalisés** pour créer un ou plusieurs groupes d'attributs qui envoient des événements pour les événements SNMP spécifiques à l'entreprise. Cliquez sur **Parcourir** pour sélectionner les événements à surveiller.

     Dans la fenêtre du **navigateur NIB (Management Information Base) SNMP (Simple Network Management Protocol)**, les événements dans le panneau de sélection sont hiérarchisés en fonction du module MIB dans lequel ils ont été définis. Développez un objet SNMP pour afficher les événements du module MIB. Dans la liste, cliquez sur l'objet à définir, puis cliquez sur **OK**.

     Cochez la case **Inclure les attributs qui présentent les informations définies dans le fichier de configuration d'alerte** si vous disposez d'un fichier de configuration des alertes contenant des données statiques relatives aux alertes. Pour plus d'informations sur le fichier de configuration des alertes SNMP, voir («Configuration des alertes SNMP», à la page 1548).

     Cochez la case **Inclure un attribut de données VarBind** si vous voulez inclure un attribut à toutes les données VarBind reçues dans l'unité de données de protocole (PDU) de l'alerte. Pour plus

d'informations sur cet attribut, voir la définition d'attribut («Groupes d'attributs d'événements SNMP», à la page 1492).

Remarque :

a. Le navigateur ne parcourt pas le système en direct ; il lit les définitions et les bases d'informations de gestion (MIB). La liste des fichiers MIB inclus avec Agent Builder est définie dans le «Surveillance de données à partir d'un serveur SNMP (Simple Network Management Protocol)», à la page 1266. Les fichiers MIB chargés par l'un ou l'autre des fournisseurs de données SNMP sont disponibles dans les deux.

b. Si vous sélectionnez un module MIB ou des événements individuels, tous les événements de ce module sont convertis en sources de données séparées. Un attribut est ajouté pour chacune des variables définies dans l'événement. Si vous souhaitez avoir tous les événements des modules sélectionnés ou toutes les alertes regroupés en une seule source d'événements, cochez la case **Collecter des événements du module dans un groupe d'attributs unique**. Si vous sélectionnez des interruptions individuelles et que **Collecter des événements dans un groupe d'attributs unique** est sélectionné, un seul attribut est ajouté pour chacune des variables définies dans chacun des événements (les variables en double sont ignorées). Si vous sélectionnez un module, les attributs de variable ne sont pas ajoutés.

c. Si vous voulez entrer votre propre filtre, utilisez la syntaxe suivante :

La valeur de l'élément "ID objet" est utilisée pour déterminer les alertes à traiter pour ce groupe d'attributs.

– **Correspondance d'alerte :** L'attribut ID objet de l'élément paramètres_événement_snmp_globaux_pour_groupe peut être une liste de jetons délimitée par des virgules. Un jeton seul a la syntaxe suivante :

```
[IDobjet_entreprise][-Type_spécifique]
```

– **Exemple :** "1.2.3.5.1.4,1.2.3.4.5.6.7.8.9-0" Le premier jeton correspond à une alerte avec un ID objet entreprise de 1.2.3.5.1.4. Le second jeton correspond à une alerte avec un ID entreprise de 1.2.3.4.5.6.7.8.9 et un type spécifique de 0. Etant donné que les jetons sont regroupés sous forme de liste au sein d'un groupe d'attributs, un événement reçu correspondant à l'un ou l'autre de ces jetons est traité par ce groupe d'attributs.

d. Chaque événement reçu est traité uniquement par le premier groupe d'attributs qui correspond à l'événement reçu. Les groupes d'attributs de sous-noeud sont traités en premier, puis les groupes d'attributs de base. Le développeur d'agent doit s'assurer que les groupes sont définis de manière à ce que les événements soient reçus dans le groupe d'attributs attendu.

5. Dans la fenêtre **Informations sur les événements SNMP**, cochez la case **Correspondance d'hôte de sous-noeud** pour faire correspondre des événements à des sous-noeuds. Si le groupe d'attributs d'événements SNMP fait partie d'un sous-noeud, vous pouvez cocher la case **Correspondance d'hôte de sous-noeud** pour définir si l'événement doit provenir de l'agent SNMP surveillé.

Par exemple : vous disposez d'un agent qui surveille les routeurs où chaque instance de sous-noeud correspond à un routeur spécifique. Vous développez un agent chargé de collecter des données à partir d'un routeur via le collecteur de données SNMP. Vous définissez également un groupe d'attributs pour recevoir des événements SNMP envoyés par ce routeur. Chaque instance de routeur contient les mêmes données définies pour le filtre d'événement. Par conséquent, vous devez disposer d'un mécanisme supplémentaire pour que les événements de votre routeur apparaissent dans le groupe d'attributs associé à ce dernier.

Lorsque l'option "Correspondance hôte/sous-noeud" est sélectionnée, l'événement envoyé par le routeur est comparé à l'hôte défini pour le collecteur de données SNMP. Si l'hôte utilisé par le collecteur de données SNMP est celui qui a envoyé l'événement reçu, l'instance de sous-noeud traite l'événement SNMP. Sinon, l'événement est transmis à l'instance de sous-noeud suivante. La comparaison d'adresse ne s'applique qu'aux sous-noeuds. Aucune correspondance d'adresse n'est recherchée par les groupes d'attributs d'événements SNMP dans l'agent de base. Pour que la correspondance d'adresse fonctionne, la définition du sous-noeud doit contenir au moins un groupe

d'attributs SNMP. L'hôte SNMP utilisé par le protocole SNMP pour cette instance de sous-noeud est l'hôte utilisé pour la correspondance.

Si la case **Correspondance d'hôte de sous-noeud** n'est pas cochée, vos instances de sous-noeud n'effectuent pas cette comparaison supplémentaire. Dans ce cas, vous devez permettre à l'utilisateur de configurer un filtre d'ID objet différent pour chaque sous-noeud. Sinon, il est inutile d'inclure des groupes d'attributs d'événements SNMP dans la définition de sous-noeud.

6. Dans la fenêtre **Informations sur les événements SNMP**, sélectionnez les systèmes d'exploitation.
7. Facultatif : Vous pouvez cliquer sur **Tester** dans la fenêtre **Informations sur les événements SNMP** pour démarrer et tester votre agent.

   Pour plus d'informations, voir «Test des groupes d'attributs d'événement SNMP», à la page 1275.
8. Facultatif :

   Dans la fenêtre **Informations sur les événements SNMP**, cliquez sur **Avancé** pour sélectionner les **Options de filtrage et de récapitulatif des événements**. Pour plus d'informations, voir «Filtrage et récapitulatif des événements», à la page 1449.

   a) Lorsque vous avez terminé de sélectionner les **Options de filtrage et de récapitulatif des événements**, revenez à la fenêtre **Informations sur les événements SNMP**. Si vous avez déjà sélectionné **Evénements personnalisés** dans cette fenêtre, cliquez sur **Suivant** pour sélectionner les attributs de clé. Dans le cas contraire, ignorez l'étape suivante.

   b) Sur la page de sélection des attributs de clé, cliquez sur un ou plusieurs attributs de clé pour le groupe d'attributs, ou cliquez sur **Génère une ligne de données unique**.
9. Si vous utilisez l'assistant de création d'agent, cliquez sur **Suivant** ou sur **Terminer** pour sauvegarder l'agent et ouvrir l'éditeur d'agent.
10.

Que faire ensuite

Pour plus d'informations sur l'ajout d'autres attributs, voir («Création d'attributs», à la page 1229).

Propriétés Configuration des événements SNMP

Des propriétés sont créées automatiquement lorsqu'un groupe d'attributs d'événements SNMP est ajouté à l'agent

Une fois qu'une source de données est ajoutée, la configuration apparaît sur la page **Informations de configuration de l'exécution** de l'éditeur d'agent. Par exemple, la Figure 32, à la page 1274 présente les sections de configuration et certaines propriétés de configuration qui sont automatiquement créées lorsqu'un groupe d'attributs d'événements SNMP est ajouté à l'agent.

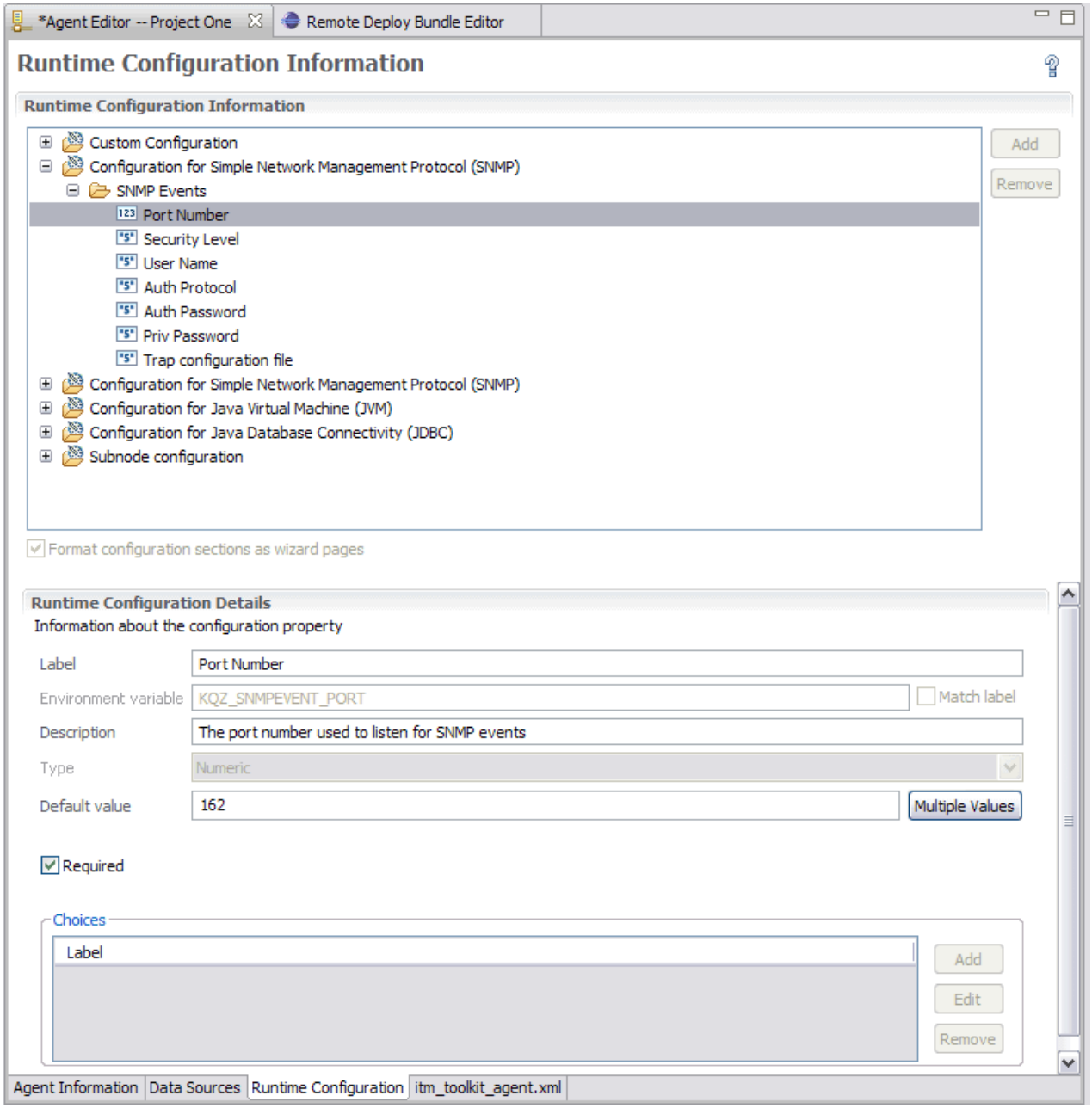


Figure 32. Page Configuration d'exécution

Les libellés, les descriptions et les valeurs par défaut des propriétés de configuration prédéfinies peuvent être modifiés, contrairement aux noms et types de variables. La section Configuration des événements SNMP contient les propriétés suivantes :

Tableau 266. Propriétés de configuration des événements SNMP

Nom	Valeurs admises	Obligatoire	Description
Numéro de port	Entier positif	Oui	Numéro de port requis utilisé pour l'écoute des événements
Niveau de sécurité	noAuthNoPriv, authNoPriv, authPriv	Non	Niveau de sécurité SNMP V3
Nom d'utilisateur	Chaîne	Non	Nom d'utilisateur SNMP V3

Tableau 266. Propriétés de configuration des événements SNMP (suite)			
Nom	**Valeurs admises**	**Obligatoire**	**Description**
Protocole d'authentification	MD5 ou SHA	Non	Protocole d'authentification SNMP V3
Mot de passe d'autorisation	Chaîne	Non	Mot de passe d'authentification SNMP V3
Mot de passe de confidentialité	Chaîne	Non	Mot de passe de confidentialité SNMP V3
Fichier de configuration des alertes	Nom de fichier qui contient le chemin	Non	Emplacement du fichier de configuration des alertes. Si le fichier ne peut pas être localisé à l'aide de cette propriété de configuration, une tentative est effectuée pour rechercher un fichier `trapcnfg` dans le répertoire bin de l'agent.

Aucune configuration n'est requise pour les événements V1 ou V2C. Tous les événements V1 ou V2C sont traités indépendamment de la source ou du nom de communauté spécifié. Le seul protocole de confidentialité pris en charge est DES, si bien qu'il n'y a aucune option pour définir le protocole de confidentialité. Les options de configuration SNMP V3 ne sont pas obligatoires (bien que chacune d'elles puisse être spécifiée de manière facultative). Si vous souhaitez les spécifier, indiquez les valeurs appropriées pour le niveau de sécurité sélectionné.

Test des groupes d'attributs d'événement SNMP
Vous pouvez tester le groupe d'attributs d'événements SNMP créé, dans Agent Builder.

Avant de commencer

Pour tester le groupe d'attributs d'événements SNMP, utilisez un programme de test ou une application pour générer des événements SNM.

Procédure

1. Vous pouvez démarrer la procédure de test de l'une des manières suivantes :
   - Lors de la création de l'agent, cliquez sur **Tester** dans la fenêtre **Informations sur les événements SNMP**.
   - Après la création de l'agent, sélectionnez un groupe d'attributs à la page **Définition de la source de données** de l'éditeur d'agent et cliquez sur **Tester**. Pour plus d'informations sur l'éditeur d'agent, voir «Utilisation de l'éditeur d'agent pour modifier l'agent», à la page 1207.

   Lorsque vous cliquez sur **Tester** dans l'une des deux étapes précédentes, la fenêtre **Test des paramètres d'événement** s'affiche.
2. Facultatif : Avant de démarrer le test, vous pouvez définir des variables d'environnement et des propriétés de configuration. Pour plus d'informations, voir «Test des groupes d'attributs», à la page 1420. Pour plus d'informations sur les propriétés de configuration SNMP, voir «Propriétés Configuration des événements SNMP», à la page 1273.
3. Cliquez sur l'option de **démarrage de l'agent**. Une fenêtre indique que l'agent est en cours de démarrage.

Lorsque l'agent démarre, il écoute les événements SNMP en fonction de sa configuration.

Remarque : L'agent qui démarre est une version simplifiée incluant le seul groupe d'attributs que vous testez.

4. Pour tester la collecte de données de l'agent, vous devez générer des événements SNMP correspondant à sa configuration. Vous pouvez effectuer cette opération à l'aide d'une application ou d'un générateur d'événements.

   Lorsque l'agent reçoit les événements SNMP correspondant à sa configuration, il les ajoute à son cache interne.

5. Pour simuler une demande de données d'agent provenant de l'environnement de surveillance, cliquez sur **Collecter des données**.

   La fenêtre **Paramètres d'événements de test** collecte et affiche toutes les données du cache de l'agent depuis son dernier démarrage. Un exemple de collecte de données est présenté à la Figure 33, à la page 1276.

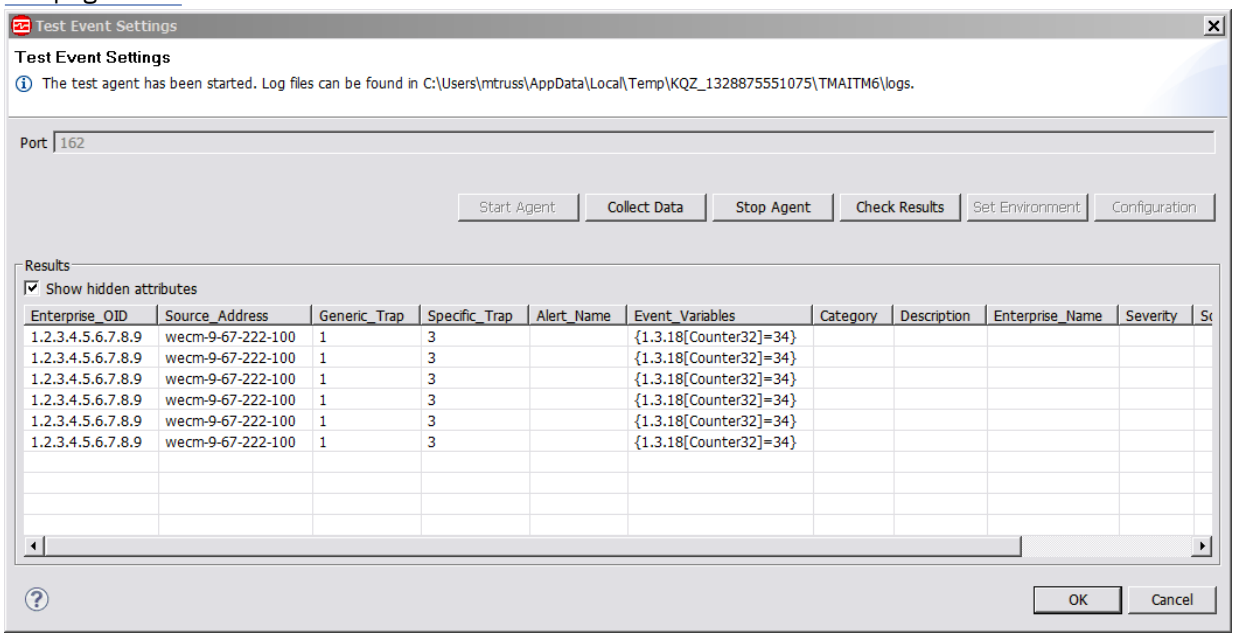


*Figure 33. Fenêtre **Test des paramètres d'événement** affichant des données d'événement SNMP collectées*

6. Facultatif : Cliquez sur **Vérifier les résultats** si les données renvoyées ne sont pas celles que vous attendez.

   La fenêtre **Statut de la collecte de données** affiche des informations supplémentaires sur les données. (Un exemple est présenté à la (Figure 34, à la page 1276.) Les données collectées et affichées dans la fenêtre **Statut de la collecte de données** sont décrites dans «Noeud de statut d'objet de performances», à la page 1466.

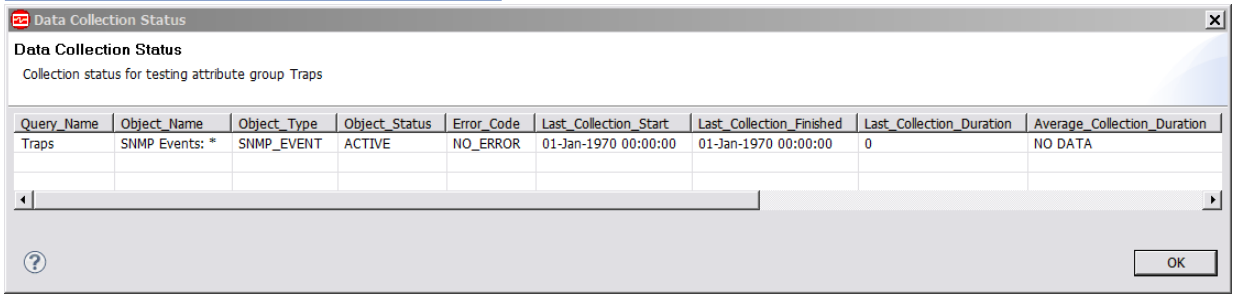


*Figure 34. Fenêtre **Statut de la collecte de données***

7. Arrêtez l'agent en cliquant sur **Arrêter l'agent**.
8. Cliquez sur **OK** ou sur **Annuler** pour quitter la fenêtre **Paramètres d'événements de test**. Cliquez sur **OK** pour sauvegarder les modifications que vous avez apportées.

Concepts associés

«Test de votre agent dans Agent Builder», à la page 1420
Après avoir utilisé Agent Builder pour créer un agent, vous pouvez tester l'agent dans Agent Builder.

Surveillance de beans gérés (MBeans) JMX (Java Management Extensions)

Vous pouvez définir une source de données pour qu'elle collecte les données des MBeans JMX. Les données de tous les MBeans surveillés sont placées dans un ensemble de données. Selon le MBean, l'ensemble de données peut générer une ou plusieurs lignes.

Pourquoi et quand exécuter cette tâche

Chaque source de données JMX définie doit identifier un MBean unique (instance unique) ou un certain type de MBean (plusieurs instances). Vous devez connaître le nom d'objet du MBean ou un modèle de nom d'objet pour un type de MBean contenant les données à collecter. Utilisez un nom d'objet uniquement pour identifier un ensemble de MBeans similaires. L'ensemble de MBeans correspondant au modèle doit fournir les données que vous voulez afficher dans la table de surveillance. Un modèle de nom d'objet standard se présente sous la forme de `*:j2eeType=Servlet,*`. Ce modèle de nom d'objet correspond à tous les MBeans dont le servlet est j2eeType. Vous pouvez vous attendre à ce que tous les MBeans correspondant à ce modèle comportent un ensemble similaire d'attributs et d'opérations exposés pouvant être ajoutés dans votre source de données. Une source de données utilisant ce modèle collecte des données de chaque MBean correspondant à ce modèle. Les attributs que vous définissez pour cette source de données doivent être disponibles pour tous les MBeans correspondant au modèle de nom d'objet de la source de données.

Java version 5 ou ultérieure n'est pas pris en charge.

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, cliquez sur **Données d'un serveur** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **JMX**.
3. Cliquez sur **Suivant**.
4. Sur la page **Informations JMX**, cliquez sur **Parcourir** pour afficher tous les MBeans JMX du serveur MBean.

   Après avoir défini la source de données, vous pouvez utiliser la fonction de navigation pour pré-remplir la liste d'attributs. Vous pouvez ensuite ajouter, supprimer ou modifier les attributs insérés par le navigateur. Les noms de ces attributs peuvent être longs et difficiles à entrer correctement. L'option Parcourir est un moyen plus facile pour entrer le nom correct.

   Remarque : Vous pouvez créer manuellement des sources de données JMX en indiquant un nom d'objet et en cliquant sur **Suivant** sans utiliser le navigateur. La création manuelle de sources de données JMX crée deux sources de données : Une source de données d'événement contenant des attributs prédéfinis pour les notifications JMX est créée. une source de données de collecte est définie avec un attribut que vous devez spécifier dans l'assistant.

   Modèle MBean
   Affiche le modèle de MBean.

   Options JMX globales
   Affiche le niveau de prise en charge.

   Les serveurs JMX suivants sont pris en charge :

   - Serveur MBean sur environnement d'exécution Java 5. La connexion est établie à l'aide du connecteur JSR-160. Les notifications et les contrôleurs sont pris en charge.
   - WebSphere Application Server, version 6 et ultérieure. Des connecteurs sont fournis pour les protocoles SOAP et RMI. Les contrôleurs JMX ne sont pas pris en charge dans la mesure où les MBeans ne peuvent pas être créés par un agent distant.

- WebSphere Community Edition et autres serveurs d'applications basés sur Apache Geronimo. La connexion est établie via des connecteurs JSR-160 standard. Les contrôleurs et les notifications JMX sont pris en charge dans les versions 1.1 et ultérieures.
- JBoss Application Server, version 4.0 et antérieure.
- JBoss Application Server, connexion JSR-160.
- WebLogic Server version 9 et ultérieure. Un connecteur est fourni pour le protocole T3.

5. Lors de la première exécution du navigateur JMX, aucun élément ne figure dans le menu déroulant du **serveur MBean**. Pour ajouter des connexions, cliquez sur le bouton **Ajouter**.

   Utilisez le bouton **Editer** pour modifier ou supprimer la connexion que vous avez déjà définie et sélectionnée dans le menu déroulant. Les définitions de connexion sont stockées dans l'espace de travail, de sorte que, lorsque vous créez une connexion, celle-ci soit retenue. Suivez les étapes ci-dessous pour créer une connexion. Si vous disposez déjà d'une connexion, allez à l'étape suivante.

   a) Pour créer une connexion à un serveur MBean, cliquez sur **Ajouter** pour ajouter une connexion ou pour modifier une connexion existante.

      La fenêtre **Navigateur JMX (Java Management Extensions)** s'affiche lorsqu'aucune connexion n'est définie.

   b) Une fois que vous avez cliqué sur **Ajouter** pour ajouter une connexion, la page **Sélectionner un type de connexion** s'ouvre.

   c) Utilisez l'assistant de connexion à un serveur de MBean pour vous connecter à un serveur de MBean. Les nouvelles connexions répertoriées peuvent être sélectionnées pour créer une connexion. Vous pouvez utiliser la liste des connexions existantes pour créer une connexion à l'aide d'une connexion existante comme modèle. Sélectionnez un des nouveaux types de connexion, puis cliquez sur **Suivant** pour démarrer la création d'une connexion.

   d) Après avoir sélectionné un type de connexion, vous pouvez être invité à sélectionner un type de connexion plus spécifique. Deux modèles basés sur le type de connexion **Connexions JMX standard (JSR-160)** sont présents. Sélectionnez le modèle le plus approprié pour votre serveur MBean, puis cliquez sur **Suivant**.

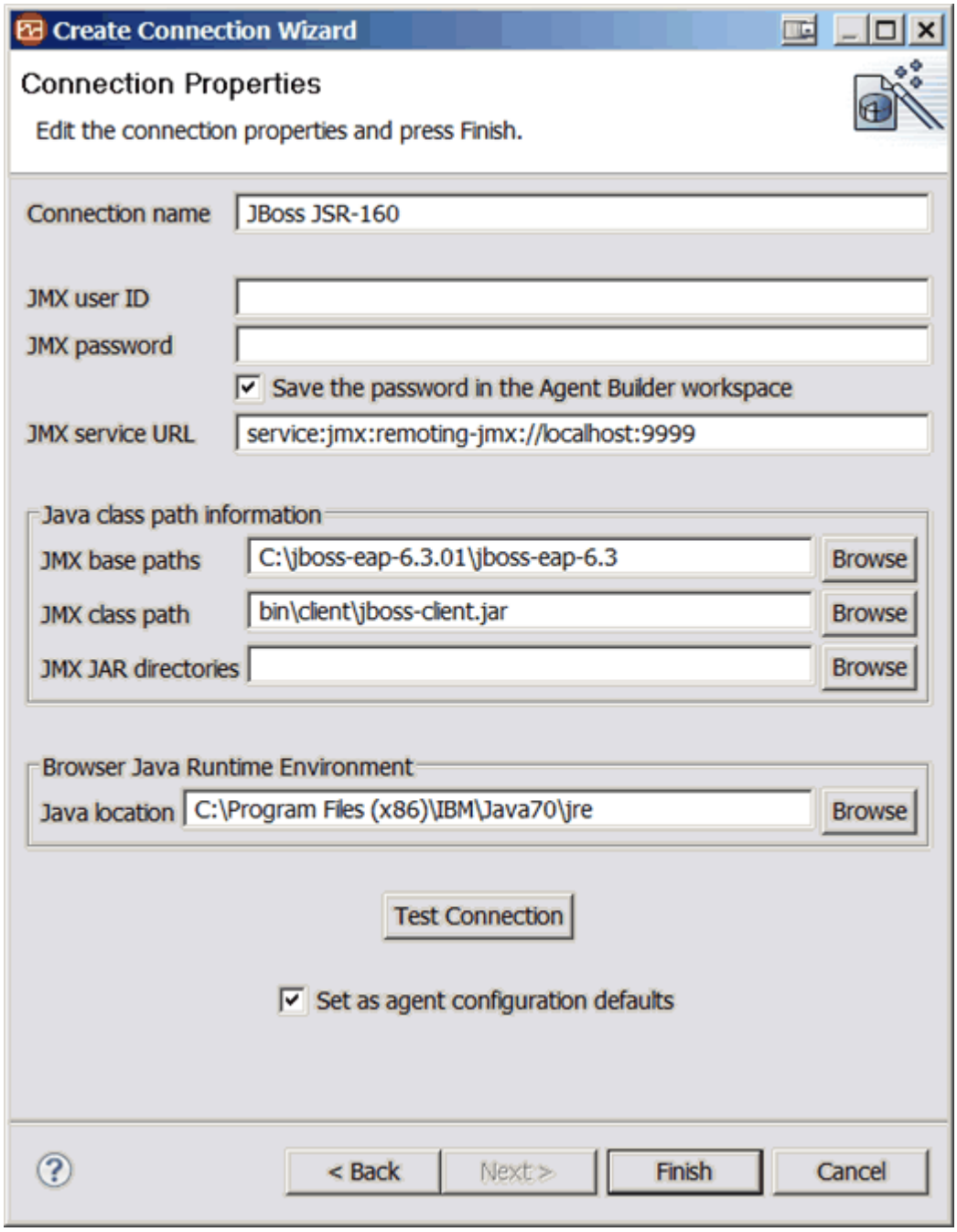


Figure 35. Propriétés de connexion JMX

La page **Propriétés de connexion** (Figure 35, à la page 1279) explique en détail comment établir une connexion à un serveur MBean. Vous devez y entrer les informations relatives au serveur MBean.

Important : Si votre source de données se connecte à un serveur WebSphere Application Server distant, assurez-vous que WebSphere Application Server est également installé sur l'hôte exécutant Agent Builder, puis associez le paramètre **Emplacement Java** à l'environnement d'exécution Java utilisé par le serveur WebSphere Application Server local.

e) Cochez la case **Sauvegarder le mot de passe dans l'espace de travail Agent Builder** si vous souhaitez sauvegarder le mot de passe pour cette connexion.

f) Facultatif : Sélectionnez **Définir comme valeurs par défaut de la configuration de l'agent** si vous voulez que les valeurs par défaut de JMX soient copiées à partir de ces propriétés.

Par exemple, dans la Figure 35, à la page 1279, le chemin de base JMX (**JMX base path**) par défaut est `C:\jboss-eap-6.3.01\jboss-eap-6.3`, l'URL de service JMX (**JMX service URL**) est `service:jmx:remoting-jmx://localhost:9999` et l'emplacement Java (**Java location**) est `C:\Program Files\IBM\Java70\jre`

1) Une fois que vous avez indiqué les propriétés requises pour la connexion, cliquez sur **Tester la connexion** pour vous assurer que la connexion peut être établie. Si la connexion n'aboutit pas, corrigez les propriétés nécessaires.
2) Lorsque la connexion aboutit, cliquez sur **Terminer** pour revenir dans le navigateur qui utilise la connexion que vous venez de configurer.

Les informations de chemin d'accès aux classes Java de la page **Propriétés de connexion** contiennent trois zones. Ces zones doivent être complétées le cas échéant pour vous connecter à un serveur de MBean qui nécessite des classes Java qui ne sont pas incluses dans l'environnement d'exécution Java. En général, le serveur de MBean auquel vous voulez vous connecter doit être installé sur le même système qu'Agent Builder. Dans ce cas, indiquez dans la zone **Chemins de base JMX** le répertoire dans lequel l'application contenant le serveur de MBean a été installée. La zone **Répertoires JAR JMX** contient alors la liste des répertoires relatifs au répertoire Chemins de base contenant les fichiers JAR requis pour la connexion au serveur de MBean. La zone de **Chemin de classes JMX** peut servir à inclure des fichiers JAR spécifiques. Les fichiers JAR répertoriés dans la zone **Répertoires JAR JMX** n'ont pas besoin d'être répertoriés séparément dans la zone **Chemin de classes JMX**.

N'importe laquelle des zones peut contenir plusieurs références ; il suffit de séparer les entrées à l'aide d'un point-virgule. Ces valeurs sont identiques à celles requises lors de la configuration de l'agent. Pour plus d'informations, voir «Configuration JMX», à la page 1285.

6. Une fois qu'une connexion a été sélectionnée, le navigateur JMX télécharge des informations relatives aux MBeans à partir du serveur JMX. Ces informations s'affichent dans les quatre zones suivantes de la fenêtre du **navigateur JMX** (Figure 36, à la page 1281) :

   Instructions pour les écrans à partir de la fenêtre de navigateur Java Management Extensions (JMX) jusqu'à l'onglet **Runtime Configuration** de l'éditeur d'agent : Sur la page **Informations JMX**, sélectionner **Parcourir**. Dans le navigateur (navigateur JMX sans connexion sélectionnée), sélectionnez **Ajouter**. Sur la page **Sélection de connexion JMX**, sélectionnez **JBoss** puis **Suivant**. Sur la page **Propriétés de connexion JMX**, personnalisez deux propriétés de connexion : le fournisseur JBoss URL: `jnp://wapwin3.tivlab.raleigh.ibm.com:1099/` et **Répertoires JAR JBoss** : Le chemin d'accès complet vers le répertoire qui contient les fichiers JAR suivants : `jbossall-client.jar`, `jboss-jmx.jar`, `jboss-jsr77-client.jar`, `jboss-management.jar`. Sélectionnez **Terminer**. Cette configuration vous permet de définir votre connexion JBoss afin d'obtenir des écrans similaires à ceux indiqués ici.

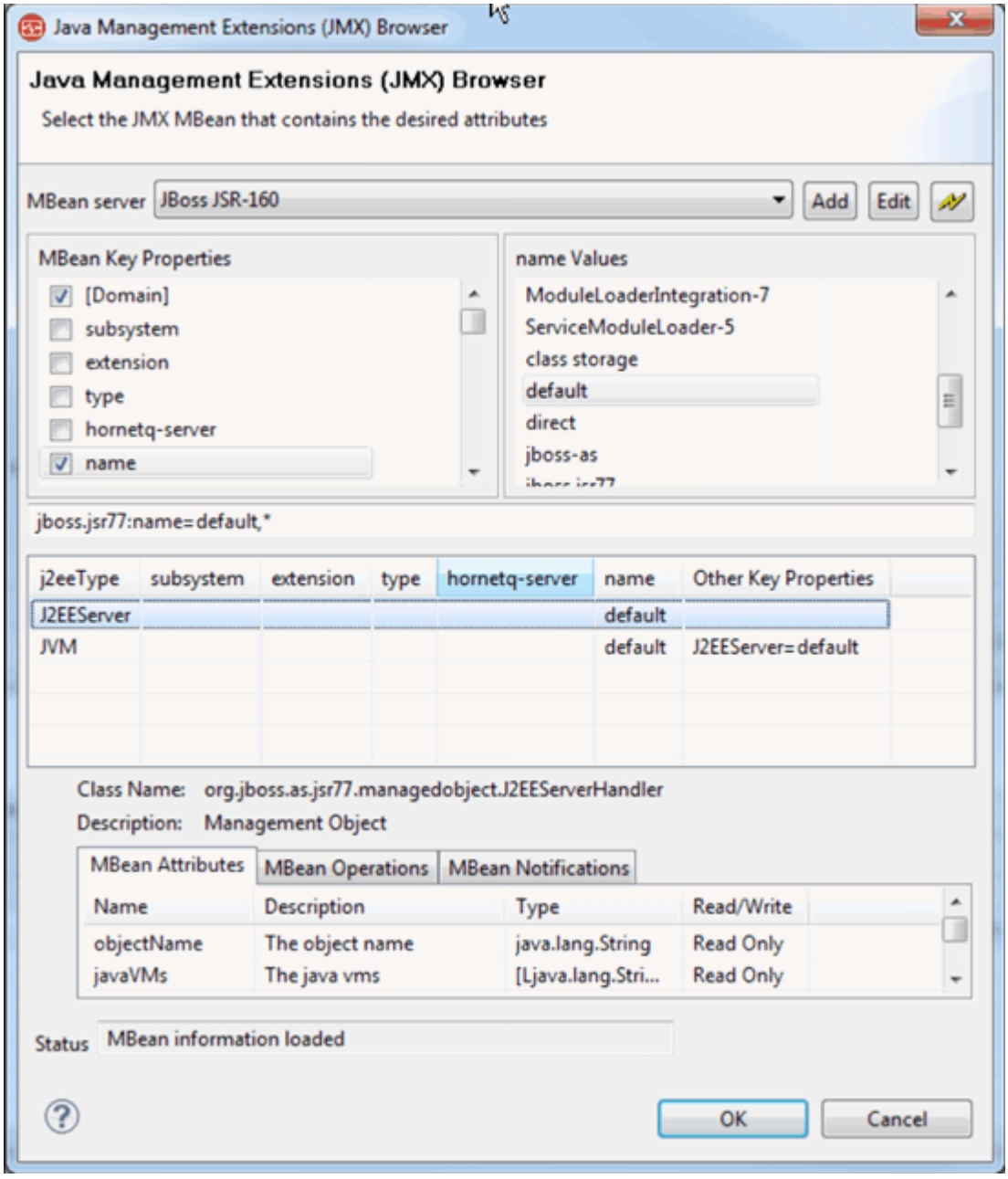


Figure 36. Fenêtre Navigateur JMX (Java Management Extensions)

- Zone **Propriétés de clé MBean** : cette zone contient chacune des clés de nom d'objet unique détectée à partir de tous les MBeans sur le serveur. L'entrée **[Domain]** est une entrée spéciale, car il ne s'agit pas réellement d'une clé. Cependant, l'entrée **[Domain]** est traitée sous la forme d'une clé implicite pour la valeur du domaine du MBean. Sélectionnez un élément dans cette liste pour rechercher les MBeans qui contiennent la propriété de clé. La liste des valeurs de la propriété clé figure dans la liste **Valeurs de propriété de clé sélectionnée**. Lorsqu'une propriété de clé est cochée, cela signifie qu'elle est incluse dans le modèle de nom d'objet de la source de données.
- Zone **Valeurs de propriété de clé sélectionnée** : cette zone affiche les valeurs de la propriété de clé de MBean sélectionnées depuis tous les MBeans. Le fait de sélectionner une de ces valeurs vérifie la propriété de clé de MBean. Cette sélection met également à jour le modèle de nom d'objet indiqué dans la zone de message contenant le nom et la valeur de la propriété de clé de MBean.
- Une table répertorie tous les MBeans correspondant au modèle de nom d'objet : lorsque vous sélectionnez des propriétés et des valeurs de clé dans les Propriétés de clé de MBean et les listes de valeurs de propriété de clé sélectionnée, la mise à jour du modèle de nom d'objet s'affiche, et la

liste des MBeans dans ce tableau change pour refléter la liste des MBeans qui correspondent au modèle sélectionné. Si vous disposez d'un modèle qui ne correspond à aucun MBean, vous pouvez désélectionner des entrées dans la liste des propriétés de clé de MBean. Vous pouvez effacer les entrées en cliquant sur la case à cocher en regard d'une clé qui est utilisée par votre modèle et en supprimant la coche. De même, vous pouvez modifier manuellement le modèle pour détecter les MBeans que vous recherchez. Le modèle *:* permet de sélectionner tous les MBeans.

Cette table permet de parcourir les MBeans à partir du serveur et de déterminer celui qui contient les données à surveiller. Pour parcourir un nombre potentiellement élevé de MBeans, vous pouvez procéder au tri par attribut de clé (à partir du menu ou en cliquant sur un en-tête de colonne). Vous pouvez également afficher n'importe quel attribut de clé dans n'importe quelle colonne en sélectionnant **Afficher une propriété de clé** dans le menu. Lorsque le tableau affiche une valeur de propriété de clé identifiant les MBeans à surveiller, cliquez à l'aide du bouton droit de la souris sur cette valeur, puis choisissez **Sélectionner uniquement les MBeans avec la propriété de clé** dans le menu.

- Un tableau contenant les détails d'un MBean sélectionné : le navigateur JMX affiche des informations relatives à un MBean unique. Pour visualiser les détails d'un MBean, sélectionnez le MBean dans le tableau contenant la liste des MBeans correspondant au filtre en cours. Les principales informations relatives au MBean sont la liste des attributs, opérations et notifications qu'il définit.

Pour créer une source de données à partir du navigateur JMX, utilisez les quatre panneaux décrits précédemment pour générer un modèle de nom d'objet. Générez le modèle de nom d'objet correspond à un ensemble de MBeans, chacun contenant les données de surveillance à collecter. Par exemple, pour surveiller des données à partir de tous les MBeans ThreadPool, procédez comme suit :

a) Sélectionnez **type** dans le panneau **Propriétés de clé MBean**. La sélection de **type** met à jour les **valeurs de propriétés de clé sélectionnée** pour répertorier toutes les valeurs uniques de la clé type de tous les MBeans.

b) Sélectionnez **ThreadPool** dans la liste des valeurs de la clé type. Après avoir sélectionné **ThreadPool**, le nom de propriété de clé type est coché dans le Panneau **Propriétés de clé de MBean** et le modèle de nom d'objet mis à jour devient *:type=ThreadPool,*. La liste des MBeans est également mise à jour de sorte que seuls les MBeans correspondant à ce modèle s'affichent.

c) Sélectionnez un des MBeans dans la liste des MBeans pour visualiser les attributs, les opérations et les notifications disponibles pour le MBean. Si la liste des MBeans contient un plus grand nombre de MBeans que vous ne voulez en surveiller, vous devez poursuivre cette procédure de sélection de propriétés et de valeurs de clé jusqu'à ce que vous ayez le modèle de nom d'objet identifiant l'ensemble des MBeans gérés à surveiller. Vous pouvez également afficher un menu dans la liste des MBeans pour mettre à jour le modèle d'objet à l'aide des valeurs de propriété de clé affichées dans le tableau.

7. Lorsque le modèle de nom d'objet est correct, sélectionnez un MBean dans la table.

   Tous les attributs du MBean sélectionné sont les attributs initiaux dans la nouvelle source de données JMX. Il se peut que certains attributs ne contiennent pas de données. Une fois la source de données JMX créée, vérifiez les attributs et supprimez ceux qui ne sont pas importants. Si le MBean sélectionné ne comporte pas d'attributs, vous êtes informé que la source de données est créée sans aucun attribut. Si le MBean sélectionné contient des notifications, une source de données "Evénement" est également créée pour recevoir les notifications des MBeans.

   Important : Pour chaque attribut de bean géré, Agent Builder crée un attribut dans le nouveau jeu de données. Pour un attribut de bean géré numérique, Agent Builder crée un attribut numérique. Pour n'importe quel type d'objet, y compris `String`, Agent Builder crée un attribut de chaîne contenant une représentation sous forme de chaîne de la valeur. Si un objet d'un attribut de bean géré est du type `javax.management.openmbean.CompositeData` et que le navigateur Agent Builder peut lire l'objet lui-même, il crée plusieurs attributs, un pour chaque objet intégré dans l'objet `CompositeData`. Pour inclure des valeurs internes à un objet autre qu'un objet `CompositeData` (des zones ou des valeurs de retour de méthode), vous devez créer un attribut qui a un nom mesure plus complexe, comme décrit dans la rubrique «Zones caractéristiques des MBeans JMX (Java Management Extensions)», à la page 1293.

8. Cliquez sur **Terminer** sur la page Informations JMX renseignée.

   Les sources de données sont créées sur la base du MBean sélectionné à l'étape précédente. Si aucun MBean n'a été sélectionné, un groupe d'attributs ne comportant aucun attribut est créé. Un avertissement s'affiche pour sélectionner un MBean. Le mot **Evénement** figure au début du nom de la source de données de notification, afin de faire la distinction entre cette source de données et la source de données affichant des attributs.
9. Pour modifier d'autres options JMX pour l'agent, cliquez sur **Options JMX globales**. Ces options vous permettent d'effectuer les opérations suivantes :
   a) Vérifiez si les contrôleurs JMX sont pris en charge par cet agent. Pour créer des groupes d'attributs de contrôleur JMX et des commandes Action, cochez la case **Insérer des groupes d'attributs et commandes Action de contrôleur JMX**.

      Pour obtenir une description des contrôleurs JMX, consultez la section ci-après.
   b) Sélectionnez les types de serveurs MBean auxquels votre agent doit se connecter lorsqu'il est déployé.

      Plusieurs types de serveurs propres au fournisseur sont répertoriés, ainsi qu'un serveur générique compatible JSR-160 pour les serveurs normalisés. Vous pouvez sélectionner autant de types de serveurs que nécessaire, mais vous ne devez sélectionner que les types de serveurs prenant en charge les MBeans à surveiller. Vous devez en sélectionner au moins un. Si vous en sélectionnez plusieurs, vous êtes invité, lors de la configuration de l'agent, à indiquer le type de serveur auquel vous voulez vous connecter.
10. Cliquez sur **OK** après avoir sélectionné l'option voulue.
11. Facultatif : Vous pouvez tester ce groupe d'attributs en cliquant sur **Tester**. Pour plus d'informations sur les tests, voir («Test des groupes d'attributs JMX», à la page 1296).
12. Facultatif : Vous pouvez créer un filtre pour limiter les données renvoyées par ce groupe d'attributs en cliquant sur **Avancé**. Pour plus d'informations sur le filtrage de données à partir d'un groupe d'attributs, voir «Filtrage des groupes d'attributs», à la page 1237.
13. Cliquez sur **Suivant**.
14. Sur la page **Sélectionner les attributs clés**, sélectionnez les attributs de clé ou indiquez que la source de données génère uniquement une ligne de données. Pour plus d'informations, voir «Sélection des attributs de clé», à la page 1206.
15. Cliquez sur **Suivant**.

    La fenêtre **Options d'agent JMX** affiche les types de serveurs d'applications pris en charge par Agent Builder. Si vous avez précédemment sélectionné **Définir comme valeurs par défaut de la configuration de l'agent** sur la page **Propriétés de connexion**, le type de serveur d'applications que vous avez recherché est automatiquement sélectionné.
16. Dans la fenêtre **Options d'agent JMX** (Figure 37, à la page 1284), sélectionnez d'autres types de serveur d'applications auxquels vous voulez que votre agent puisse se connecter.

    Remarque : Dans l'exemple fourni, la sélection de **Connexion JBoss Application Server JSR-160** revient à sélectionner **Serveur conforme à JSR-160** à l'exception que des valeurs par défaut différentes sont fournies.

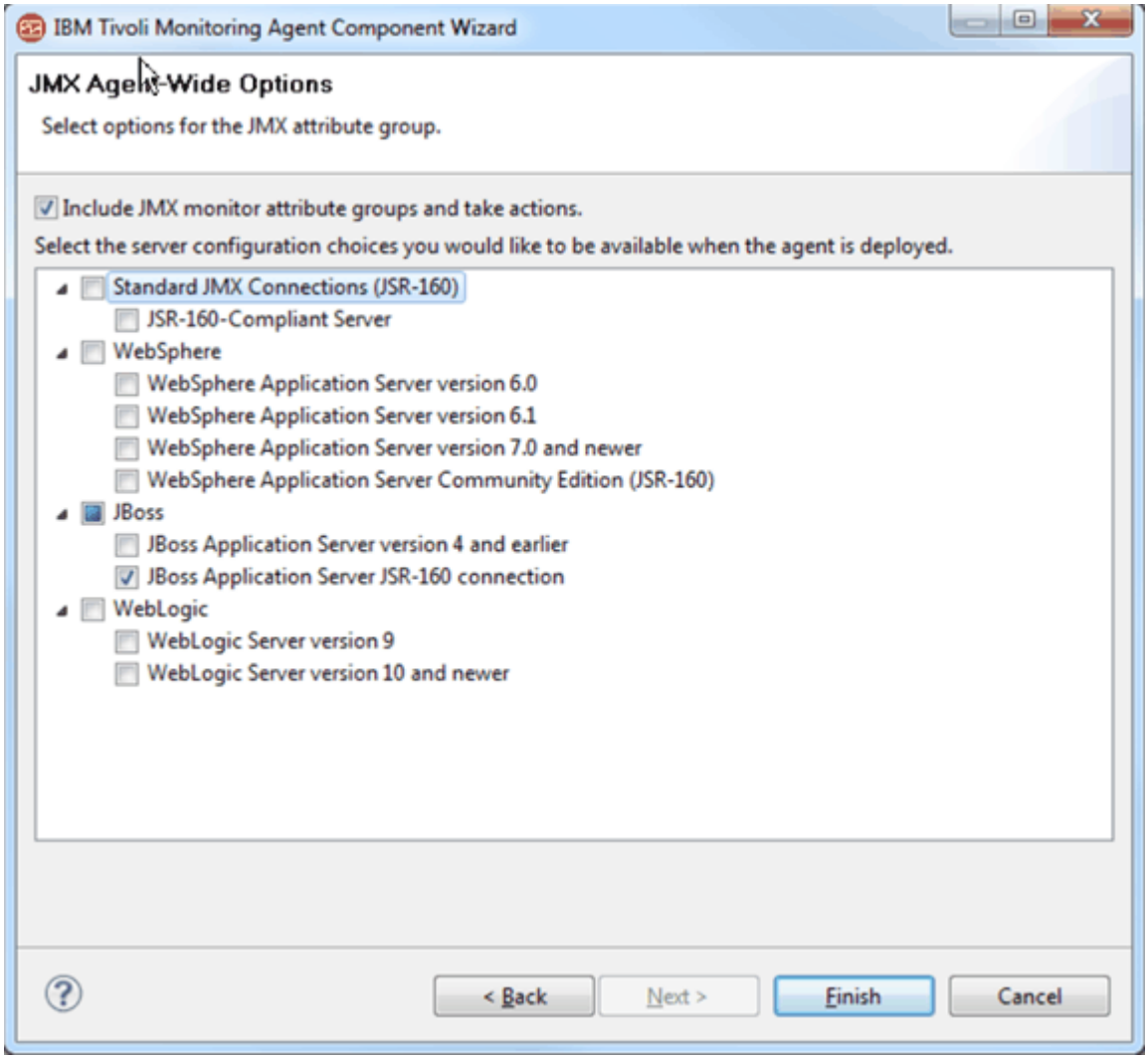


Figure 37. Fenêtre Options d'agent JMX

17. Effectuez l'une des opérations suivantes :
    - Si vous utilisez l'assistant de création d'agent, cliquez sur **Suivant**.
    - Cliquez sur **Terminer** pour sauvegarder la source de données et ouvrir l'éditeur d'agent.
18. Pour modifier les types de serveur d'applications auxquels vous connecter une fois l'agent créé, cliquez sur **Options JMX globales** dans la zone **Informations sur la source de données JMX**.
19. Dans la fenêtre **Options d'agent JMX**, modifiez toutes les sélections désirées.
20. Cliquez sur **OK**.
21. Pour afficher les sections et propriétés de configuration qui ont automatiquement été générées, cliquez sur l'onglet **Configuration d'exécution** de l'éditeur d'agent.

    La valeur par défaut de la propriété des `chemins de base JBoss` est la même que celle entrée dans le navigateur JMX.

Que faire ensuite

Pour plus d'informations sur les groupes d'attributs relatifs aux événements JMX, voir «Groupes d'attributs d'événements JMX», à la page 1494,

Configuration JMX
Lorsque vous définissez une source de données JDBC dans l'agent, des propriétés de configuration sont créées automatiquement.

La configuration d'exécution JMX est unique car elle permet de contrôler la quantité de configuration affichée. Le client JMX de l'agent peut se connecter à plusieurs types de serveurs d'applications différents. Toutefois, il n'est pas nécessaire de prendre en charge tous ces types de serveurs d'applications dans un agent. Vous pouvez déterminer les types de serveurs d'applications à prendre en charge, de sorte que les sections de configuration inutiles ne sont pas incluses dans l'agent.

Dans la plupart des cas, un agent est conçu pour surveiller un seul type de serveur d'applications JMX. Lorsque vous créez la source de données JMX, vous pouvez utiliser le navigateur JMX. Lors de l'utilisation du navigateur JMX, les options de configuration de serveur JMX permettant de parcourir le serveur de MBean sont sélectionnées et ajoutées automatiquement dans l'agent. Pour modifier les types de serveur d'applications auxquels vous connecter une fois l'agent créé, cliquez sur **Options JMX globales** dans la zone **Informations JMX**. Sur la page **Options d'agent JMX**, modifiez toutes les sélections désirées.

Vous pouvez concevoir un agent générique qui surveille plusieurs types de serveurs d'applications JMX. Dans ce cas, plusieurs options de configuration de serveur JMX peuvent être sélectionnées sur la page **Options d'agent JMX**. Lorsque plusieurs types de connexions JMX sont pris en charge, la configuration d'exécution demande de préciser le type de connexion à utiliser pour l'instance d'agent.

Remarque : Une instance d'un agent ne peut se connecter qu'à un seul type de serveur d'applications JMX. Les sous-noeuds permettent d'établir une connexion à des serveurs d'applications JMX différents du même type dans une instance d'agent. Pour vous connecter à plusieurs types de serveur d'applications JMX, vous devez configurer au moins une instance d'agent pour chaque type de serveur d'applications JMX.

Vous pouvez visualiser, ajouter et modifier les propriétés de configuration à l'aide de l'éditeur d'agent. Pour obtenir des instructions, voir «Modification des propriétés de configuration à l'aide de l'éditeur d'agent», à la page 1407. Si une source de données JMX est définie dans un sous-noeud, vous pouvez également définir des substitutions de configuration. Pour obtenir des instructions, voir «Configuration de sous-noeud», à la page 1394.

Si vous définissez une source de données JMX dans votre agent, celui-ci doit utiliser Java pour se connecter au serveur d'applications JMX. Les propriétés de configuration Java s'ajoutent automatiquement à l'agent.

Les propriétés de configuration Java suivantes sont propres à la configuration d'exécution de l'agent :

Répertoire de base Java
Chemin qualifié complet pointant vers le répertoire d'installation Java

Configurez l'agent de sorte qu'il utilise la même JVM que l'application surveillée, notamment pour le serveur WebLogic et pour WebSphere Application Server.

Arguments JVM
Indique une liste facultative d'arguments pour la machine virtuelle Java.

Niveau de trace
Définit la quantité d'informations à écrire dans le fichier de trace Java. Par défaut, les données d'erreur sont écrites dans le fichier journal.

Remarque : Agent Builder n'a pas besoin de ces propriétés, dans la mesure où il utilise sa propre JVM et sa propre consignation qui sont configurées via le plug-in JLog.

Si vous définissez une source de données SNMP dans votre agent, les zones de configuration courantes obligatoires suivantes s'ajoutent automatiquement à l'agent :

Connexion
Type de la connexion au serveur MBean

ID utilisateur
Nom d'utilisateur servant à l'authentification auprès du serveur MBean.

Mot de passe
Mot de passe de l'ID utilisateur.

Chemins de base
Liste des répertoires dans lesquels les fichiers JAR nommés dans la zone **Chemin d'accès aux classes** sont recherchés ou répertoires nommés dans **Répertoires JAR** qui ne sont pas complètement qualifiés. Les noms de répertoire sont séparés par un point-virgule (`;`) sur Windows, et par un point virgule ((`;`) ou deux points (`:`) sur les systèmes UNIX.

Chemin d'accès aux classes
Fichiers JAR explicitement nommés dans lesquels l'agent doit faire ses recherches. Les répertoires qui ne sont pas complètement qualifiés s'ajoutent à chacun des chemins de base tant que le répertoire n'est pas trouvé.

Répertoires JAR
Liste des répertoires dans lesquels les fichiers JAR sont recherchés. Les noms de répertoire sont séparés par un point-virgule (`;`) sur Windows, et par un point virgule ((`;`) ou deux points (`:`) sur les systèmes UNIX. Les fichiers JAR de ces répertoires n'ont pas besoin d'être identifiés explicitement ; ils seront détectés, car ils se trouvent dans l'un de ces répertoires. La recherche ne s'applique pas aux sous-répertoires de ces répertoires. Les répertoires qui ne sont pas complètement qualifiés s'ajoutent à chacun des chemins de base tant que le répertoire n'est pas trouvé.

Remarque : Lors de la surveillance à distance, les fichiers JAR et tous leurs fichiers JAR dépendants doivent être installés en local sur l'ordinateur sur lequel l'agent est en cours d'exécution. Ces fichiers JAR sont les fichiers qui sont requis pour la connexion à l'application qui est surveillé. Ces fichiers JAR doivent être configurés dans **Répertoires JAR** et dans **Chemins de base** et **Chemin d'accès aux classes**. En outre, vous devez installer en local une JVM prise en charge pour l'application que vous surveillez et spécifier le chemin dans la zone de configuration **Répertoire de base Java**.

Exemples :

- Pour WebLogic 10, le chemin d'accès aux classes est `server/lib/wlclient.jar;server/lib/wljmxclient.jar`. Le chemin de base pointe vers le répertoire de serveur d'applications WebLogic qui contient le répertoire `server/lib`.
- Pour WebSphere, le chemin de base pointe vers l'emplacement où le serveur d'applications WebSphere est installé. Plusieurs chemins de base sont répertoriés dans cet exemple, afin de fournir une valeur par défaut pour Windows et UNIX. Le chemin d'accès aux classes répertorie les fichiers JAR relatifs au chemin de base. La valeur relative `lib` de la zone **Répertoires JAR** charge tous les fichiers JAR de ce répertoire dans le chemin de base.
  - **Chemins de base** : `C:\Program Files\IBM\WebSphere\AppServer;/opt/IBM/WebSphere/AppServer`
  - **Chemin d'accès aux classes** : `runtimes/com.ibm.ws.admin.client_6.1.0.jar;plugins/com.ibm.ws.security.crypto_6.1.0.jar`
  - **Répertoires JAR** : `lib`

En fonction des types de serveur JMX sélectionnés sur la page Options d'agent JMX, quelques-unes ou l'ensemble des propriétés de configuration ci-dessous sont ajoutées. Les valeurs par défaut sont fournies par Agent Builder et peuvent être modifiées :

Propriétés de configuration spécifiques à la connexion au serveur compatible JSR-160 :

Adresse URL du service JMX
Adresse URL de services JMX à laquelle se connecter pour la surveillance.

Propriétés de configuration spécifiques à la connexion WebSphere Application Server version 6.0 et ultérieure :

Nom d'hôte
Nom d'hôte du système où réside le serveur d'applications que vous surveillez. Si la surveillance est effectuée en local, il s'agit du nom du système local. Si la surveillance est effectuée à distance, il s'agit du nom d'hôte du système où réside le serveur d'applications.

Port
Numéro de port à utiliser sur l'hôte à surveiller.

Protocole de connecteur
Protocole de connecteur à utiliser par la connexion de surveillance. RMI et SOAP sont pris en charge.

Nom de profil
Nom du profil à utiliser pour la configuration de la connexion.

Propriétés de configuration spécifiques à la connexion à JBoss Application Server (non JSR-160) :

Nom JNDI
Nom JNDI utilisé pour rechercher le serveur de MBean.

Adresse URL de fournisseur
Adresse URL de services JMX à laquelle vous vous connectez pour la surveillance.

Propriétés de configuration spécifiques à la connexion à WebLogic Server :

Adresse URL de service
Adresse URL du fournisseur de services JMX à laquelle vous vous connectez pour la surveillance, qui inclut également le nom JNDI.

Remarque : Si la sécurité administrative WebSphere est activée, vous devez vous assurer que les invites de connexion du client sont désactivées dans les fichiers de propriétés appropriés de la connexion du client. Pour les connexions RMI, vous devez modifier la propriété *com.ibm.CORBA.loginSource* dans le fichier `sas.client.props` dans le répertoire des propriétés de profil de WebSphere Application Server pour empêcher les clients d'envoyer des invites aux utilisateurs. Pour une connexion SOAP, vous devez modifier la propriété *com.ibm.SOAP.loginSource* dans le fichier `soap.client.props` dans le même répertoire. Dans les deux cas, la propriété *loginSource* doit être définie de manière à ne pas contenir de valeur.

Vous pouvez visualiser, ajouter et modifier les propriétés de configuration à l'aide de l'éditeur d'agent. Voir («Modification des propriétés de configuration à l'aide de l'éditeur d'agent», à la page 1407). Si une source de données Windows est définie dans un sous-noeud, vous pouvez également indiquer des substitutions de configuration de sous-noeud. Voir «Configuration de sous-noeud», à la page 1394.

Notifications JMX
Outre la fourniture de données à la demande, certains MBeans envoient également des notifications.

Une notification est un objet généré par un MBean qui, lorsqu'un événement se produit, est transmis aux modules d'écoute enregistrés.

Les agents générés par Agent Builder peuvent définir des groupes d'attributs contenant des valeurs issues des notifications et non de MBeans.

Lors du démarrage de l'agent, un `module d'écoute de notification` est connecté à chaque MBean correspondant au modèle MBean du groupe d'attributs. Le groupe d'attributs affiche ensuite une ligne par notification reçue. Chaque colonne contient un seul élément de données de la notification. Les données souhaitées de la notification sont définies par une valeur de colonne de la même façon que les colonnes de données sont définies pour les MBeans.

Pour les groupes d'attributs autres que ceux basés sur des événements, les données sont collectées si nécessaire. Pour les groupes d'attributs basés sur des événements, l'agent gère une mémoire cache des 100 derniers événements reçus. Ces événements servent à répondre aux demandes émanant de Tivoli Enterprise Portal. Les événements sont immédiatement réacheminés pour être analysés par des situations et l'entreposage.

Contrôleurs JMX
Outre la fourniture des données de surveillance demandées, certains MBeans fournissent des contrôleurs.

Le fournisseur JMX permet à un agent de créer des contrôleurs JMX. Un contrôleur JMX est un MBean que l'agent JMX crée sur le serveur JMX. Il surveille la valeur d'un attribut d'un autre MBean et envoie une notification lorsque la valeur répond à certains critères. Des seuils permettant au contrôleur de générer un rapport sur des valeurs d'attribut spécifiques sont définis.

Tous les serveurs d'applications ne prennent pas en charge la création de contrôleurs à partir d'un client JMX, ce qui est valable pour les éditions en cours de WebSphere Application Server. Vous pouvez inclure des commandes Action et des contrôleurs JMX dans votre agent si vous sélectionnez **Insérer des groupes d'attributs et commandes Action de contrôleur JMX** sous **Options JMX globales**.

Tout MBean générant un rapport sur un attribut d'un autre MBean peut être considéré comme étant un contrôleur. En pratique, JMX définit trois classes de contrôleurs concrètes qui sont les types de contrôleurs créés. Les types de contrôleurs concrets suivants sont créés :

- contrôleur de chaînes – surveille un attribut de chaîne et signale l'égalité ou l'inégalité de cette chaîne.
- Contrôleur de jauge – surveille un attribut numérique variable et signale les mouvements vers le haut ou le bas dépassant les valeurs de seuil.
- Contrôleur de compteur – surveille un attribut numérique croissant et génère un rapport lorsque celui-ci atteint une valeur de seuil ou qu'il augmente d'une certaine quantité.

Les groupes d'attributs suivants peuvent automatiquement être ajoutés dans l'agent pour collecter ou représenter des notifications de contrôleur JMX :

- `Contrôleurs enregistrés`

  Ce groupe d'attributs affiche tous les contrôleurs JMX qui ont été ajoutés par l'utilisateur.
- `Notifications de compteur`

  Ce groupe d'attributs signale toutes les notifications reçues des contrôleurs de compteur.
- `Notifications de jauge`

  Ce groupe d'attributs signale toutes les notifications reçues des contrôleurs de jauge.
- `Notifications de chaîne`

  Ce groupe d'attributs signale toutes les notifications qui reçues des contrôleurs de chaînes.

Commandes Actions pour les moniteurs JMX
Un contrôleur est créé via l'exécution d'une commande Action.

Trois commandes Action sont définies : une pour créer chaque type de contrôleur et une quatrième pour supprimer un contrôleur existant. Une limite de 256 caractères s'applique aux commandes Action.

Les groupes d'attributs de contrôleur font partie de tous les agents JMX générés, y compris tous les agents générés par Agent Builder. Les quatre commandes Action sont accessibles à tous les agents, même si elles ne peuvent être utilisées qu'avec un agent JMX.

JMX Add String Metric Watcher
Utilisez cette commande Action pour créer un contrôleur pour surveiller un attribut de chaîne.

Paramètres

Modèle MBean
Tous les MBeans correspondant à ce modèle sont surveillés par ce contrôleur.

Attribut observé
Nom de l'attribut de chaîne MBean qui est en cours de surveillance.

Notifier occurrence
True si une notification doit être envoyée lorsque la chaîne surveillée correspond à une valeur de référence ; dans le cas contraire, ce paramètre a pour valeur false (valeur par défaut : false).

Notifier différence
True si une notification doit être envoyée lorsque la chaîne surveillée ne correspond pas à la valeur de référence ; dans le cas contraire, ce paramètre a pour valeur false (valeur par défaut : true).

Valeur de référence
Chaîne à comparer à l'attribut observé.

Lorsqu'une valeur par défaut est indiquée, cela signifie que l'argument n'est pas spécifié.

Exemple : Demander une notification lorsqu'un service est arrêté

```
STRING_METRIC_WATCHER [*:type=Service,*] [StateString] [true] [false] [Stopped]
```

Où :

`*:type=Service,*`
Modèle de MBean : permet de surveiller les objets MBean ayant une propriété de clé unique nommée type dont la valeur est Service.

`StateString`
Attribut observé : attribut de chaîne commun à tous les MBeans dans `type=Service`.

true
Notifier occurrence : vous voulez qu'une notification soit envoyée à votre agent lorsque l'attribut `StateString` correspond à votre valeur de référence Stopped (arrêté).

false
Notifier différence : vous ne voulez pas recevoir de notification lorsque l'attribut Service ne correspond pas à la valeur Stopped (arrêté).

Arrêté
Valeur de référence : lorsque l'attribut `StateString` est remplacée par Stopped (arrêté), une notification est envoyée.

JMX Add Gauge Metric Watcher
Utilisez cette commande Action pour créer un contrôleur pour surveiller un attribut de jauge.

Paramètres

Modèle MBean
Tous les MBeans correspondant à ce modèle sont surveillés par ce contrôleur.

Attribut observé
Nom de l'attribut de chaîne MBean qui est en cours de surveillance.

Mode différence
True si la valeur surveillée est la différence entre les valeurs actuelle et précédente réelles de l'attribut. False si la valeur surveillée est la différence entre les valeurs actuelle et précédente réelles de l'attribut (False par défaut).

Notifier valeur haute
True si une notification doit être envoyée lorsqu'une valeur surveillée croissante dépasse le seuil haut ; dans le cas contraire, false (valeur par défaut : true).

Notifier valeur basse
True si une notification doit être envoyée lorsqu'une valeur surveillée décroissante dépasse le seuil bas ; dans le cas contraire, false (valeur par défaut : true).

Seuil haut
Valeur en dessous de laquelle l'attribut observé doit rester.

Seuil bas
Valeur au-dessus de laquelle l'attribut observé doit rester.

Exemple : demander une notification lorsque la mémoire libre tombe en dessous de 10 Mo

```
GAUGE_METRIC_WATCHER [ServerInfo] [FreeMemory] [false] [false] [true] [30000000] [10000000]
```

Où :

***:type=ServerInfo**
Modèle MBean : Permet de surveiller tous les objets MBean dont le nom comporte une propriété de clé unique nommée type dont la valeur est ServerInfo.

FreeMemory
Attribut observé : Attribut numérique fluctuant vers le haut ou vers le bas, indiquant l'espace mémoire disponible dans le serveur d'applications.

false
Mode différence : Surveille la valeur d'attribut réelle et non la différence entre une observation et une autre.

false
Notifier valeur haute : Aucune notification n'est envoyée lorsque la mémoire disponible augmente.

true
Notifier valeur basse : Aucune notification n'est envoyée lorsque la mémoire disponible diminue excessivement.

30000000
Seuil haut : Même si vous n'êtes pas concerné par le dépassement d'un seuil haut, vous avez besoin d'une valeur de seuil haut raisonnable. Une deuxième notification de seuil base ne se produit que lorsque la valeur d'attribut atteint ou dépasse le seuil haut.

10000000
Seuil bas : Valeur de seuil bas pour laquelle vous voulez être notifié.

JMX Add Counter Metric Watcher
Utilisez cette commande Action pour créer un contrôleur pour surveiller un attribut de compteur.

Paramètres

Modèle MBean
Tous les MBeans correspondant à ce modèle sont surveillés par ce contrôleur.

Attribut observé
Nom de l'attribut de chaîne MBean qui est en cours de surveillance.

Seuil initial
Valeur à laquelle l'attribut observé est comparé.

Décalage
Valeur ajoutée au seuil une fois ce dernier dépassé, afin de créer une modification de seuil.

Modulo
Valeur maximale du compteur après laquelle il est remis à 0.

Mode différence
True si la valeur surveillée est la différence entre les valeurs actuelle et précédente réelles de l'attribut. False si la valeur surveillée est la différence entre les valeurs actuelle et précédente réelles de l'attribut (False par défaut). Ce mode active le contrôle de fréquence de changement.

Période de granularité
Fréquence à laquelle les mesures sont effectuées (valeur par défaut : 20 secondes). Très important si le mode de différence a la valeur true

Exemple : Demander une notification lorsqu'un serveur comporte au moins trois erreurs.

```
COUNTER_METRIC_WATCHER [*:j2eeType=Servlet,*] [errorCount] [3] [4] [] [diff] [gran]
```

Où :

:j2eeType=Servlet,
Modèle de MBean : permet de surveiller les MBeans servlet J2EE ayant une propriété de clé unique nommée type dont la valeur est `ServerInfo`.

errorCount
Attribut observé : Attribut numérique croissant, indiquant le nombre d'erreurs du servlet.

3
Seuil initial : vous voulez être averti lorsque `errorCount` atteint ou dépasse 3.

4
Décalage : lorsque vous recevez une notification pour trois erreurs, 4 est ajouté au seuil précédent 3 pour créer le nouveau seuil 7. Une deuxième notification est envoyée une fois que `errorCount` atteint 7, une troisième à 11, une quatrième à 15, etc. Zéro ou l'absence n'est pas valide, car la valeur du compteur doit toujours augmenter et la non-augmentation du décalage n'a pas de sens pour un compteur.

Modulo :
errorCount ne comporte aucune valeur maximale structurée ; utilisez donc une valeur exagérément élevée.

false
Mode différence : Vous êtes concerné par les nombres d'erreur absolus. La différence a pour valeur true si vous êtes intéressé par le taux d'augmentation du nombre d'erreurs (errorCount).

Période de granularité : Non définie ; par conséquent, la période de granularité par défaut de 20 secondes est utilisée. La période de granularité est disponible pour tous les types de contrôleurs. Cependant, elle est utilisée avec un contrôleur de compteur de sorte qu'un taux de modification significatif (mode différence = true) puisse être déterminé.

JMX Delete Metric Watcher
Cette commande Action permet de supprimer un contrôleur.

Paramètre

Numéro
Numéro de contrôleur, tel qu'il est présenté dans la table REGISTERED_MONITORS.

Exemple : Supprimer le contrôleur numéro 2

```
DELETE_WATCHER [2]
```

Où :

2=
Numéro du contrôleur à supprimer.

Opérations JMX
Outre la fourniture des données de surveillance demandées, certains MBeans fournissent des opérations.

Les agents comportant des sources de données JMX incluent la commande Action `JMX_INVOKE` qui vous permet d'exécuter des opérations JMX sur le serveur que vous surveillez.

Syntaxe des commandes Action

L'action a la syntaxe suivante :

```
JMX_INVOKE [Modèle MBean] [Nom de l'opération] [Argument 1] [Argument 2]
[Argument 3] [Argument 4]
```

Où :

Modèle MBean
Requête de MBean qui sélectionne les MBeans sur lesquels l'opération va s'exécuter. Si le modèle correspond à plusieurs MBeans, l'opération s'exécute sur chacun des MBeans appariés.

Nom de l'opération
Nom de l'opération MBean à exécuter.

Argument 1, Argument 2, Argument 3, Argument 4
Arguments facultatifs pouvant être fournis à l'opération MBean. Les arguments doivent correspondre à un type de données simple, tel qu'une chaîne ou un entier.

La commande Action JMX `invoke` renvoie une indication de réussite si l'opération est correctement exécutée. Si l'opération renvoie une valeur, cette dernière est consignée dans le fichier journal du fournisseur de données JMX.

Exemple : démarrage d'une opération pour réinitialiser un compteur

Cette action exécute l'opération resetPeakThreadCount sur les MBeans Threading :

```
JMX_INVOKE [*:type=Threading,*] [resetPeakThreadCount][] [] [] []
```

Où :

:type=Threading,
Modèle MBean : ce modèle correspond à tous les MBeans dont le type est Threading.

resetPeakThreadCount
Nom de l'opération : il s'agit de l'opération exécutée sur tous les MBeans correspondants au modèle.

[] [] [] []
Arguments 1, 2, 3, 4 : Les arguments ne sont pas nécessaires pour cette opération. Ils ne sont indiqués que pour la conformité avec la syntaxe de l'action.

Exemple : démarrage d'une opération avec un argument

Cette action exécute l'opération getThreadCpuTime sur les MBeans Threading. Le résultat est consigné dans le fichier de trace du fournisseur JMX.

```
JMX_INVOKE [*:type=Threading,*] [getThreadCpuTime] [1] [] [] []
```

Où :

:type=Threading,
Modèle MBean : Ce modèle correspond à tous les MBeans dont le type est Threading.

getThreadCpuTime
Nom de l'opération : il s'agit de l'opération exécutée sur tous les MBeans correspondants au modèle.

1
Argument 1 : Identificateur de l'unité d'exécution en cours d'interrogation.

[] [] []
Arguments 2, 3, 4 : Ces arguments ne sont pas nécessaires pour cette opération. Ils sont indiqués sous forme d'arguments vides pour la conformité avec la syntaxe de commande Action.

Exécution de la commande Action JMX_INVOKE

Le développeur d'agent ne peut pas s'attendre à ce que l'utilisateur exécute la commande Action JMX_INVOKE. En revanche, des actions supplémentaires exécutant la commande Action JMX_INVOKE doivent être développées. Si possible, dans ces actions, masquez les détails tels que le nom de l'opération et le modèle MBean pour que l'utilisateur ne les voit pas.

Démarrage et arrêt des contrôleurs JMX
Les contrôleurs sont persistants tout au long des démarrages et arrêts de l'agent et du serveur JMX.

Si l'agent détecte que le serveur JMX a été recyclé, il ré-enregistre les contrôleurs. Si l'agent est recyclé, les contrôleurs sont ré-enregistrés. Les définitions de contrôleur sont stockées dans un fichier intitulé `default_`*`nom_instance`*`.monitors`, où *nom_instance* correspond au nom d'instance de l'agent ou à default s'il s'agit d'un agent à instance unique. Ce fichier se trouve dans le répertoire suivant (*xx* représente le code produit de 2 caractères) :

- Systèmes Windows : TMAITM6/k*xx*/config
- Systèmes UNIX et Linux : *architecture*/*xx*/config (voir «Nouveaux fichiers sur votre système», à la page 1438 pour savoir comment déterminer la valeur d'architecture)

Si l'agent est redémarré, il utilise le fichier des définitions des contrôleurs pour restaurer les contrôleurs.

Zones caractéristiques des MBeans JMX (Java Management Extensions)
La syntaxe du nom de métrique d'un groupe d'attributs JMX doit respecter certaines règles lorsque cela est spécifié dans la fenêtre **Informations d'attribut**.

La syntaxe du nom de métrique d'un groupe d'attributs JMX est constituée de jetons séparés par un point. Les jetons forment des valeurs principales et, le cas échéant, des valeurs secondaires :

- **Valeur principale** : valeur obtenue directement du MBean ou d'une notification dans une ligne donnée de la table. Les valeurs principales d'un MBean sont obtenues d'un attribut MBean ou de l'appel d'une opération MBean (appel de méthode). Les valeurs principales d'une notification sont obtenues d'une zone ou d'un appel d'une méthode sur l'objet Notification. Les valeurs principales peuvent être des types primitifs ou des objets Java.
- **Valeur secondaire** : valeur obtenue par le traitement supplémentaire d'une valeur principale ou d'une autre valeur secondaire. Les valeurs secondaires sont traitées en interne dans le moteur et n'impliquent pas d'appels émis au serveur JMX. Si la valeur principale (ou l'autre valeur secondaire) est un objet Java, une valeur secondaire est le résultat de l'extraction d'une zone publique à partir de cet objet. Une valeur secondaire peut également être le résultat d'un appel de méthode sur cet objet. Les valeurs secondaires sont obtenues à l'aide de l'introspection Java de l'objet Java principal (ou d'un autre objet Java secondaire). Si la valeur principale (ou l'autre valeur secondaire) est une chaîne Java sous la forme d'un nom de MBean, la valeur secondaire peut correspondre au domaine. La valeur secondaire peut également correspondre à l'une des propriétés composant le nom du MBean.

La syntaxe suivante décrit le format de la zone **Nom de métrique** :

```
Metric Name    =    valeur_principale [ .valeur_secondaire ]
PrimaryValue    =    Attribute.nom_attribut |
        Method.nom_méthode |
        Domain |
        Property.nom_propriété |
        Field.nom_zone |
        Nom
SecondaryValue    =    Field.nom_zone |
        Method.nom_méthode |
        Domain |
        Property.nom_propriété |
        Explode |
        ElementCount
```

```
propertyName    =    nom d'une propriété de clé dans un nom d'objet MBean
attributeName    =    nom d'un attribut MBean
methodName    =    opération à zéro argument d'un MBean ou méthode à zéro argument d'une
notification ou d'un autre objet Java.
nom_méthode(argument) = Opération à argument unique d'un MBean ou méthode à
argument unique d'une notification ou d'un autre objet Java. La commande
L'argument
sera transmis à la méthode sous la forme d'une chaîne.
fieldName    =    nom d'une variable d'instance publique dans une
            notification ou un autre objet Java
notificationMethod    =    nom d'une méthode publique à zéro argument d'un
                    objet Notification
```

En insérant uniquement une valeur principale dans la définition de nom de métrique, les données collectées peuvent correspondre à l'un des éléments suivants :

- Domaine de MBean
- Valeur de chaîne du MBean
- Propriété de clé issue du nom du MBean
- Valeur d'attribut numérique ou de type chaîne dans un attribut d'un MBean (y compris le nom complet d'un autre MBean). Une valeur de retour de type chaîne ou numérique à partir d'une opération d'un MBean.

- Valeur d'une variable d'instance publique numérique ou de type chaîne dans un objet Notification
- Valeur de retour numérique ou de type chaîne d'une opération d'une notification.

En ajoutant une valeur secondaire à définition d'une métrique, vous pouvez explorer en aval la valeur principale d'un objet Java. En outre, vous pouvez démarrer une méthode publique ou extraire une variable d'instance publique.

En ajoutant une valeur secondaire à une autre valeur secondaire dans la définition de la métrique, vous pouvez explorer en aval un objet de valeur secondaire. Vous pouvez continuer cette exploration en aval aussi loin que les objets sont imbriqués dans un MBean ou une notification.

Les jetons qui composent les valeurs principales ou secondaires sont des mots clés ou des noms. Dans la plupart des cas, un jeton de mot clé est suivi d'un jeton de nom. Le tableau suivant présente quelques exemples :

Exemple de nom d'unité de mesure	**Type de groupe d'attributs**	**Description des données renvoyées**
`Domain`	MBean	Partie domaine du MBean (partie située avant le signe deux-points).
`Nom`	MBean	Représentation de chaîne complète du MBean.
`Attribute.serverVendor`	MBean	Attribut MBean serverVendor.
`Method.getHeapSize`	MBean	Valeur renvoyée par getHeapSize() sur le MBean.
`Property.j2eeType`	MBean	La valeur de j2eeType est extraite du nom de MBean.
`Field.Message`	Evénement (Notification)	Zone **Message** dans une notification.

Les mots clés `Attribute`, `Method` et `Field` peuvent renvoyer des objets Java contenant d'autres données. Vous pouvez effectuer des opérations sur ces objets en ajoutant des définitions de valeur secondaire. Autres exemples :

Exemple de nom d'unité de mesure	**Type de groupe d'attributs**	**Description des données renvoyées**
Attribute.deployedObject.Method.getName	MBean	Extrait l'attribut deployedObject du MBean et obtient le résultat de la méthode getName().
Attribute.eventProvider.Method.getException.Method.getDescription	MBean	Trois étapes : un attribut intitulé eventProvider est censé être un objet comportant une méthode getException(). Cette méthode renvoie un objet à l'aide d'une méthode getDescription(). Cette méthode est appelée et la valeur de retour est placée dans la colonne.

Exemple de nom d'unité de mesure	Type de groupe d'attributs	Description des données renvoyées
Attribute.HeapMemoryUsage.Method.get(used)	MBean	Extrait l'attribut HeapMemoryUsage du MBean et obtient le résultat de la méthode get(String valeur). La chaîne utilisée est transmise à la méthode sous forme d'argument. Un seul argument peut être fourni et celui-ci doit correspondre à une valeur de chaîne littérale. Explique comment collecter des données d'une structure de données composites MBean ouverte.

`Domain` et `Property` peuvent être utilisés comme mots clés dans les valeurs secondaires si la valeur précédente a renvoyé une chaîne au format d'un nom de MBean. Par exemple :

Exemple de nom d'unité de mesure	Type de groupe d'attributs	Description des données renvoyées
`Attribute.jdbcDriver.Property.name`	MBean	L'attribut jdbcDriver renvoie un nom de MBean et la propriété de clé name est extraite du nom de MBean.
`Attribute.jdbcDriver.Domain`	MBean	L'attribut jdbcDriver renvoie un nom de MBean et le domaine est extrait du nom de MBean.

Les mots clés `ElementCount` et `Explode` effectuent des opérations sur des tableaux ou des collectes de données.

- `ElementCount` – renvoie le nombre d'éléments d'un tableau.
- `Explode` – scinde une ligne en plusieurs lignes correspondant chacune à un élément d'un tableau.

Exemples de chaque mot clé :

Exemple de nom d'unité de mesure	Type de groupe d'attributs	Description des données renvoyées
Attribute.deployedObjects.ElementCount	MBean	L'attribut MBean deployedObjects est un tableau et cette colonne contient le nombre d'éléments dans le tableau.
Attribute.deployedObjects.Explode.MBean.Property.j2eeType	MBean	La table comporte une seule ligne pour chaque élément des objets déployés. Cette colonne contient le type j2eeType de l'objet déployé.
Attribute.SystemProperties.Method.values.Explode.Method.get(key)	MBean	Permet d'extraire une nouvelle ligne pour chaque entrée dans une structure de données tabulaires MBean ouverte. Chaque structure de données tabulaires contient une structure de données composites comportant un élément intitulé key, qui est renvoyé.

Test des groupes d'attributs JMX

Vous pouvez tester le groupe d'attributs JMX que vous avez créé dans Agent Builder.

Procédure

1. Vous pouvez démarrer la procédure de test de l'une des manières suivantes :
   - Lors de la création de l'agent, cliquez sur **Tester** sur la page **Informations JMX**.
   - Après la création de l'agent, sélectionnez un groupe d'attributs à la page **Définition de la source de données** de l'éditeur d'agent et cliquez sur **Tester**. Pour plus d'informations sur l'éditeur d'agent, voir «Utilisation de l'éditeur d'agent pour modifier l'agent», à la page 1207.

   Après avoir cliqué sur **Tester** dans l'une des deux étapes précédentes, la fenêtre **Test JMX** s'affiche.
2. Sélectionnez une connexion dans la liste disponible sous **Nom de la connexion**, ou bien cliquez sur **Ajouter** pour ajouter une nouvelle connexion et suivez la procédure détaillée à l'étape «Surveillance de beans gérés (MBeans) JMX (Java Management Extensions)», à la page 1277.
3. Facultatif : Avant de démarrer le test, vous pouvez définir les variables d'environnement, les propriétés de configuration, ainsi que des informations Java.

   Pour plus d'informations, voir «Test des groupes d'attributs», à la page 1420. Pour plus d'informations sur la configuration JMX, voir «Configuration JMX», à la page 1285.
4. Cliquez sur l'option de **démarrage de l'agent**.

   Une fenêtre indique que l'agent est en cours de démarrage.
5. Pour simuler une demande de données d'agent provenant de Tivoli Enterprise Portal ou de SOAP, cliquez sur **Collecte de données**.

   L'agent surveille les données du serveur JMX. La fenêtre **Test JMX** collecte et affiche toutes les données du cache de l'agent depuis son dernier démarrage.
6. Facultatif : Cliquez sur **Vérifier les résultats** si les données renvoyées ne sont pas celles que vous attendez.

   La fenêtre **Statut de la collecte de données** affiche des informations supplémentaires sur les données. Les données collectées et affichées par la fenêtre Statut de la collecte de données sont décrites dans «Noeud de statut d'objet de performances», à la page 1466
7. Arrêtez l'agent en cliquant sur **Arrêter l'agent**.
8. Cliquez sur **OK** ou **Annuler** pour quitter la fenêtre **Test JMX**. Cliquez sur **OK** pour sauvegarder les modifications que vous avez apportées.

Concepts associés

«Test de votre agent dans Agent Builder», à la page 1420
Après avoir utilisé Agent Builder pour créer un agent, vous pouvez tester l'agent dans Agent Builder.

Surveillance de données à partir d'un modèle CIM (Common Information Model)

Vous pouvez définir une source de données pour qu'elle reçoive les données d'une source de données CIM (Common Information Model). Une source de données surveille une classe CIM unique et place toutes les valeurs de cette classe dans l'ensemble de données qu'elle produit. Si la classe fournit plusieurs instances, l'ensemble de données comporte plusieurs lignes ; vous pouvez effectuer un filtrage par nom d'instance pour vous assurer que l'ensemble de données comporte une ligne uniquement.

Pourquoi et quand exécuter cette tâche

Cette tâche décrit la procédure de configuration d'une source de données CIM.

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, cliquez sur **Données d'un serveur** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **CIM**.
3. Cliquez sur **Suivant**.

4. Sur la page **Informations sur le modèle CIM**, dans la zone **Informations sur le modèle CIM**, procédez de l'une des manières suivantes :

   - Complétez les zones **Espace de nom** et **Nom de classe CIM** pour les données que vous souhaitez collecter.
   - Cliquez sur **Parcourir** pour accéder à un référentiel CIM sur un système spécifique.

     La fenêtre **Afficheur de classe de modèle CIM** apparaît. Ce navigateur se connecte à serveur CIM et fournit des informations relatives aux classes existant sur ce serveur.

     Pour parcourir un système distant, sélectionnez un système dans la liste **Nom d'hôte** (si une liste a été définie). Vous pouvez également cliquer sur **Ajouter** pour ajouter le nom d'hôte du système sur lequel le serveur CIM est installé.

     La syntaxe de spécification du nom d'hôte est `http[s]://`*`nom_hôte`*`:`*`port`*. Si vous n'indiquez que le nom d'hôte, la fenêtre de navigation de classe de modèle CIM se connecte en utilisant une adresse URL par défaut : `http://`*`nom_hôte`*`:5988`.

     Si vous indiquez un protocole sans spécifier de port, 5988 est utilisé comme port par défaut pour `http`, ou 5989 pour `https`.

     Si vous indiquez un port sans préciser de protocole, `http` est utilisé avec le port fourni.

     Indiquez un ID utilisateur et un mot de passe pour un compte doté de droits en lecture sur les objets de l'espace de nom que vous voulez parcourir. La fenêtre est mise à jour avec les informations du système distant.

     Agent Builder tente de découvrir les espaces de nom disponibles sur le serveur CIM. Les espaces de nom reconnus sont affichés dans la liste **Espace de nom**. Toutefois, Agent Builder peut ne pas être à même de détecter tous les espaces de nom disponibles sur le serveur. Si vous souhaitez parcourir un espace de nom qui n'est pas répertorié dans la liste **Espace de nom**, cliquez sur l'icône plus (+) en regard de la liste **Espace de nom**. Entrez le nom de l'espace de nom dans la zone et cliquez sur **OK**. Si l'espace de nom est présent sur le serveur CIM, les classes définies dans l'espace de nom sont listées. Les espaces de nom que vous entrez sont sauvegardés et répercutés dans la liste **Espace de nom** la prochaine fois que vous explorez ce serveur CIM spécifique.

     Lorsqu'un espace de nom est sélectionné dans la liste **Espace de nom**, Agent Builder collecte toutes les informations de classe de cet espace de nom spécifique. Agent Builder met ensuite en mémoire cache ces informations de sorte que vous puissiez passer rapidement d'un espace de nom à l'autre. Si vous souhaitez forcer Agent Builder à re-collecter les informations de classe pour un espace de nom particulier, sélectionnez ce dernier et cliquez sur **Connecter**. Cliquer sur **Connecter** supprime toutes les informations mises en cache et oblige Agent Builder à recollecter les informations de classe.

     Vous pouvez cliquer sur l'icône **Rechercher** (jumelles) pour rechercher votre sélection dans la liste. Entrez une phrase dans la zone **Rechercher une phrase** ; indiquez votre préférence en cliquant sur l'une des zones **Rechercher par nom** ou **Rechercher par propriétés de classe** et cliquez sur **OK**. Si vous trouvez l'élément que vous recherchez, sélectionnez-le et cliquez sur le bouton **OK**.
5. Sur la page Informations sur le modèle CIM, zone **Systèmes d'exploitation**, sélectionnez les systèmes d'exploitation sur lesquels la collecte doit être effectuée.
6. Si vous avez tapé l'espace de nom et le nom de classe CIM dans la zone **Informations sur le modèle CIM**, procédez comme suit :
   a) Cliquez sur **Suivant** pour afficher la page **Information d'attribut** et définir le premier attribut du groupe d'attributs.
   b) Indiquez les informations sur la page d'**Informations d'attribut**, puis cliquez sur **Terminer**.
7. Si vous avez parcouru les informations CIM, la page Sélectionner les attributs clés s'affiche. Sur cette page, sélectionnez des attributs de clé ou indiquez que cette source de données ne génère qu'une seule ligne de données. Pour plus d'informations, voir «Sélection des attributs de clé», à la page 1206.

8. Si vous avez accédé aux informations sur le modèle CIM, cliquez sur **Terminer**.
9. Facultatif : Vous pouvez tester ce groupe d'attributs en cliquant sur **Tester**. Pour plus d'informations sur le test, voir «Test des groupes d'attributs CIM», à la page 1298.
10. Facultatif : Vous pouvez créer un filtre pour limiter les données renvoyées par ce groupe d'attributs en cliquant sur **Avancé**. Pour plus d'informations sur le filtrage de données à partir d'un groupe d'attributs, voir «Filtrage des groupes d'attributs», à la page 1237.
11. Effectuez l'une des opérations suivantes :
    a) Si vous utilisez l'assistant d'**agent**, cliquez sur **Suivant**.
    b) Cliquez sur **Terminer** pour sauvegarder la source de données et ouvrir l'éditeur d'agent.

Configuration de modèle CIM
Informations détaillées sur les propriétés de configuration d'un modèle CIM.

Si vous définissez une source de données CIM dans votre agent, les propriétés de configuration CIM s'ajoutent automatiquement à l'agent. Vous pouvez visualiser, ajouter et modifier les propriétés de configuration à l'aide de l'éditeur d'agent. Pour obtenir des instructions, voir «Modification des propriétés de configuration à l'aide de l'éditeur d'agent», à la page 1407. Si une source de données CIM est définie dans un sous-noeud, indiquez les substitutions de configuration de sous-noeud. Pour obtenir des instructions, voir «Configuration de sous-noeud», à la page 1394.

Les propriétés de configuration suivantes, spécifiques aux connexions, figurent sur la page de configuration de modèle CIM :

Connexion CIM locale ou distante
Authentification locale ou à distance sur le serveur CIM. Valeur par défaut : Distante

ID utilisateur CIM
L'ID utilisateur permettant d'accéder au serveur CIM

Mot de passe CIM
Mot de passe permettant d'accéder au serveur CIM

Nom d'hôte CIM
Nom d'hôte accessible pour les données CIM

CIM sur SSL
Utilisez SSL pour les communications avec le serveur CIM. Les options sont Oui et Non. Valeur par défaut : Non.

Numéro de port CIM
Numéro de port utilisé pour les communications non sécurisées.

Numéro de port SSL CIM
Numéro de port utilisé pour les communications sécurisées. Valeur par défaut : 5989. (La valeur par défaut pour Solaris 8 est normalement différente.)

Test des groupes d'attributs CIM
Vous pouvez tester le groupe d'attributs CIM créé dans Agent Builder.

Procédure

1. Démarrez la procédure de test de l'une des manières suivantes :
   - Lors de la création de l'agent, cliquez sur **Tester** sur la page **Informations CIM**.
   - Après la création de l'agent, sélectionnez un groupe d'attributs à la page **Définition de la source de données** de l'éditeur d'agent et cliquez sur **Tester**. Pour plus d'informations sur l'éditeur d'agent, voir «Utilisation de l'éditeur d'agent pour modifier l'agent», à la page 1207.

   Après avoir cliqué sur **Tester** dans l'une des deux étapes précédentes, la fenêtre **Paramètres de test** s'affiche.
2. Facultatif : Avant de démarrer le test, définissez des variables d'environnement et des propriétés de configuration.

Pour plus d'informations, voir «Test des groupes d'attributs», à la page 1420.

3. Sélectionnez ou ajoutez un **Nom d'hôte**.

   Pour plus d'informations sur l'ajout d'un **Nom d'hôte**, voir «Surveillance de données à partir d'un modèle CIM (Common Information Model)», à la page 1296.

4. Cliquez sur l'option de **démarrage de l'agent**.

   Une fenêtre indique que l'agent est en cours de démarrage.

5. Pour simuler une demande de données d'agent provenant de Tivoli Enterprise Portal ou de SOAP, cliquez sur **Collecte de données**.

   L'agent demande les données au serveur CIM. La fenêtre **Paramètres de test** collecte et affiche toutes les données du cache de l'agent depuis son dernier démarrage.

6. Facultatif : Cliquez sur **Vérifier les résultats** si les données renvoyées ne sont pas celles que vous attendez.

   La fenêtre **Statut de la collecte de données** affiche des informations supplémentaires sur les données. Les données collectées et affichées dans la fenêtre **Statut de la collecte de données** sont décrites dans «Noeud de statut d'objet de performances», à la page 1466.

7. Arrêtez l'agent en cliquant sur **Arrêter l'agent**.
8. Cliquez sur **OK** ou sur **Annuler** pour quitter la fenêtre **Tester les paramètres**. Cliquez sur **OK** pour sauvegarder les modifications que vous avez apportées.

Concepts associés

«Test de votre agent dans Agent Builder», à la page 1420
Après avoir utilisé Agent Builder pour créer un agent, vous pouvez tester l'agent dans Agent Builder.

Surveillance d'un fichier journal

Vous pouvez définir une source de données pour qu'elle reçoive les données d'un fichier journal. L'agent analyse régulièrement les lignes ajoutées dans le fichier journal et génère les informations liées aux événements sur la base de ces lignes. Vous pouvez configurer la manière dont l'agent traduit le journal en événements. Vous pouvez également le configurer de manière à filtrer et récapituler les données. Les événements en résultant sont placés dans un ensemble de données.

Avant de commencer

Remarque : L'agent surveille des fichiers journaux qui se trouvent dans le même environnement local et la même page de codes où l'agent s'exécute.

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, cliquez sur **Données consignées** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **Un fichier journal**.
3. Cliquez sur **Suivant**.
4. Sur la page **Informations sur le fichier journal**, entrez le nom du fichier journal que vous voulez contrôler dans la zone **Informations sur le fichier journal**.

   Le nom de fichier doit être complet.

   a) Facultatif : Une partie du nom du fichier journal peut provenir d'une propriété de la configuration d'exécution. Pour créer un nom de fichier journal, cliquez sur **Insérer une propriété de configuration** et sélectionnez une propriété de configuration.

   b) Facultatif : Le fichier peut aussi être un nom de fichier dynamique . Pour plus d'informations, voir «Prise en charge des noms de fichier dynamiques», à la page 1544.

5. Dans la zone **Identification de zone**, cliquez sur une des options suivantes :

   Nombre de caractères fixe
   Lorsque cette option est sélectionnée, elle limite le nombre de caractères.

Avec cette option, chaque attribut est affecté au nombre maximal de caractères qu'il peut détenir provenant du fichier journal. Par exemple, s'il existe trois attributs A, B, et C (dans cet ordre) et que chaque attribut est une chaîne d'une longueur maximale de 20. Ensuite, les 20 premiers octets de l'enregistrement de journal vont dans l'attribut A, les 20 suivants dans l'attribut B et les 20 suivants dans l'attribut C.

Séparateur de tabulation
Lorsque cette option est sélectionnée, vous pouvez utiliser des séparateurs de tabulation.

Séparateur espace
Lorsque cette option est sélectionnée, plusieurs espaces simultanés peuvent être utilisés comme séparateurs uniques.

Texte de séparateur
Si sélectionné, saisissez le texte du séparateur.

Textes de début et de fin
Si sélectionné, saisissez les textes de début et de fin.

XML dans l'élément
Lorsque cette option est sélectionnée, entrez le nom de l'élément XML à utiliser comme enregistrement, ou cliquez sur **Parcourir** pour définir l'élément.

Si vous avez cliqué sur **Parcourir**, la fenêtre **Navigateur XML** apparaît. Si vous utilisez la fonctionnalité Parcourir, Agent Builder identifie tous les attributs possibles de l'enregistrement en consultant les balises enfant et leurs attributs.

Remarque : A moins que vous ne cliquiez sur **Avancé** pour entrer les informations dans cette fenêtre, les hypothèses retenues sur les informations que vous fournissez sont les suivantes :

- Seul un fichier journal est surveillé à la fois.
- Chaque ligne du fichier journal comporte toutes les zones nécessaires pour entrer les attributs à définir.

Pour plus d'informations sur l'analyse syntaxique des fichiers journaux et les séparateurs, voir («Analyse syntaxique et séparateurs de fichiers journaux», à la page 1308).

6. Facultatif : Cliquez sur **Avancé** dans la page **Informations sur le fichier journal** pour effectuer les opérations suivantes à l'aide de la page **Propriétés avancées de la source de données** :
   - Surveiller plusieurs fichiers à la fois ou surveiller des fichiers avec des noms différents sur des systèmes d'exploitation différents ou surveiller des noms de fichier correspondant à des expressions régulières.
   - Dessiner un ensemble de zones à partir de plusieurs lignes dans le fichier journal.
   - Choisir des **options de filtrage et de récapitulatif des événements**.
   - Générer des informations récapitulatifs de sortie. Ce récapitulatif génère un groupe d'attributs supplémentaire à chaque intervalle. Pour plus d'informations sur ce groupe d'attributs, voir «Synthèse du fichier journal», à la page 1477. Cette fonction est remplacée par les options disponibles dans l'onglet Informations sur les événements.

   a) Pour surveiller plusieurs fichiers journaux, cliquez sur **Ajouter** et entrez le nom.

   Si plusieurs fichiers sont indiqués, un libellé unique doit être entré pour chaque fichier. Le libellé peut être affiché comme un attribut pour indiquer quel fichier a généré l'enregistrement. Il ne doit pas comporter d'espaces.

   b) Facultatif : Pour sélectionner les systèmes d'exploitation sur lesquels chaque fichier journal sera surveillé, procédez comme suit :

      1) Cliquez dans la colonne **Systèmes d'exploitation** qui correspond au fichier journal.
      2) Cliquez sur **Editer**.
      3) Dans la fenêtre **Systèmes d'exploitation**, sélectionnez les systèmes d'exploitation.
      4) Cliquez sur **OK** pour sauvegarder vos modifications et revenir à la page **Propriétés avancées de la source de données**.

c) Facultatif : Sélectionnez **Les noms de fichier correspondent à l'expression régulière** si le nom de fichier que vous indiquez est une expression régulière servant à rechercher le fichier à la place d'un nom de fichier.

Pour plus d'informations, voir «Expressions régulières ICU», à la page 1534. Si vous ne cochez pas cette case, le nom doit être un nom réel. Sinon, il doit s'agir d'un modèle qui suit les règles des modèles de nom de fichier décrites dans «Syntaxe de nom de fichier dynamique», à la page 1545.

d) Facultatif : Sélectionnez **Un élément du répertoire correspond à l'expression régulière** pour faire correspondre un sous-répertoire du chemin du nom de fichier à une expression régulière.

Vous ne pouvez sélectionner cette option que si vous avez également sélectionné **Les noms de fichier correspondent à l'expression régulière** à l'étape précédente.

Si des métacaractères sont utilisés dans le nom de chemin, ils ne peuvent être utilisés que dans un seul sous-répertoire du chemin. Par exemple, vous pouvez spécifier `/var/log/[0-9\.]*/journal.*` pour avoir des métacaractères dans un sous-répertoire. La chaîne `[0-9\.]*` fait correspondre les sous-répertoire de `/var/log` comportant uniquement des chiffres et des points `(.)`. La chaîne `mylog.*` fait correspondre les noms des fichiers des sous répertoires `/var/log` qui commencent par le mot `journal` et suivis de zéro caractère ou plus.

Etant donné que certains systèmes d'exploitation utilisent la barre oblique inversée `(\)` comme séparateur de répertoire, il peut être confondu avec un métacaractère d'échappement d'expression régulière. C'est pourquoi les barres obliques doivent toujours être utilisées pour désigner des répertoires. Par exemple, les fichiers Windows qui sont spécifiés sous la forme `C:\temp\mylog. *` peuvent signifier que le `\t` est un caractère de tabulation abrégé. Par conséquent, utilisez toujours des barres obliques `(/)` comme séparateurs de répertoire sur tous les systèmes d'exploitation. L'exemple `C:/temp/journal.*` représente tous les fichiers du répertoire `C:/temp` qui commencent par `journal`.

e) Dans la liste **Lorsque plusieurs fichiers correspondent**, sélectionnez une des options suivantes :

- **Le fichier dont le nom comporte la valeur numérique la plus élevée**
- **Le fichier le plus volumineux**
- **Le fichier mis à jour le plus récemment**
- **Le fichier créé le plus récemment**
- **Tous les fichiers correspondants**

Remarque : Lorsque vous sélectionnez **Tous les fichiers correspondants**, l'agent identifie tous les fichiers du répertoire qui correspondent au modèle de nom de fichier dynamique. L'agent surveille les mises à jour de tous les fichiers en parallèle. Les données de tous les fichiers sont entremêlées durant le processus de collecte de données. Il est donc préférable d'ajouter un attribut en sélectionnant **Nom du fichier journal** dans la zone **Informations sur la zone de l'enregistrement** pour corréler les messages de journaux aux fichiers journaux qui contiennent ces messages. Vérifiez que tous les fichiers qui correspondent au modèle de nom de fichier dynamique peuvent être scindés, de manière cohérente, en attributs. Si les fichiers journaux sélectionnés ne peuvent pas être analysés de manière cohérente, il est préférable de sélectionner **Enregistrement complet** dans la zone **Informations sur la zone de l'enregistrement** pour définir un attribut unique. Pour plus d'informations sur la spécification des attributs dans la zone **Informations sur la zone de l'enregistrement**, voir l'étape («8», à la page 1303).

f) Choisissez le traitement du fichier.

L'option **Traiter tous les enregistrements lorsque le fichier est échantillonné** permet le traitement de tous les enregistrements du fichier complet chaque fois que l'intervalle d'échantillonnage défini pour la surveillance du journal expire. L'intervalle par défaut est de 60 secondes. Il peut être modifié à l'aide de la variable d'environnement *KUMP_DP_COPY_MODE_SAMPLE_INTERVAL* (valeur indiquée en secondes). Les mêmes enregistrements sont signalés chaque fois sauf s'ils sont supprimés du fichier. Avec cette sélection, les données d'événements ne sont pas produites lorsque de nouveaux enregistrements sont écrits dans le fichier. L'option **Traiter les nouveaux enregistrements ajoutés au fichier** permet de traiter les nouveaux enregistrements ajoutés au fichier pendant que l'agent est en

cours d'exécution. Un enregistrement d'événement est généré pour chaque enregistrement ajouté au fichier. Si le fichier est remplacé (le premier enregistrement change de toute manière), la totalité du fichier est traitée et un événement est généré pour chaque enregistrement du fichier.

Remarque : Si vous ajoutez des enregistrements dans un fichier journal XML, ces enregistrements doivent contenir un jeu complet des éléments définis au sein de l'élément XML sélectionné comme **Identification de zone**.

g) Si vous choisissez de traiter les nouveaux enregistrements attachés au fichier, vous pouvez également choisir la manière dont sont détectés les nouveaux enregistrements.

L'option **Détecter les nouveaux enregistrements lorsque le nombre d'enregistrements augmente** permet aux nouveaux enregistrements d'être détectés lorsque le nombre d'enregistrements du fichier augmente, que la taille du fichier augmente ou pas. Cette fonction est utile lorsque la totalité d'un fichier journal est préallouée avant que les enregistrements ne soient écrits dans le fichier. Vous pouvez sélectionner cette option pour les fichiers qui ne sont pas préalloués, mais elle est moins efficace que la surveillance de la taille du fichier. L'option **Détecter les nouveaux enregistrements lorsque la taille du fichier augmente** permet de déterminer de façon classique à quel moment une nouvelle entrée est ajoutée dans un fichier. Le remplacement d'un fichier surveillé peut être détecté avec un léger retard.

h) Si vous avez sélectionné **Détecter les nouveaux enregistrements lorsque la taille du fichier augmente**, vous pouvez également choisir le mode de traitement d'un fichier qui existe lorsque l'agent de surveillance démarre.

L'option **Ignorer les enregistrements existants** désactive la production d'événements pour tout enregistrement du fichier au démarrage de l'agent. L'option **Traiter___ enregistrements existants à partir du fichier** indique la production d'un événement pour un nombre fixe d'enregistrements depuis la fin du fichier au démarrage de l'agent. L'option **Traiter les enregistrements non précédemment traités par l'agent** permet aux données de redémarrage d'être conservées par l'agent de surveillance afin que l'agent sache les enregistrements qui ont été traités la dernière fois qu'il s'est exécuté. Les événements sont générés pour tout enregistrement attaché au fichier depuis la dernière exécution de l'agent. Cette option implique un peu de temps supplémentaire chaque fois qu'un enregistrement est ajouté au fichier.

i) Si vous avez sélectionné **Traiter les enregistrements non précédemment traités par l'agent**, vous pouvez choisir ce qu'il faut faire au démarrage de l'agent et lorsqu'il apparaît que le fichier existant a été remplacé.

Traiter tous les enregistrements si le fichier a été remplacé : si les informations sur le fichier surveillé et les informations des données de redémarrage ne correspondent pas, les événements sont générés pour tous les enregistrements du fichier. Exemples de non-concordance : le nom du fichier ou l'heure de création du fichier sont différents, la taille du fichier a diminué, ou bien l'heure de la dernière modification du fichier est antérieure à ce qu'elle était. L'option **Ne pas traiter les enregistrements si le fichier a été remplacé** désactive le traitement des enregistrements existants dans le fichier si les informations concernant le fichier surveillé et les informations des données de redémarrage ne correspondent pas.

j) Cliquez sur l'onglet **Identification de l'enregistrement** pour traiter plusieurs lignes du fichier journal comme un enregistrement logique unique.

Remarque : L'onglet **Identification de l'enregistrement** ne s'affiche pas si vous sélectionnez **XML dans l'élément** comme identification de zone sur la page **Informations sur le fichier journal**.

- **Ligne unique** interprète chaque ligne comme un enregistrement logique unique.
- **Ligne de séparateur** permet d'entrer une séquence de caractères identifiant une ligne séparant deux enregistrements.

  Remarque : La ligne de séparateur ne fait ni partie de l'enregistrement précédent, ni partie de l'enregistrement suivant.
- **Règle** permet d'indiquer le nombre maximal de lignes constituant un enregistrement et, si vous le souhaitez, une séquence de caractères marquant le début ou la fin d'un enregistrement. Avec l'option **Règle**, vous pouvez définir les propriétés suivantes :

- **Ligne de données non vide maximum** : définit le nombre maximal de lignes non vides pouvant être traitées par une règle.
- **Type de règle** : valeurs possibles :
  - **Aucune comparaison de texte** (le nombre maximal de lignes par enregistrement indique un enregistrement logique unique).
  - **Identifier le début de l'enregistrement** : marque le début de l'enregistrement logique unique.
  - **Identifier la fin de l'enregistrement** : marque la fin de l'enregistrement logique unique.
- **Décalage** indique l'emplacement au sein d'une ligne où la chaîne de comparaison doit apparaître.
- **Test de comparaison** peut prendre la valeur **Egal à**, ce qui requiert qu'une séquence de caractères corresponde au décalage spécifié ou **Non égal à**, ce qui indique qu'une séquence particulière de caractères n'apparaît pas au décalage spécifié.
- **Chaîne de comparaison** définit la séquence de caractères à comparer.

• **Expression régulière** identifie un modèle utilisé pour indiquer le début ou la fin d'un enregistrement. Grâce à l'option **Expression régulière**, vous pouvez définir les propriétés suivantes :

- **Chaîne de comparaison** définit la séquence de caractères sur la base de laquelle doit être établie la correspondance.

  OU

- Début ou fin d'un enregistrement :
  - **Identifier le début de l'enregistrement** marque le début de l'enregistrement logique unique.
  - **Identifier la fin de l'enregistrement** marque la fin de l'enregistrement logique unique.

k) Si vous avez sélectionné **Traiter tous les enregistrements lorsque le fichier est échantillonné**, cliquez sur l'onglet **Expression de filtrage**. Si vous cliquez sur **Expression de filtrage**, vous pouvez filtrer les données qui sont renvoyées sous forme de lignes en fonction des valeurs d'un ou de plusieurs attributs, variables de configuration ou les deux.

Si vous avez sélectionné **Traiter les nouveaux enregistrements attachés au fichier**, vous ne pouvez pas créer d'expression de filtrage. Pour plus d'informations sur le filtrage des données à partir d'un groupe d'attributs, voir («Filtrage des groupes d'attributs», à la page 1237).

l) Si vous avez sélectionné **Traiter les nouveaux enregistrements attachés au fichier**, cliquez sur l'onglet **Informations sur les événements** pour sélectionner les **Options de filtrage et de récapitulatif des événements**.

Pour plus d'informations, voir «Filtrage et récapitulatif des événements», à la page 1449.

Remarque : L'onglet Récapitulatif peut être présent si l'agent a été créé avec une version antérieure d'Agent Builder. L'onglet Récapitulatif a été rendu obsolète par l'onglet Informations sur les événements.

7. Facultatif : Cliquez sur **Paramètres de fichier journal test** sur la page **Informations sur le fichier journal** pour démarrer et tester la source de données . Cliquez sur **Paramètres de fichier journal test** après avoir sélectionné les options de la source de journal. Lorsque vous testez la source de données de fichier journal et indiquez du contenu, Agent Builder crée les attributs du groupe automatiquement, sur la base des résultats de l'analyse du journal. Pour plus d'informations sur la procédure de test, voir «Test des groupes d'attributs de fichier journal», à la page 1310.
8. Si vous n'avez pas utilisé la fonction de test précédemment et que vous avez tapé le nom du fichier journal dans la zone **Informations sur le fichier journal** de la page **Informations sur le fichier journal**, procédez comme suit :
   a) Cliquez sur **Suivant** pour afficher la page **Information d'attribut** et définir le premier attribut du groupe d'attributs.
   b) Spécifiez les informations sur la page **Information d'attribut**, puis cliquez sur **Terminer**.

Remarque : Lorsqu'un groupe d'attributs du fichier journal est ajouté à un agent à la version minimale par défaut de Tivoli Monitoring 6.2.1 ou une version ultérieure, un groupe d'attributs `Statut du fichier journal` est inclus. Pour plus d'informations sur le groupe d'attributs `Statut du fichier journal`, voir («Groupe d'attributs de statut du fichier journal», à la page 1508).

Outre les zones applicables à toutes les sources de données, la page **Information d'attribut** de la source de données du fichier journal contient des zones supplémentaires dans la zone **Informations sur la zone d'enregistrement**.

Les zones **Informations sur la zone d'enregistrement** sont :

Zone suivante
Affiche la zone après l'analyse syntaxique, en utilisant les délimiteurs du groupe d'attributs (ou des délimiteurs spéciaux de cet attribut provenant de la boîte de dialogue Avancé).

Reste de l'enregistrement
Affiche le reste de l'enregistrement une fois que les attributs précédents ont été analysés. Cet attribut est le dernier attribut, à l'exception, éventuellement, du nom ou du libellé du fichier journal.

Enregistrement complet
Affiche la totalité de l'enregistrement, ce qui peut correspondre au seul attribut, à l'exception, éventuellement, du nom ou du libellé du fichier journal.

Nom du fichier journal
Affiche le nom du fichier journal.

Libellé du fichier journal
Affiche le libellé affecté au fichier dans le panneau Avancé.

Remarque : Utilisez l'onglet **Détails de l'attribut dérivé** uniquement si vous voulez un attribut dérivé et non un attribut issu directement du fichier journal.

9. Cliquez sur **Avancé** dans la zone **Informations sur la zone d'enregistrement** pour afficher la page **Informations d'attribut avancées du fichier journal**.
   a) Dans la section **Filtres d'attribut**, indiquez les critères pour les données à inclure ou à exclure.

      Le filtrage des attributs peut améliorer les performances de votre solution en réduisant la quantité de données traitées. Cliquez sur un ou plusieurs des filtres d'attribut suivants :

      - **Inclusif** indique que l'ensemble de filtres d'attribut définis est un filtre d'acceptation ; en d'autres termes, si l'ensemble de filtres aboutit, l'enregistrement franchit le filtre et il est généré.
      - **Exclusif** indique que l'ensemble de filtres d'attribut définis est un filtre de rejet ; en d'autres termes, si l'ensemble de filtres d'attribut aboutit, l'enregistrement est rejeté et n'est pas généré.
      - **Correspondance avec tous les filtres** indique que tous les filtres définis pour l'ensemble de filtres doivent correspondre à l'enregistrement d'attribut de sorte que l'ensemble de filtres aboutisse.
      - **Correspondance avec un filtre quelconque** indique que, si un des filtres définis pour l'ensemble de filtres correspond à l'enregistrement d'attribut, l'ensemble de filtres aboutit.

   b) Utilisez **Ajouter**, **Modifier** et **Supprimer** pour définir les filtres individuels d'un ensemble de filtres d'attribut.

   c) Pour ajouter un filtre, procédez comme suit :

      1) Cliquez sur **Ajouter**, puis complétez les options de la fenêtre **Ajouter un filtre** en procédant comme suit :

         a) La section **Critères de filtrage** définit les caractéristiques de base du filtre, y compris les propriétés suivantes :

            - **Décalage de début** définit l'emplacement dans la chaîne d'attribut où la comparaison doit commencer.

- **Chaîne de comparaison** définit le modèle de chaîne par rapport auquel l'attribut est défini.

  Entrez un modèle de chaîne ou une expression régulière utilisée par l'agent pour filtrer les données lues dans le fichier. Les enregistrements correspondant au modèle de filtre sont supprimés des enregistrements renvoyés à l'environnement de surveillance ou ils sont les seuls enregistrements renvoyés. Le résultat varie selon que vous décidez que le filtre est inclusif ou exclusif.
- **Correspondance avec la valeur totale** : recherche une occurrence exacte de la chaîne de comparaison dans la chaîne d'attribut. La vérification démarre à la position de décalage de début.
- **Correspondance avec une partie quelconque de la valeur** ; recherche la chaîne de comparaison n'importe où dans la chaîne d'attribut. La vérification démarre à la position de décalage de début.

b) **La chaîne de comparaison est une expression régulière** : indique que la chaîne de comparaison est un modèle d'expression régulière pouvant être appliqué à la chaîne d'attribut.

   Le filtrage d'expression régulière est pris en charge via des bibliothèques ICU (International Components for Unicode) pour vérifier si la valeur d'attribut examinée correspond ou non au modèle indiqué.

   Pour utiliser efficacement la prise en charge des expressions régulières, vous devez savoir comment ICU implémente les expressions régulières. Cette méthode diffère du mode d'implémentation de la prise en charge des expressions régulières dans les expressions régulières `Perl`, `grep`, `sed` et Java, et d'autres implémentations. Voir «Expressions régulières ICU», à la page 1534 pour plus d'informations sur la création de filtres d'expression régulière.

c) **Définir un filtre de substitution** indique que vous souhaitez fournir une comparaison par filtrage plus spécifique, qui remplace les caractéristiques de base précédemment définies. Cette chaîne de comparaison supplémentaire est utilisée pour inverser le résultat de filtrage. Lorsque le filtre est de type **Inclusif**, l'opération de remplacement agit comme un qualificateur d'exclusion pour l'expression de filtrage. Lorsque le filtre est de type **Exclusif**, l'opération de remplacement agit comme un qualificateur d'inclusion pour l'expression de filtrage. (Pour plus d'informations sur **Inclusif** et **Exclusif**, consultez l'étape «9», à la page 1304, ainsi que les exemples qui suivent). Le filtre de substitution a les propriétés suivantes :

   - **Décalage de début** définit l'emplacement dans la chaîne d'attribut où la comparaison doit commencer.
   - **Chaîne de comparaison** définit le modèle de chaîne auquel l'attribut doit satisfaire.

     Entrez une expression régulière qui sera utilisée par l'agent pour filtrer les données lues à partir du fichier. Les enregistrements correspondant au modèle de filtre sont supprimés des enregistrements renvoyés à l'environnement de surveillance ou ils sont les seuls enregistrements renvoyés. Le résultat varie selon que vous décidez que le filtre est inclusif ou exclusif.

d) **Valeur de remplacement** permet de remplacer la chaîne d'attribut brute par une nouvelle valeur. Voir «Expressions régulières ICU», à la page 1534 pour plus d'informations sur les caractères spéciaux pouvant être utilisés.

e) **Remplacer la première occurrence** remplace par un nouveau texte la première occurrence appariée par la chaîne de comparaison.

f) **Remplacer toutes les occurrences** remplace par un nouveau texte toutes les occurrences appariées par la chaîne de comparaison.

2) Cliquez sur **OK**.

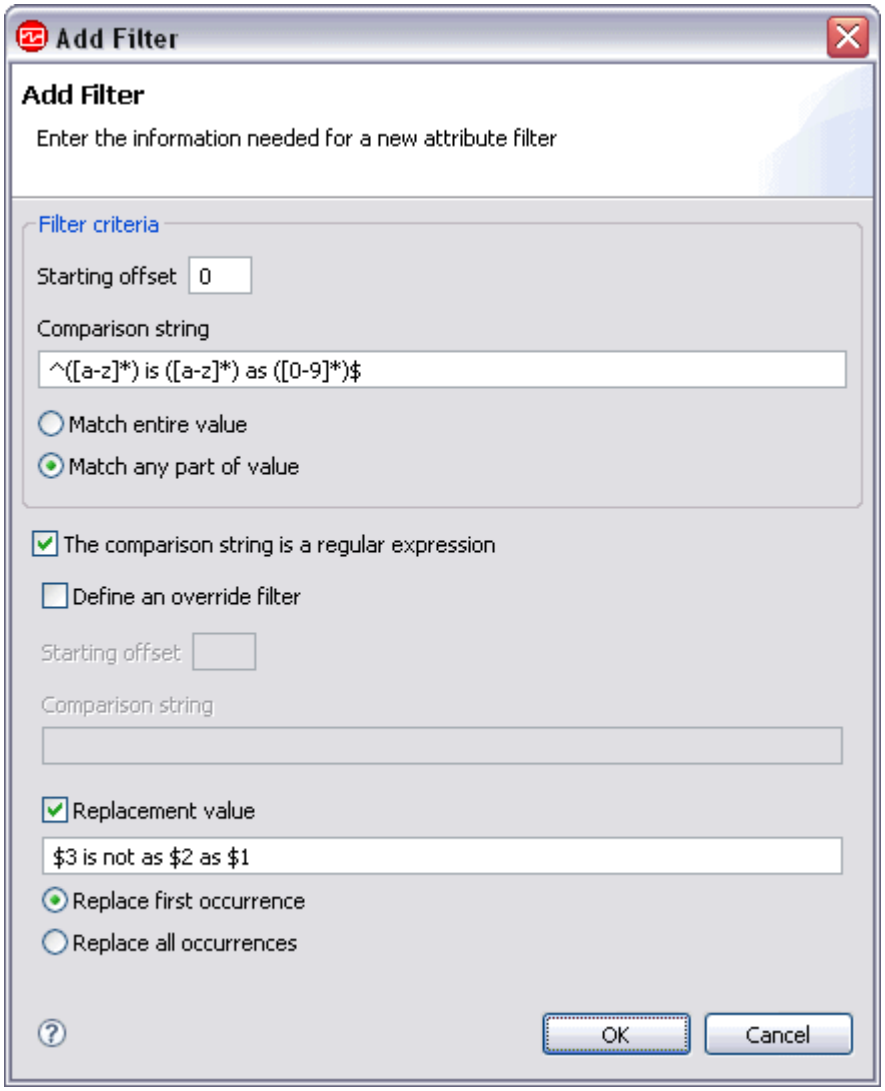


*Figure 38. **Ajouter un filtre** - Exemple 1*

Si la chaîne d'attribut est `abc is easy as 123` (abc est aussi simple que 123), la chaîne remplacée qui est affichée dans Tivoli Enterprise Portal ou dans la console IBM Cloud Application Performance Management est `123 is not easy as abc` (123 n'est pas aussi simple que abc).

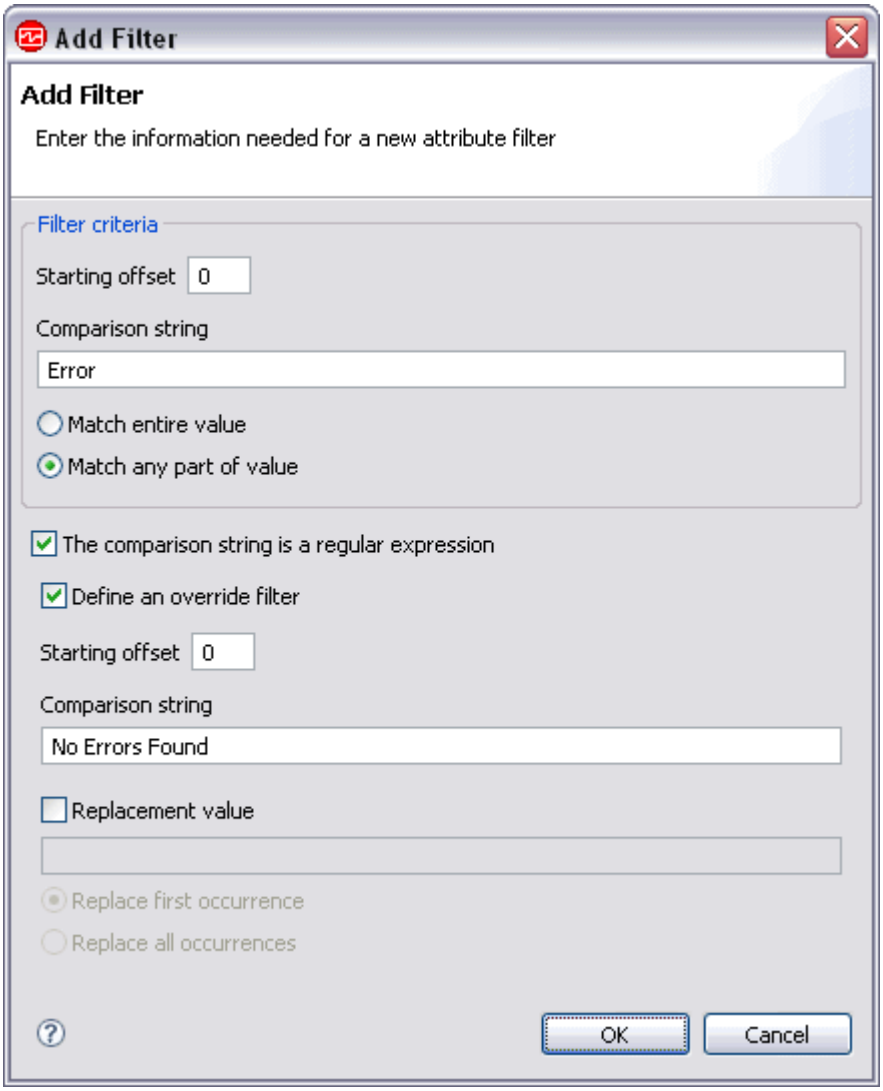


*Figure 39. **Ajouter un filtre** - Exemple 2*

Si la chaîne d'attribut est `Unrecoverable Error reading from disk` et que le filtre est de type **Inclusif**, l'attribut s'affiche dans Tivoli Enterprise Portal ou dans la console IBM Cloud Application Performance Management. Si la chaîne d'attribut est `Aucune erreur détectée lors de la sauvegarde hebdomadaire` et que le filtre est de type **Inclusif**, l'attribut ne s'affiche pas.

d) Dans la section **Identification de zone** de la page **Informations d'attribut avancées du fichier journal**, indiquez comment remplacer les délimiteurs de zone du groupe d'attributs pour ce seul attribut. Cliquez sur un des filtres d'attribut, puis complétez les zones requises pour l'option :

- **Nombre de caractères** : Entrez la valeur limite du nombre de caractères.
- **Séparateur de tabulation** indique l'utilisation de séparateurs de tabulation.
- **Texte de séparateur** : Entrez le texte de séparateur que vous souhaitez utiliser.
- **Textes de début et de fin** : Entrez le texte de **début** et le texte de **fin**.

e) Dans la section **Récapitulatif** de la page **Informations d'attribut avancées de fichier journal**, cochez la case **Inclure l'attribut dans le groupe d'attributs récapitulatif** pour ajouter l'attribut dans le groupe d'attributs récapitulatif.

Ce groupe d'attributs est généré lorsqu'un utilisateur active la synthèse d'attributs de journal.

f) Cliquez sur **OK**.

10. Si vous avez utilisé la fonction de test à l'étape («7», à la page 1303), la page **Sélectionner les attributs clés** s'affiche. Sur la page **Sélectionner les attributs clés**, sélectionnez les attributs de clé ou indiquez que la source de données génère uniquement une ligne de données.

    Pour plus d'informations, voir «Sélection des attributs de clé», à la page 1206.
11. Effectuez l'une des opérations suivantes :
    - Si vous utilisez l'assistant de création d'agent, cliquez sur **Suivant**.
    - Cliquez sur **Terminer** pour sauvegarder la source de données et ouvrir l'éditeur d'agent.

    Remarque : Lorsqu'un groupe d'attributs du fichier journal est ajouté à un agent qui possède la version minimale par défaut de Tivoli Monitoring 6.2.1 ou une version ultérieure, un groupe d'attributs `Statut du fichier journal` est inclus. Pour plus d'informations sur le groupe d'attributs `Statut du fichier journal`, voir («Groupe d'attributs de statut du fichier journal», à la page 1508).

Analyse syntaxique et séparateurs de fichiers journaux
Vous pouvez modifier le séparateur par défaut utilisé pour séparer un ou plusieurs attributs dans un enregistrement de fichier journal.

Lorsque vous créez un groupe d'attributs de fichier journal, un séparateur est affecté par défaut. Le séparateur par défaut est un onglet. Le séparateur est utilisé par l'agent pour analyser et délimiter les données pour chaque attribut dans la ligne de données. Vous pouvez remplacer le séparateur d'attribut par défaut par :

- Un nombre fixe de caractères
- Une espace
- Un ou des caractères différents
- Un texte de début et de fin spécifique
- Un élément XML

Vous pouvez modifier le séparateur par défaut utilisé pour tous les attributs du groupe de plusieurs façons :

1. Lors de la création du groupe d'attributs, sur la page **Informations sur le fichier journal**.
2. Après la création du groupe d'attributs, en ouvrant l'onglet **Editeur d'agent** > **Sources de données**, en sélectionnant le groupe d'attributs et en choisissant un séparateur dans la zone **Identification de zone**.

Vous pouvez également affecter des séparateurs spécifiques à un ou plusieurs attributs pris séparément. Vous pouvez affecter des séparateurs spécifiques pour les attributs individuels pour utiliser :

- Un nombre fixe de caractères
- Un séparateur d'onglet
- Un séparateur d'espace
- Un ou des caractères différents
- Un texte de début et de fin spécifique

Vous pouvez modifier le séparateur utilisé pour les attributs individuels de plusieurs façons :

1. En sélectionnant **Avancé** sur la page **Informations d'attribut** lorsque vous créez un attribut.
2. En ouvrant l'onglet **Editeur d'agent** > **Sources de données** et en sélectionnant l'attribut, puis **Avancé** dans l'onglet **Informations d'attribut du fichier journal**.

Exemple 1 - Sortie de fichier journal simple

Certains enregistrements de fichier journal comprennent des séparateurs clairs et ordinaires, par exemple :

```
un, deux, trois
```

Ici, le caractère " , " est un séparateur clair et ordinaire entre les trois éléments de données sur la ligne. Dans ce cas, sélectionnez **Texte comme séparateur**, puis indiquez " , " comme séparateur par défaut pour le groupe d'attributs. Il n'est pas nécessaire de modifier ou de définir d'autres séparateurs.

L'effet de la définition de ce séparateur pour un fichier journal qui contient les lignes de données indiquées précédemment dans cet exemple, est indiqué dans la sortie suivante :

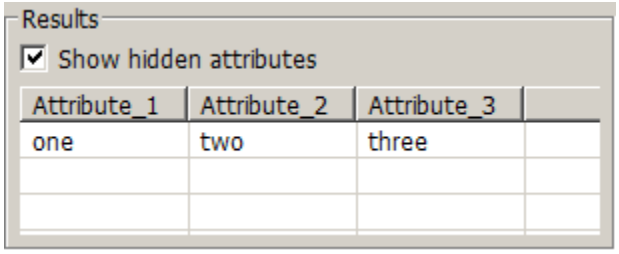


Figure 40. Exemple de sortie de valeur d'attribut lorsque l'agent analyse une ligne de données simple de fichier journal.

Exemple 2 - Sortie complexe de fichier journal

Certains fichiers journaux peuvent contenir des lignes de données qui ont des séparateurs irréguliers ou variables, par exemple :

```
un, deux, trois, [quatre] 12:42, cinq
```

Dans cet exemple, vous pouvez affecter des séparateurs à des définitions d'attribut comme suit :

1. Dans l'exemple précédent, vous avez défini le séparateur par défaut sur " , ". Ce séparateur est utilisé pour tous les attributs sauf si vous l'avez remplacé par un séparateur spécifique. Dans cet exemple, le séparateur par défaut " , " peut être réutilisé pour les trois premiers attributs de la ligne.
2. Examinons le quatrième attribut. Supposons que la chaîne entre "[" et "]" soit une valeur que vous souhaitez extraire. Dans ce cas, lorsque vous définissez le quatrième attribut, vous devez définir un type de séparateur **Textes de début et de fin** avec les valeurs de texte de début et de fin suivantes : "[" et "]".
3. Pour le cinquième attribut, supposez que vous devez extraire les valeurs entre les caractères "]" et " : ". Dans ce cas, lorsque vous définissez le cinquième attribut, vous devez affecter le type de séparateur **Texte comme séparateur** défini sur " : ".
4. Pour le sixième attribut, votre séparateur de groupe d'attributs par défaut " , " convient également.
5. Pour le septième attribut, vous n'avez pas besoin de spécifier un séparateur, car il s'agit du dernier attribut.

L'effet de la définition de ces séparateurs pour un fichier journal qui contient les lignes de données indiquées précédemment dans cet exemple, est indiqué dans la sortie suivante :

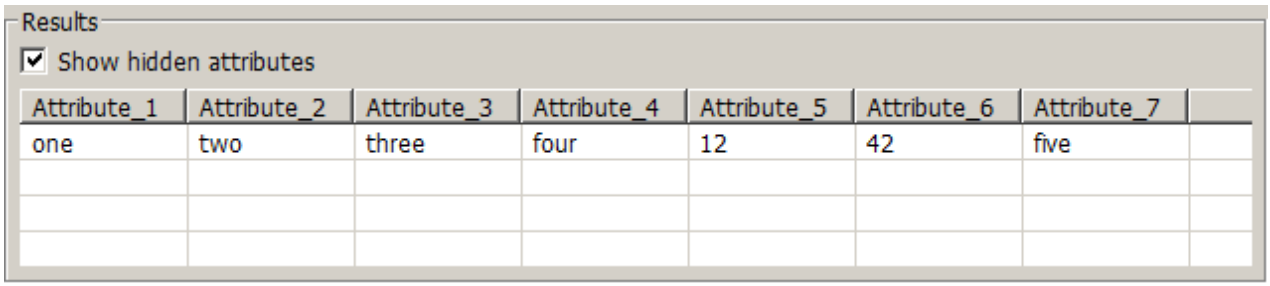


Figure 41. Exemple de sortie de valeur d'attribut lorsque l'agent analyse une ligne de données complexe de fichier journal.

La procédure de définition des séparateurs d'attribut est décrite à l'étape «5», à la page 1299 de «Surveillance d'un fichier journal», à la page 1299.

Test des groupes d'attributs de fichier journal

Vous pouvez utiliser Agent Builder pour tester l'ensemble des données du fichier journal (groupe d'attributs) que vous avez créé. Si aucun attribut n'est défini pour le groupe, la procédure de test les définit automatiquement.

Avant de commencer

Si des attributs sont déjà définis pour ce fichier et que vous voulez définir des attributs automatiquement pendant le test, employez l'éditeur d'agent pour supprimer tous les attributs existants de l'ensemble de données. Pour plus d'informations, voir «Suppression d'attributs», à la page 1231.

Procédure

1. Vous pouvez démarrer la procédure de test de l'une des manières suivantes :
   - Lors de la création de l'agent, cliquez sur **Paramètres de fichier journal test** sur la page **Informations sur le fichier journal**.
   - Après la création de l'agent, sélectionnez un groupe d'attributs à la page **Définition de la source de données** de l'éditeur d'agent et cliquez sur **Paramètres de fichier journal test**. Pour plus d'informations sur l'éditeur d'agent, voir «Utilisation de l'éditeur d'agent pour modifier l'agent», à la page 1207.

   Lorsque vous cliquez sur **Paramètres du fichier journal test** dans l'une des deux étapes précédentes, la fenêtre **Analyser le journal** s'affiche.
2. Sélectionnez la source des données de journal pour le test :
   - **Utiliser les paramètres du groupe d'attributs** : utilisez le nom de fichier et l'emplacement indiqués dans la source de données. Par défaut, la source de données traite seulement les informations qui sont ajoutées au fichier journal après que la procédure de test est commencée. Vous pouvez utiliser cette option si le fichier journal est mis à jour en temps réel.
   - **Spécifier un fichier exemple** : fournissez un exemple de fichier journal. Avec ce paramètre, la procédure de test fait une analyse syntaxique de tout le contenu du fichier journal. Avec cette option, vous pouvez tester la source de données et créer ses attributs immédiatement, en fonction d'un échantillon existant. Indiquez le chemin d'accès et le nom du fichier dans la zone **Nom du fichier journal** ou utilisez le bouton **Parcourir** pour sélectionner le fichier.
3. Facultatif : Avant de démarrer le test, vous pouvez définir des variables d'environnement et des propriétés de configuration.

   Pour plus d'informations, voir «Test des groupes d'attributs», à la page 1420.
4. Cliquez sur l'option de **démarrage de l'agent**.

   Une fenêtre indique que l'agent est en cours de démarrage. Lorsque l'agent démarre, il surveille le fichier journal configuré pour identifier les nouveaux enregistrements.
5. Pour tester la collecte de données de votre agent, générez de nouveaux enregistrements dans le fichier journal surveillé.

   Lorsque de nouveaux enregistrements sont ajoutés au fichier journal, l'agent les analyse en fonction de sa configuration et met à jour les valeurs d'attributs correspondantes dans son cache.
6. Pour simuler une demande de données d'agent provenant de Tivoli Enterprise Portal ou de SOAP, cliquez sur **Collecte de données**.

   La fenêtre **Analyser le journal** collecte et affiche toutes les nouvelles valeurs d'attribut présentes dans le cache de l'agent depuis son dernier démarrage. Un exemple de collecte de données est présenté dans Figure 42, à la page 1311

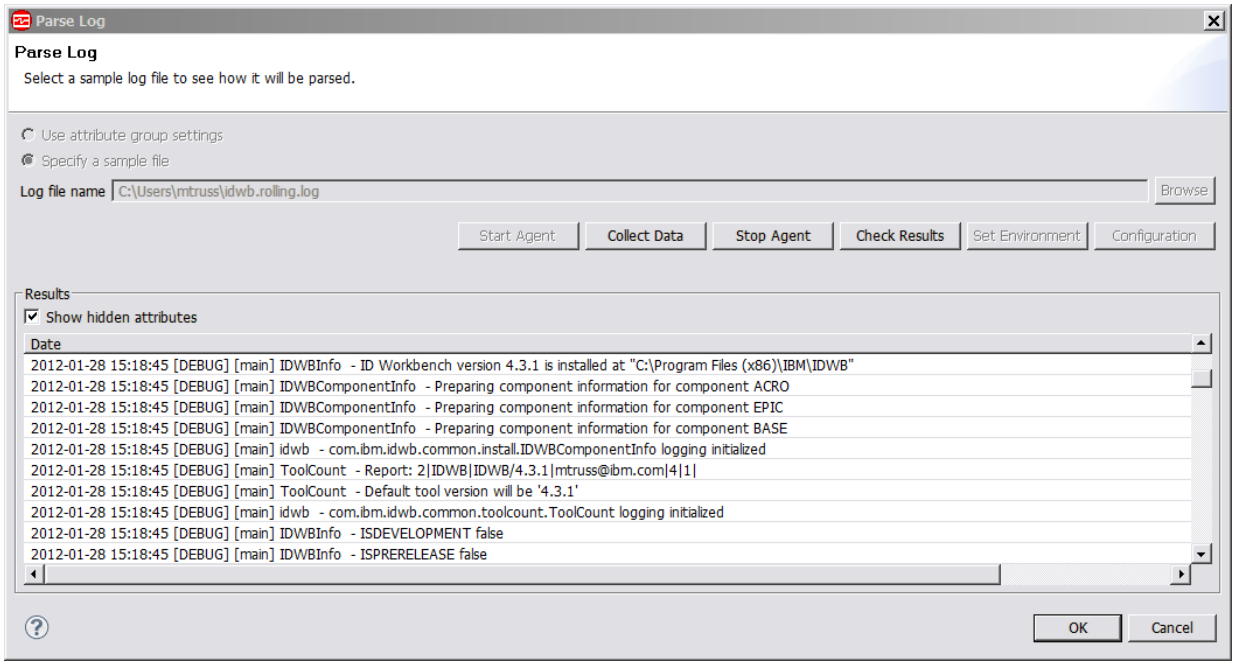


Figure 42. Fenêtre Analyser le journal affichant les valeurs d'attributs du fichier journal analysé

7. Facultatif : Cliquez sur **Vérifier les résultats** si les données renvoyées ne sont pas celles que vous attendez.

   La fenêtre **Statut de la collecte de données** affiche des informations supplémentaires sur les données. Les données collectées et affichées dans la fenêtre Statut de la collecte de données sont décrites dans «Noeud de statut d'objet de performances», à la page 1466.
8. L'agent peut être arrêté en cliquant sur **Arrêter l'agent**.
9. Cliquez sur **OK** ou sur **Annuler** pour quitter la fenêtre **Analyser le journal**. Cliquez sur **OK** pour sauvegarder les modifications que vous avez apportées.

Concepts associés

«Test de votre agent dans Agent Builder», à la page 1420
Après avoir utilisé Agent Builder pour créer un agent, vous pouvez tester l'agent dans Agent Builder.

Surveillance d'un journal binaire AIX

Vous pouvez définir une source de données pour qu'elle surveille les journaux binaires des erreurs AIX via la commande `errpt`. Vous pouvez également la configurer de manière à filtrer et récapituler les données. Les événements en résultant sont placés dans un ensemble de données.

Pourquoi et quand exécuter cette tâche

L'application de surveillance des journaux prend en charge la surveillance des journaux binaires des erreurs AIX via la commande `errpt`. La commande `errpt` génère un rapport d'erreur à partir des entrées d'un journal des erreurs. Cela inclut les indicateurs de sélection d'erreurs correspondant à des critères spécifiques. Cette prise en charge de la surveillance des journaux binaires des erreurs AIX via la commande `errpt` est modélisée sur la prise en charge de la même fonction dans l'agent Tivoli Monitoring UNIX Logs (code produit `kul` ou `ul`).

Lorsque vous fournissez à Agent Builder une chaîne de commande **`errpt`**, le système traite les événements provenant de l'exécution de cette commande. Agent Builder impose les mêmes contraintes à cette commande que l'agent de surveillance des journaux UNIX. En particulier, vous devez utiliser l'option **`-c`** (mode simultané) pour que la commande s'exécute continuellement et vous ne pouvez pas utiliser l'option **`-t`** ou les options suivantes qui donnent lieu à une sortie détaillée : **`-a`**, **`-A`** ou **`-g`**.

Un agent Agent Builder qui surveille automatiquement la commande AIX **`errpt`** inclut automatiquement les mêmes informations qu'un agent de surveillance pour journaux UNIX. Pour plus d'informations sur les

groupes d'attributs des journaux d'erreur binaires AIX, voir «Groupe d'attributs du journal binaire AIX», à la page 1479.

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, cliquez sur **Données consignées** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **journal binaire AIX**.
3. Cliquez sur **Suivant**.
4. Sur la page d'**informations de journal binaire**, entrez une commande `errpt`.
   La valeur par défaut est :

   ```
   errpt -c -smmddhhmmyy
   ```

   L'agent recherche la chaîne 'mmddhhmmyy' et la remplace par la date et l'heure réelles au démarrage. Seule la première occurrence de la chaîne est remplacée.

   Vous pouvez fournir votre propre commande `errpt` mais Agent Builder impose les mêmes contraintes à cette commande que l'agent de surveillance des journaux UNIX. En particulier, vous devez utiliser l'option **`-c`** (mode simultané) pour que la commande s'exécute continuellement et vous ne pouvez pas utiliser l'option **`-t`** ou les options suivantes qui donnent lieu à une sortie détaillée : **`-a`**, **`-A`** ou **`-g`**.
5. (Facultatif) cliquez sur **Avancé** pour sélectionner les options de filtrage et de récapitulatif des événements. Pour plus d'informations, voir «Contrôle des événements en double», à la page 1450.
6. Effectuez l'une des opérations suivantes :
   - Si vous utilisez l'assistant d'**agent**, cliquez sur **Suivant**.
   - Cliquez sur **Terminer** pour sauvegarder la source de données et ouvrir l'éditeur d'agent.

Référence associée

«Groupe d'attributs du journal binaire AIX», à la page 1479
Le groupe d'attributs du journal binaire AIX affiche les événements du journal binaire AIX fournis par la chaîne de commande `errpt`.

Surveillance d'un journal des événements Windows

Vous pouvez définir une source de données pour qu'elle collecte les données d'un journal des événements Windows. Vous pouvez la configurer de manière à filtrer les données. Les événements en résultant sont placés dans un ensemble de données de journal des événements.

Pourquoi et quand exécuter cette tâche

Vous pouvez collecter les données du journal des événements Windows à l'aide du type, de la source ou de l'ID des événements. Vous pouvez utiliser ces paramètres pour filtrer les événements de journal collectées par le système Windows. L'agent compare chaque nouvel événement du journal des événements surveillé avec le filtre indiqué. Si l'événement correspond à un des types d'événement, sources d'événement ou ID événement indiqués dans le filtre, il est transmis.

Par exemple, si le filtre du journal des événements s'applique au journal de l'application, indiquez **Erreur** comme type d'événement. Cette option fait correspondre tous les événements consignés dans le journal de l'application à une valeur de type d'événement `erreur`. Si vous ajoutez les sources d'événement **Diskeeper** et **Symantec AntiVirus**, l'agent transmettra tous les événements d'erreur provenant de l'une de ces sources. Vous pouvez ajouter des ID événement particuliers pour détailler encore le filtre. Aucune association directe n'existe entre le type d'événement, la source d'événement et l'ID événement. Si l'une des valeurs de chacune de ces catégories correspond au filtre, l'événement y correspond.

Par défaut, seuls les événements générés après le démarrage de l'agent sont traités. Cependant, vous pouvez activer l'agent au redémarrage pour traiter les événements du journal générés à l'arrêt de l'agent. Pour plus d'informations sur l'activation de l'agent afin de traiter des événements générés tandis que l'agent est arrêté, voir l'étape «6», à la page 1313.

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, cliquez sur **Données consignées** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **Journal des événements Windows**.
3. Cliquez sur **Suivant**.
4. Dans la page **Journal des événements Windows**, sélectionnez le nom de l'un des journaux de la liste **Nom du journal des événements Windows**, ou entrez un nom pour le journal des événements.

   La liste est construite à partir de l'ensemble des journaux sur le système en cours, par exemple :

   ```
   Application
   Sécurité
   System
   ```
5. Dans la page **Journal des événements Windows**, indiquez si vous voulez filtrer les résultats à l'aide d'un ou de plusieurs des mécanismes suivants :

   - «Filtrage par type d'événement», à la page 1314
   - «Filtrage par source d'événement», à la page 1314
   - «Filtrage par identificateur d'événement», à la page 1315

   Remarque : Vous devez sélectionner au moins un de ces critères de filtrage.
6. Pour traiter les événements du journal générés pendant que l'agent est arrêté, sur un redémarrage de l'agent, cliquez sur **Paramètres d'événements hors ligne** dans la page **Journal des événements Windows**.

   La fenêtre **Paramètres de signets du journal des événements Windows** s'affiche.
7. Sélectionnez une des options de signet suivantes :

   Remarque : Ces options s'appliquent à tous les journaux des événements Windows en cours de surveillance.

   - **Ne collectez pas d'événements hors ligne** : les événements générés lorsque l'agent est arrêté ne sont pas traités. Cette option est l'option par défaut.
   - **Collectez tous les événements hors ligne** : tous les événements générés lorsque l'agent est arrêté sont traités.
   - **Indiquez les paramètres de collecte personnalisés** : vous pouvez entrer une valeur pour réguler le traitement des anciens événements en fonction d'une valeur temporelle et/ou du nombre d'événements. Cette option vous permet de vous assurer que l'environnement de surveillance n'est pas surchargé d'événements au démarrage de l'agent.

     Par exemple, si 100 est entré dans **Nombre maximal d'événements à collecter** et 30, dans la zone **Restreindre la collecte en fonction d'un intervalle de temps (en secondes)**, le nombre d'événements traités correspond soit aux 100 derniers événements générés avant le démarrage de l'agent, ou à tout événement généré dans les 30 secondes qui suivent le démarrage de l'agent. Le résultat dépend de la première variable avec laquelle une correspondance est établie.

     Lorsque vous entrez le nombre maximal d'événements à collecter, la variable d'environnement *CDP_DP_EVENT_LOG_MAX_ BACKLOG_EVENTS* est ajoutée. Lorsque vous entrez une valeur pour restreindre la collecte en fonction d'une fréquence, la variable d'environnement *CDP_DP_EVENT_LOG_MAX_BACKLOG_TIME* est ajoutée. Lorsqu'au moins l'une de ces variables ou les deux variables sont ajoutées, le programme crée le fichier *nomjournalévénement_codeproduit_nominstance_nomsousnoeud*`.rst` contenant le dernier enregistrement d'événement traité pour le journal des événements. Ce fichier se trouve dans le répertoire *%CANDLE_HOME%*`\tmaitm6\logs` et est utilisé au redémarrage de l'agent pour traiter les anciens événements générés lorsque celui-ci était arrêté.
8. Si vous voulez définir des options globales pour la source de données, cliquez sur **Options globales** sur la page **Journal des événements Windows**.

   La fenêtre **Options de source de données Windows globales** s'ouvre.

9. Cochez la case **Include remote Windows configuration properties** si vous souhaitez inclure cette option, puis cliquez sur **OK**.

   Pour plus d'informations sur la configuration des connexions distantes Windows pour les sources de données Windows, voir «Configuration d'une connexion distante Windows», à la page 1407.
10. Après avoir défini le filtre et cliqué sur **OK**, sur la page **Journal des événements Windows**, effectuez l'une des étapes suivantes :
    - Si vous utilisez l'assistant d'**agent**, cliquez sur **Suivant**.
    - Cliquez sur **Terminer** pour sauvegarder la source de données et ouvrir l'éditeur d'agent. Le nom du nouveau journal des événements Windows s'affiche sur la page **Définition de la source de données** de l'**éditeur d'agent**.

Que faire ensuite

Pour plus d'informations sur la configuration des connexions distantes Windows pour les sources de données du journal des événements Windows, voir «Configuration d'une connexion distante Windows», à la page 1407.

Filtrage par type d'événement
Filtrer les résultats Journal des événements Windows par type d'événement

Procédure

1. Dans la page **Journal des événements Windows**, sélectionnez **Filtrer par type d'événement**.
2. Sélectionnez un ou plusieurs des types d'événements suivants :
   - **Informations**
   - **Avertiss.**
   - **Erreur**
   - **Réussite de l'audit**
   - **Audit d'anomalie**
3. Cliquez sur **Terminer** pour valider les ajouts.

Filtrage par source d'événement
Filtrer les résultats du Journal des événements Windows par source d'événement

Procédure

1. Sélectionnez **Filtrer par source d'événement**, puis cliquez sur **Ajouter** dans la zone **Sources d'événement** de la page **Journal d'événements Windows**.

   La fenêtre **Source d'événement** s'ouvre.
2. Procédez de l'une des manières suivantes.
   - Tapez le nom de la source d'événement et cliquez sur **OK**.
   - Cliquez sur **Parcourir** pour rechercher et sélectionner une source d'événement dans une liste et cliquez sur **OK**.

     Le nom que vous avez sélectionné s'affiche dans la fenêtre **Source d'événement**.

     Remarque :

     a. Pour trier la liste des sources d'événement, cliquez sur l'en-tête de colonne.
     b. Pour régénérer les informations dans la fenêtre, cliquez sur l'icône **Régénérer**.
     c. Pour rechercher des sources d'événement particulières, cliquez sur l'icône **Rechercher** (jumelles).

3. Cliquez sur **OK** pour afficher le nouveau filtre de source d'événement dans la liste des sources d'événement de la fenêtre **Journal des événements Windows**.

Filtrage par identificateur d'événement
Pour la source de données Journal des événements Windows, vous pouvez filtrer les événements par identificateur d'événement.

Pourquoi et quand exécuter cette tâche

Pour filtrer par identificateur d'événement, utilisez la procédure suivante :

Procédure

1. Sélectionnez **Filtrer par identificateur d'événement**, puis cliquez sur **Ajouter** dans la zone **Identificateurs d'événement** de la fenêtre **Journal d'événements Windows**.

   La fenêtre **Editeur de situations** s'affiche.
2. Si vous savez que vous voulez surveiller des événements particuliers d'une application, indiquez les numéros des événements tels que l'application les définit. Entrez un entier comme identificateur d'événement et cliquez sur le bouton **OK**.

   Le nouveau filtre d'identificateur d'événement numérique s'affiche dans la liste Identificateurs d'événement de la fenêtre **Journal des événements Windows**.

   Remarque : Chaque identificateur d'événement doit être défini individuellement.
3. Si vous voulez modifier un journal des événements Windows, sélectionnez-le et cliquez sur **Modifier**.
4. Si vous voulez supprimer un journal des événements Windows, sélectionnez-le et cliquez sur **Supprimer**.
5. Vous pouvez ajouter d'autres journaux des événements dans la liste ou cliquer sur **Terminer**.

Surveillance d'un code retour de commande

Vous pouvez définir une source de données pour qu'elle surveille une application ou un système à l'aide d'un *code retour de commande*. L'agent exécute la commande, collecte le code retour et ajoute le résultat à l'ensemble de données de disponibilité.

Pourquoi et quand exécuter cette tâche

Un script, un fichier exécutable, une requête ou une commande de système créés par l'utilisateur peuvent renvoyer un code. Il s'agit d'un mécanisme propre à l'application qui permet de déterminer si l'application ou le système surveillé est disponible. L'agent exécute la commande spécifiée et détermine l'état de l'application ou du système surveillé en examinant le code retour.

La commande doit présenter un code retour unique pour chaque état descriptif. Elle doit également définir un message utilisé par l'agent pour chacun de ces codes retour. La commande peut utiliser des variables d'environnement et de configuration dans le script créé par l'utilisateur, le fichier exécutable, la requête ou la commande système. Elle ne doit pas utiliser de variables d'environnement ou de configuration dans l'appel de ligne de la commande aux seules exceptions suivantes : *AGENT_BIN_DIR*, *AGENT_ETC_DIR*, *AGENT_LIB_DIR*, *CANDLE_HOME* et *CANDLEHOME*.

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, sélectionnez **Commande ou script** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **Un code retour de commande**.
3. Cliquez sur **Suivant**.
4. Dans la zone **Informations sur le code retour de commande** de la page **Code retour de commande**, entrez le nom affiché.
5. Les sous-étapes suivantes vous permettent de définir et de décrire les lignes de commande que le code retour de commande doit utiliser.

Remarque : Définissez une commande pour chaque système d'exploitation pris en charge par l'agent. Les commandes peuvent être partagées, mais la totalité des systèmes d'exploitation concernés par toutes les commandes doit être égale à l'ensemble des systèmes d'exploitation pris en charge par l'agent.

a) Cliquez sur **Ajouter** dans la zone **Commandes** de la fenêtre **Code retour de commande** pour ouvrir la fenêtre **Informations de Commande**.

b) Entrez une ligne de commande et sélectionnez un système d'exploitation dans la liste de la zone **Systèmes d'exploitation** de la fenêtre **Informations de commande**.

Remarque :

1) Pour une commande Windows, vous devez saisir le nom complet de la commande. Par exemple, `commande_à_exécuter.bat` et pas seulement `commande_à_exécuter`.
2) Placez le nom entre guillemets de sorte qu'il ne soit pas analysé par l'interpréteur de commandes. Par exemple, entrez `argument "ceci est un test.bat"` et non `argument ceci est un test.bat`.
3) Vous pouvez cliquer sur une commande, puis cliquer sur **Modifier** pour la modifier ou cliquer sur **Supprimer** pour la supprimer.

c) Cliquez sur **Ajouter** dans la zone **Codes retour** de la fenêtre **Informations de commande**.

d) Sélectionnez un type de code retour dans la liste qui s'affiche dans la fenêtre **Définition du code retour**.

Vous pouvez attribuer les états suivants aux codes retour de test :

- `ALREADY_RUNNING`
- `DEPENDENT_NOT_RUNNING`
- `GENERAL_ERROR`
- `NOT_RUNNING`
- `OK`
- `PREREQ_NOT_RUNNING`
- `WARNING`

e) Entrez une valeur numérique pour le type de code retour que vous avez sélectionné.

La valeur du code retour est un entier qui indique un code retour défini pour le code retour de commande. Pour la portabilité entre les systèmes d'exploitation, utilisez une valeur de code retour comprise entre `0 et 255`. Pour une commande qui s'exécute uniquement sous Windows, la valeur de code retour peut être comprise entre `-2147483648 et 2147483647`.

f) Vous devez définir un message pour chaque code retour afin que le message et le code apparaissent ensemble. Cliquez sur **Parcourir** pour définir le texte du message.

La zone de messages montre les messages définis dans l'agent. La fenêtre (liste) **Messages** s'ouvre.

Remarque :

1) Vous pouvez choisir le texte précédemment entré, en le sélectionnant dans la liste de textes de message, au lieu de cliquer sur **Parcourir**. Ensuite, passez à l'étape 5k.
2) La liste reste vide jusqu'à ce que vous définissiez des messages. Vous pouvez utiliser **Modifier** pour modifier un message défini et **Supprimer** pour supprimer un ou plusieurs messages que vous avez définis.

g) Dans la fenêtre (liste) **Messages**, cliquez sur **Ajouter**.

La fenêtre **Définition de message** s'ouvre.

Remarque : L'identificateur de message est automatiquement généré pour vous.

h) Entrez le texte qui décrit la signification du nouveau message dans la zone **Texte du message**.

i) Cliquez sur **OK**.

La fenêtre (liste) **Messages** s'ouvre en affichant le nouveau message.

j) Pour vérifier le message et le rendre permanent, sélectionnez-le dans la liste et cliquez sur le bouton **OK**.

Le nouveau type de code retour, la valeur et le texte sont affichés dans la fenêtre **Définition de code retour**.

k) Si vous voulez que ce code retour soit accessible à d'autres commandes sur d'autres systèmes d'exploitation, sélectionnez **Le code retour global s'applique à toutes les commandes**. Si vous voulez que ce code retour soit accessible uniquement à cette commande, laissez la case **Le code retour local ne s'applique qu'à cette commande** cochée.

l) Cliquez sur **OK** dans la fenêtre **Définition du code retour**.

m) Définissez au moins deux codes retour avant de quitter la fenêtre **Informations de commande**. Un code retour pour indiquer qu'il n'y a pas de problème de disponibilité, l'autre pour signaler un incident. Si vous souhaitez ajouter un autre code retour, retournez à l'étape c.

n) Facultatif : Dans la fenêtre **Informations de commande**, zone **Fichiers de commandes**, cliquez sur **Ajouter** si vous voulez sélectionner un ou plusieurs scripts ou fichiers exécutables à exécuter par l'agent.

Les fichiers sont copiés dans le dossier du projet de l'agent sous `scripts/`*`système d'exploitation`*, où *système d'exploitation* est une variable qui dépend de la valeur sélectionnée dans la zone **Systèmes d'exploitation** de la fenêtre **Informations de commande**. Ces fichiers sont également intégrés à des packages et distribués avec l'agent. Pour modifier la définition d'un fichier de commandes existant, ou le fichier de commandes d'origine depuis sa copie dans le projet, sélectionnez le fichier et cliquez sur **Modifier**. Voir «Modification d'une définition de fichier de commandes», à la page 1319.

o) Cliquez sur **OK** dans la fenêtre **Informations de commande**.

Remarque : la table des fichiers de commande est l'endroit où vous définissez tous les fichiers externes à inclure dans le module d'agent. Ces fichiers sont copiés dans le répertoire projet et groupés avec l'agent pour la distribution.

6. Si vous disposez d'autres codes retour qui ne sont pas encore définis, définissez et décrivez les codes retour globaux que le code retour de commande doit utiliser :

a) Cliquez sur **Ajouter** dans la zone **Codes retour globaux** sur la page **Code retour de commande**.

Remarque : Les codes retour définis ici sont globaux. Cela signifie qu'ils sont adaptés à toutes les commandes définies pour le code retour de commande. (Ils ne sont pas partagés entre les codes retour de commande). En outre, vous pouvez définir les codes retour lorsque vous entrez des informations de commande. Les codes retour définis ici peuvent être globaux ou locaux. Les codes retour locaux ne sont appropriés que pour cette commande spécifique. Cette hiérarchie est utile si vous avez un code retour identique sur tous les systèmes d'exploitation. (Par exemple, si un code retour correspond à 0, cela signifie que tout fonctionne correctement. Vous pouvez le définir au niveau global, puis toutes les commandes définies interprètent le 0 de cette manière.) Si aucun des autres systèmes d'exploitation ne renvoie un 5, vous pouvez définir le code retour 5 uniquement pour la commande Windows. Si vous définissez un code retour au niveau de la commande locale qui est déjà défini au niveau global, le niveau de la commande est utilisé. Vous pouvez utiliser cette méthode pour remplacer les codes retour de systèmes d'exploitation spécifiques. Par exemple, si sur tous les systèmes d'exploitation UNIX, un code retour de 2 signifie une chose, sous Windows, il signifie toute autre chose. Vous pouvez définir un code retour de 2 au niveau global, comme attendu par les systèmes d'exploitation UNIX. Ensuite, dans la commande pour Windows, vous pouvez redéfinir la signification du code retour 2 sous Windows.

b) Sélectionnez un type de code retour dans la liste qui s'affiche dans la fenêtre **Définition du code retour**.

Vous pouvez attribuer les états suivants aux codes retour de test :

- `ALREADY_RUNNING`

- DEPENDENT_NOT_RUNNING
- GENERAL_ERROR
- NOT_RUNNING
- OK
- PREREQ_NOT_RUNNING
- WARNING

c) Entrez une valeur numérique pour le type de code retour que vous avez sélectionné. La valeur du code retour est un entier qui indique un code retour défini pour le code retour de commande.

d) Cliquez sur **Parcourir** pour définir le texte du message et la signification associée. Vous devez définir un message pour chaque code retour afin que le message et le code apparaissent ensemble.

La fenêtre **Messages** affiche les messages définis dans l'agent.

Remarque :

1) La liste reste vide jusqu'à ce que vous définissiez des messages. Vous pouvez utiliser **Modifier** pour modifier un message défini et **Supprimer** pour supprimer un ou plusieurs messages que vous avez définis.
2) Vous pouvez choisir le texte précédemment entré, en le sélectionnant dans la liste **Texte du message** au lieu de cliquer sur **Parcourir**. Ensuite, passez à l'étape 6h.

e) Dans la fenêtre (liste) **Messages**, cliquez sur **Ajouter** pour afficher une fenêtre **Définition de message**, dans laquelle vous pouvez saisir le texte de description de la signification du nouveau message.

f) Cliquez sur **OK**.

g) La fenêtre (liste) **Messages** s'ouvre en affichant le nouveau message. Pour vérifier le message et le rendre permanent, sélectionnez-le dans la liste et cliquez sur le bouton **OK**.

h) Lorsque le nouveau texte, le type et la valeur s'affichent dans la fenêtre **Définition de code retour**, cliquez sur **OK**.

i) Sur la page Code retour de commande, une fois que vous avez fini de définir les codes retour et les commandes pour tous les systèmes d'exploitation, procédez comme suit :

- Si vous utilisez l'assistant de création d'agent, cliquez sur **Suivant** ou sur **Terminer** pour sauvegarder la source de données et ouvrir l'éditeur d'agent.
- Si vous utilisez l'assistant de création de composant d'agent, cliquez sur **Terminer** pour revenir à l'éditeur d'agent.

Que faire ensuite

Si vous souhaitez utiliser les données issues de cette source de données dans le tableau de bord récapitulatif pour IBM Cloud Application Performance Management, vous devez créer un ensemble de données filtré (un groupe d'attributs) basé sur l'ensemble de données Disponibilité et le configurer comme fournissant une ligne unique. Sélectionnez la ligne pour votre processus à l'aide de la zone NAME.

Dans le nouveau groupe d'attributs filtré, sélectionnez la zone Statut et indiquez les valeurs de gravité associées.

Pour des instructions, voir :

- «Création d'un groupe d'attributs filtré», à la page 1383
- «Spécification de la gravité pour un attribut utilisé comme indicateur de statut», à la page 1236
- «Préparation de l'agent pour Cloud APM», à la page 1417

Modification d'une définition de fichier de commandes
Vous pouvez modifier le fichier de commandes importé dans le projet ou importer des modifications apportées au fichier de commandes existant dans le projet.

Procédure

1. Sélectionnez le fichier dans la zone **Fichiers de commandes** de la fenêtre **Informations de commande**.
2. Cliquez sur **Modifier** pour ouvrir la fenêtre **Importation d'un fichier de commandes**.

   Dans la fenêtre **Importation d'un fichier de commandes**, vous pouvez obtenir le statut du fichier de commandes mais également modifier l'emplacement du fichier source d'origine et recopier le fichier source sur l'agent.
3. Choisissez l'une des étapes suivantes :
   - Cliquez sur **OK** pour planifier la copie du fichier lors de la prochaine sauvegarde de l'agent.
   - Cliquez sur **Copier immédiatement** pour copier le fichier sans effectuer au préalable la sauvegarde de l'agent.

   Remarque : L'option **Copier immédiatement** n'est pas disponible lorsque vous accédez à la fenêtre d'**Importation d'un fichier de commandes** à partir de l'assistant de création d'agent.

Séparation et consolidation des fichiers
Vous pouvez utiliser les fonctions Séparer et Consolider pour déplacer les fichiers dans ou hors des dossiers spécifiques aux systèmes d'exploitation de l'agent.

Lorsqu'un fichier est ajouté à l'agent pour la première fois, une copie unique est ajoutée dans le dossier `scripts/all_windows`, `scripts/all_unix` ou `scripts/common`. Le dossier `scripts/common` est privilégié si le fichier est utilisé à la fois sur Windows et UNIX.

Pour placer plusieurs copies du fichier sur plusieurs systèmes d'exploitation (par exemple, un fichier exécutable binaire), cliquez sur **Modifier** et sur **Séparer**. Le fichier est supprimé du dossier commun et copié dans les dossiers propres au système d'exploitation. Vous pouvez alors remplacer chaque copie du fichier par les copies appropriées aux systèmes d'exploitation spécifiques.

Remarque : Les fichiers de ressource Java doivent rester dans le dossier `scripts/common`. Vous ne pouvez pas cliquer sur **Séparer** pour créer des copies distinctes de fichiers de ressources Java pour tel ou tel système d'exploitation en particulier.

Si vous avez séparé les fichiers pour les placer dans des dossiers de système d'exploitation, vous pouvez utiliser **Consolider** pour les replacer dans un dossier commun. Si vous avez créé l'agent dans une version d'Agent Builder qui ne prenait pas en charge les dossiers courants, utilisez **Consolider** pour les replacer dans un dossier commun. Si une des copies du fichier diffère de l'autre, vous devez, à l'invite, sélectionner le fichier à utiliser comme fichier commun. Toutes les autres copies sont supprimées.

Surveillance de la sortie d'un script

Vous pouvez définir une source de données pour qu'elle collecte les données d'un script ou d'un programme externe. Utilisez-la lorsque les données d'application ne sont pas disponibles via une interface de gestion standard ou lorsque vous devez fournir un récapitulatif des données multiligne sur une seule ligne. L'agent exécute le script et collecte sa sortie. Chaque ligne de la sortie de script est analysée sous la forme d'une ligne de l'ensemble de données obtenu.

Les données peuvent être collectées à partir d'un système local ou distant. La sortie du programme ou du script ne doit contenir que les valeurs de chaque attribut du groupe d'attributs. Pour renvoyer plusieurs lignes de données, les données de chaque ligne doivent être séparées par un retour à la ligne. Les attributs de chaque ligne de données sont séparés par les séparateurs que vous définissez. Pour plus d'informations sur les séparateurs, voir «Script d'analyse et séparateurs», à la page 1320.

La commande peut utiliser des variables d'environnement et de configuration dans le script créé par l'utilisateur, le fichier exécutable, la requête ou la commande système. La commande ne peut pas utiliser de variables d'environnement ou de configuration dans l'appel de ligne de commande de la commande,

aux seules exceptions suivantes : AGENT_BIN_DIR, AGENT_ETC_DIR, AGENT_LIB_DIR, CANDLE_HOME et CANDLEHOME.

L'agent surveille la sortie du script qui est écrit en utilisant le même environnement local et la même page de codes où l'agent s'exécute.

Collecte des données de script depuis un système distant
Pour collecter les données de script ou de programme d'un système distant, Agent Builder utilise un SSH (Secure Shell).

Pour collecter des données d'un système distant, Agent Builder crée une session SSH (Secure Shell) et appelle un script ou un programme externe sur ce système distant. L'agent établit une session SSH et s'y connecte. Il télécharge ensuite les scripts sur le système distant, appelle le script ou le programme externe et récupère la sortie. L'agent peut être configuré de manière à conserver la session ouverte ou à la rétablir à chaque appel. Si la session est maintenue ouverte, le script peut être réutilisé ou téléchargé à chaque appel. Par défaut, la session SSH est maintenue ouverte et les scripts sont réutilisés à chaque appel.

Agent Builder prend en charge uniquement SSH Protocol Version 2 avec des clés Rivest, Shamir et Adleman (RSA) ou DSA (Digital Signature Algorithm). L'agent est authentifié soit par un nom d'utilisateur et un mot de passe, soit via une clé publique. La génération et la distribution des clés publiques est une tâche d'administration qui doit être effectuée en dehors de l'agent et du composant Agent Builder.

Pour exécuter une commande Action créée pour un fournisseur de données de script activé SSH (Secure Shell) sur le système distant, voir «Action SSHEXEC», à la page 1552.

Restriction : Si votre agent a été créé avec une version d'Agent Builder antérieure à la version 6.3 et qu'il a un fournisseur de données de script qui utilise le protocole SSH, le fournisseur échoue lors d'une exécution avec IBM Tivoli Monitoring version 6.3 ou ultérieure. Pour résoudre ce problème, régénérez l'agent à l'aide de la version actuelle d'Agent Builder.

Cette restriction existe, car la version 6.3 de IBM Tivoli Monitoring utilise une version plus récente de l'API de Global Secure ToolKit (GSKit). Vous devez régénérer l'agent avec Agent Builder 6.3 ou version ultérieure pour l'exécution avec IBM Tivoli Monitoring version 6.3 ou ultérieure. Si vous générez l'agent avec Agent Builder 6.3, il peut également s'exécuter avec des versions précédentes de IBM Tivoli Monitoring.

Script d'analyse et séparateurs
Vous pouvez modifier et attribuer des séparateurs de script spécifiques à un ou plusieurs attributs.

Lorsque vous créez un groupe d'attributs de script, un séparateur textuel de caractère unique est affecté par défaut. Le séparateur par défaut est " **;** ". Le séparateur est utilisé par l'agent pour analyser et délimiter les données pour chaque attribut dans la ligne de données. Vous pouvez modifier le séparateur par défaut pour utiliser un caractère différent. Vous pouvez également affecter des séparateurs spécifiques à un ou plusieurs attributs individuels.

Vous pouvez affecter des séparateurs spécifiques pour les attributs individuels qui :

- extraient un nombre fixe d'octets dans la sortie ;
- séparent un attribut du suivant avec un séparateur personnalisé qui peut comporter plusieurs caractères ;
- délimitent une valeur d'attribut avec une chaîne au début et à la fin de la valeur ;
- renvoient le reste du texte comme valeur d'attribut (avec séparateurs imbriqués ou non).

Vous pouvez utiliser un ou plusieurs de ces séparateurs pour extraire les valeurs d'attribut à partir de lignes de données.

Exemple 1 - Sortie de script simple

Certains scripts peuvent comporter des lignes de données de sortie avec des séparateurs clairs et normaux, par exemple :

```
Ligne Un;1;2
Ligne Deux;3;4
Ligne Trois;5;6
```

Dans ce cas, le caractère ";" est un séparateur clair et normal entre les trois éléments de données de chaque ligne. Dans ce cas, le séparateur par défaut est parfait et il n'est pas nécessaire de modifier ou définir d'autres séparateurs. Il est facile d'imaginer une sortie de script où le séparateur est un caractère différent, comme dans l'exemple ci-dessous.

```
Ligne Un-1-2
Ligne Deux-3-4
Ligne Trois-5-6
```

Dans cet exemple, le séparateur ";" est remplacé par le caractère "-". Dans ce cas, lorsque vous définissez les attributs, vous devez modifier le séparateur par défaut pour utiliser le caractère " - ".

Exemple 2 - Sortie de script complexe

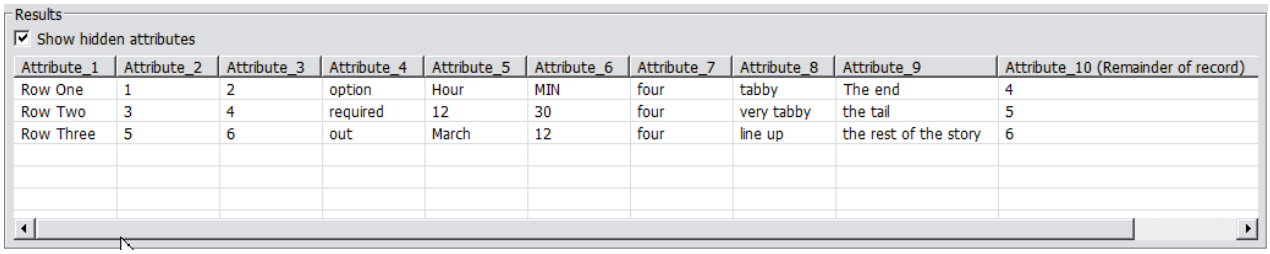
Certains scripts peuvent générer des lignes de données avec des séparateurs irréguliers ou variables, par exemple :

```
Row One;1;2;[option]Hour:MIN;fourtabby     The end;4
Row Two;3;4;[required]12:30;fourvery tabby the tail;5
Row Three;5;6;[out]March:12;fourline up    the rest of the story;6
```

Dans cet exemple, vous pouvez affecter des séparateurs à des définitions d'attribut comme suit :

1. Initialement, le séparateur par défaut ";" convient pour les trois premiers attributs dans chaque ligne de données. Dans ce cas, vous affectez le type de séparateur **Texte de séparateur** réglé sur ";" lorsque vous définissez chaque attribut (ce paramètre est utilisé par défaut).
2. Examinons le quatrième attribut. Supposons que la chaîne entre "[" et "]" soit une valeur que vous souhaitez extraire. Dans ce cas, lorsque vous définissez le quatrième attribut, vous devez définir un type de séparateur **Textes de début et de fin** avec les valeurs de texte de début et de fin suivantes : "[" et "]".
3. Pour le cinquième attribut, supposez que vous devez extraire les valeurs entre les caractères "]" et ":". Dans ce cas, lorsque vous définissez le cinquième attribut, vous devez affecter le type de séparateur **Texte comme séparateur** défini sur ":".
4. Pour le sixième attribut, acceptez le séparateur par défaut ";" car il convient également.
5. Pour le septième attribut, vous souhaitez extraire la chaîne dans les quatre caractères suivants "four". Cette chaîne ne se termine pas par un séparateur net. Vous pouvez affecter un nombre de caractères pour définir la séparation de l'attribut suivant. Vous pouvez affecter un séparateur de type **Nombre de caractères** et indiquer une longueur de quatre caractères.
6. Pour le huitième attribut, vous souhaiterez extraire les chaînes tabby, very tabby et line up. Dans ce cas, vous pouvez supposer que toutes ces chaînes sont suivies d'un caractère de tabulation. Dans ce cas, vous attribuez un séparateur de type **Séparateur de tabulation**.
7. Pour le neuvième attribut, vous pouvez rétablir le type de séparateur par défaut pour extraire le texte restant.
8. Pour le dixième attribut, vous spécifiez **Reste de l'enregistrement** afin d'affecter le reste de la ligne de données à cet attribut.

L'effet de la définition de ces séparateurs dans un script qui génère les lignes de données indiquées précédemment dans cet exemple, est indiqué dans la sortie suivante :



Attribute_1	Attribute_2	Attribute_3	Attribute_4	Attribute_5	Attribute_6	Attribute_7	Attribute_8	Attribute_9	Attribute_10 (Remainder of record)
Row One	1	2	option	Hour	MIN	four	tabby	The end	4
Row Two	3	4	required	12	30	four	very tabby	the tail	5
Row Three	5	6	out	March	12	four	line up	the rest of the story	6

Figure 43. Exemple de sortie de valeur d'attribut lorsque l'agent analyse une sortie de script complexe.

La procédure de définition des séparateurs d'attribut est décrite à l'étape «10», à la page 1324 de «Procédure de surveillance de la sortie à partir d'un script», à la page 1322.

Procédure de surveillance de la sortie à partir d'un script
Configurer l'agent pour recevoir les données d'une source de données de script.

Avant de commencer
Voir «Surveillance de la sortie d'un script», à la page 1319.

Pourquoi et quand exécuter cette tâche

Pour surveiller la sortie d'un script, procédez comme suit :

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, sélectionnez l'option **Commande ou script** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **Sortie d'un script**.
3. Cliquez sur **Suivant**.
4. Dans la page **Liste des commandes**, cliquez sur **Ajouter** pour afficher une fenêtre **Informations de commande**.

   Remarque : La case **Activer la collecte de données via SSH** permet d'activer SSH pour ce groupe d'attributs. Si cette case n'est pas cochée, le groupe d'attributs s'exécute en local.

   Remarque : S'il existe une commande pouvant être exécutée sur le système d'exploitation sur lequel Agent Builder est en cours d'exécution, l'option **Tester** est activée. Vous pouvez utiliser **Tester** pour tester une commande que vous avez définie.
5. Dans la zone **Informations de commande** de la fenêtre **Informations de commande**, entrez un nom de commande à l'aide des arguments nécessaires dans la zone **Commande**, puis un séparateur dans la zone **Séparateur**.

   Remarque :

   a. Les scripts dans Windows sont fréquemment appelés sans indiquer l'extension `.bat` ou `.cmd` sur la ligne de commande. Pour une exécution à distance, un environnement d'interpréteur de commandes doit être installé et vous devez indiquer l'extension `.bat` ou `.cmd` dans la commande de source de données pour que le script s'exécute. `Cygwin` est un exemple d'environnement d'interpréteur de commandes disponible sous Windows, Linux, Red Hat et AIX. Pour vérifier l'existence d'un environnement d'interpréteur de commandes, utilisez SSH ou connectez-vous à l'hôte distant et entrez la commande :

   ```
   PATH=$PATH:. <commande>
   ```

   Si la commande s'exécute, cela prouve l'existence d'un environnement d'interpréteur de commandes.

b. Placez le nom entre guillemets de sorte qu'il ne soit pas analysé par l'interpréteur de commandes. Par exemple, `ceci est un argument test.bat` devient :

```
"ceci est un argument test.bat"
```

c. Des variables d'environnement et variables de configuration peuvent être utilisées dans le script fourni par l'utilisateur, mais elles ne peuvent faire partie de la ligne de commande qui appelle le script. Les variables suivantes sont des exceptions à cette règle :

AGENT_BIN_DIR
Répertoire dans lequel l'agent place les fichiers binaires ou les scripts

AGENT_ETC_DIR
Répertoire dans lequel l'agent place les fichiers de configuration

AGENT_LIB_DIR
Répertoire dans lequel l'agent place les bibliothèques partagées ou les bibliothèques de liens dynamiques

CANDLEHOME
Répertoire d'installation de Tivoli Monitoring pour Linux ou UNIX.

CANDLE_HOME
Répertoire d'installation de Tivoli Monitoring pour Windows

d. Si l'option de collecte de données SSH est utilisée, la ligne de commande est exécutée par rapport au répertoire de base de l'utilisateur sur le système distant. Si vous téléchargez en amont des scripts ou des exécutables sur le système distant, ils seront copiés dans l'emplacement indiqué dans la variable d'environnement de l'agent *CDP_SSH_TEMP_DIRECTORY*. L'emplacement correspond par défaut au répertoire de base de l'utilisateur sur le système distant. Sur certains systèmes, vous devrez peut-être utiliser un chemin relatif pour la ligne de commande : par exemple `./Script.sh`.

6. Dans la zone **Systèmes d'exploitation**, sélectionnez un ou plusieurs systèmes d'exploitation. Lorsque vous collectez des données d'un système distant via le protocole SSH, l'option Systèmes d'exploitation est une propriété du système sur lequel l'agent est installé. Il ne s'agit pas du système d'exploitation du système distant. Il est conseillé de cocher la case **Tous les systèmes d'exploitation** lorsque vous utilisez les fonctions de collecte des données SSH.
7. Facultatif : Si un ou plusieurs fichiers définis par l'utilisateur sont nécessaires pour exécuter la commande, cliquez sur **Ajouter** dans la zone Fichiers de commandes pour indiquer les fichiers du système.

   Les fichiers sont copiés dans le dossier du projet de l'agent sous `scripts/`*`système d'exploitation`*, où *système d'exploitation* est une variable qui dépend de la valeur sélectionnée dans la fenêtre **Informations de commande**. Ces fichiers sont également intégrés à des packages et distribués avec l'agent. Si vous souhaitez modifier la définition d'un fichier de commandes qui a déjà été ajouté ou dont vous avez modifié le contenu, sélectionnez le fichier et cliquez sur **Editer**. Voir «Modification d'une définition de fichier de commandes», à la page 1319.
8. Cliquez sur **OK**. La page **Liste des commandes** s'affiche.
9. Pour tester la commande, procédez comme suit :

   a) Cliquez sur **Tester** pour afficher les informations de commande et pour afficher la fenêtre **Tester la commande**. Pour tester le script sur un système distant, sélectionnez un système dans la liste **Nom de connexion** ou cliquez sur **Ajouter** pour ajouter le nom d'hôte d'un système.

   b) Utilisez la fenêtre **Tester la commande** pour modifier la commande, le séparateur par défaut et les séparateurs d'attribut, puis pour déterminer l'impact des changements sur les données renvoyées.

      1) Tapez la commande et le séparateur dans les zones, s'ils ne sont pas déjà renseignés.

         Remarque : Vous pouvez spécifier d'autres séparateurs à l'aide de la fenêtre **Informations d'attribut** au moment de la création d'attribut ou à l'aide de l'éditeur d'agent pour modifier un attribut existant. Pour plus d'informations sur l'éditeur d'agent, voir «Utilisation de l'éditeur d'agent pour modifier l'agent», à la page 1207 ; pour plus d'informations sur la manipulation

des source de données et des attributs, voir «Modification des propriétés de sources de données et d'attributs», à la page 1227

2) Avant de démarrer le test, vous pouvez définir des variables d'environnement et des propriétés de configuration. Pour plus d'informations, voir «Test des groupes d'attributs», à la page 1420.
3) Cliquez sur **OK** pour revenir à la fenêtre **Paramètres de test**.
4) Cliquez sur l'option de **démarrage de l'agent**. Une fenêtre indique que l'agent est en cours de démarrage.
5) Pour simuler une demande de données d'agent provenant de Tivoli Enterprise Portal ou de SOAP, cliquez sur **Collecte de données**. Agent Builder exécute votre commande. Si vous avez indiqué un système distant, fournissez un ID utilisateur et un mot de passe. Même si le code retour n'est pas 0, Agent Builder analyse les résultats de la commande selon la même méthode utilisée par l'agent.
6) La fenêtre **Paramètres de test** collecte et affiche toutes les données du cache de l'agent depuis son dernier démarrage. Les noms initiaux des attributs sont **Attribute_1, Attribute_2**, etc. Toutefois, vous pouvez modifier les propriétés des attributs en cliquant sur l'en-tête de colonne approprié.
7) Cliquez sur **Vérifier les résultats** pour afficher le code retour généré par la commande, les données non analysées et les éventuels messages d'erreur renvoyés.
8) L'agent peut être arrêté en cliquant sur **Arrêter l'agent**.
9) Cliquez sur **OK** pour revenir à la fenêtre **Informations de commande**.

   Si vous modifiez la commande ou le séparateur, la commande appropriée est mise à jour pour refléter ces modifications.

   Si cette fenêtre a été lancée lors de la création de la source de données de script, les attributs ont été ajoutés dans la nouvelle source de données de script.

   Si cette fenêtre a été ouverte à partir d'une source de données de script existante, les modifications apportées aux attributs sont appliquées à la source de données de script. Les attributs supplémentaires sont ajoutés, mais les attributs superflus ne sont pas supprimés. Ces options ont une incidence uniquement sur les attributs soumis à l'analyse à partir du script de sortie. Aucun attribut dérivé n'est affecté. Si l'un de ces attributs n'est plus valide en fonction des attributs auxquels ils font référence, vous devez mettre à jour ou supprimer manuellement les attributs dérivés. La formule d'attribut dérivé s'affiche et non pas la valeur du résultat.

Remarque : Si le groupe d'attributs existe, procédez comme suit pour commencer un test :

a. Sélectionnez le groupe d'attributs sur la page **Définition des sources de données** de l'**éditeur d'agent**.
b. Sélectionnez le script à tester dans la liste des commandes.
c. Cliquez sur **Tester** et suivez la procédure de l'étape «9», à la page 1323.

10. Si vous avez ignoré le test de la commande à l'étape («9», à la page 1323), procédez comme suit :
    a) Sur la page **Liste des commandes** qui contient les informations de commande, cliquez sur **Suivant**.
    b) Sur la page **Information d'attribut**, fournissez le nom de l'attribut et les informations de type en utilisant le Tableau 261, à la page 1232. Sélectionnez **Ajouter des attributs supplémentaires** pour ajouter d'autres attributs.
    c) Dans la page **Information d'attribut**, utilisez l'onglet **Informations d'attribut de script** pour choisir un séparateur de données spécifique pour cet attribut.

       Le séparateur standard `;` est sélectionné par défaut. Vous pouvez choisir un certain nombre d'autres séparateurs, par exemple une chaîne, un certain nombre de caractères, une tabulation ou un espace. Vous pouvez également choisir d'utiliser un autre séparateur de chaînes pour le début et la fin des données. Enfin, vous pouvez également choisir **Reste de l'enregistrement** pour

affecter le reste de l'enregistrement à l'attribut. Pour plus d'informations sur l'analyse syntaxique et les séparateurs de script, voir «Script d'analyse et séparateurs», à la page 1320.

11. Effectuez l'une des opérations suivantes :
    - Si vous utilisez l'assistant d'**agent**, cliquez sur **Suivant**.
    - Cliquez sur **Terminer** pour sauvegarder la source de données et ouvrir l'éditeur d'agent.
12. Vous pouvez ajouter des attributs et fournir les informations correspondantes. Pour plus d'informations, voir «Création d'attributs», à la page 1229.

    Outre les zones applicables à toutes les sources de données (décrites dans «Zones et options de définition des attributs», à la page 1232), la page **Définition des sources de données** de la source de données du script propose les options suivantes :

    Liste des commandes
    Fournit un accès aux commandes et scripts à démarrer lors d'une collecte de données.

    Ajouter
    Permet à l'utilisateur d'ajouter une commande à démarrer en fonction de ce groupe d'attributs.

    Modifier
    Permet à l'utilisateur de modifier une entrée de commande existante.

    Supprimer
    Permet à l'utilisateur de supprimer une entrée de commande existante.

    Test
    Permet à l'utilisateur d'accéder à l'environnement de test de ce groupe d'attributs.

    Activer la collecte de données via SSH
    Cette case à cocher permet d'activer SSH pour ce groupe d'attributs. Si cette case n'est pas cochée, le groupe d'attributs s'exécute en local.

    Pour plus d'informations sur la configuration des connexions SSH distantes pour les sources de données de script, voir «Configuration d'une connexion distante SSH (Secure Shell)», à la page 1410.

Surveillance de données à partir de JDBC (Java Database Connectivity)

Vous pouvez définir une source de données pour qu'elle reçoive les données d'une base de données JDBC. L'agent exécute une requête SQL pour collecter les données de la base de données. Chaque colonne renvoyée par la requête est un attribut dans le jeu de données obtenu.

Pourquoi et quand exécuter cette tâche

Le fournisseur de données JDBC prend en charge les serveurs de base de données suivants :

- IBM DB2 9.x et 8.x
- Microsoft SQL Server 2008, 2005 et 2000
- Base de données Oracle 11g et 10g

Agent Builder n'inclut pas les pilotes JDBC de ces bases de données. Les pilotes JDBC sont un ensemble de fichiers JAR fournis par le fournisseur qui sont nécessaires pour l'établissement d'une connexion JDBC à la base de données. Par souci de commodité, voici des liens vers les sites sur lesquels ces pilotes peuvent être téléchargés :

- IBM DB2 : Les pilotes JDBC sont intégrés à l'installation de serveur de base de données dans un sous-répertoire intitulé `java` qui se trouve sous le répertoire de base d'installation DB2.
- Site Web de Microsoft SQL Server à l'adresse www.microsoft.com
- Base de données Oracle : Base de données Oracle compatible JDBC (http://www.oracle.com/technetwork/database/features/jdbc/index.html)

Remarque : Il est à noter que le fournisseur de données JDBC peut surveiller à distance vos serveurs de base de données. Un environnement d'exécution Java et les fichiers JAR du pilote JDBC pour le serveur de base de données auquel vous vous connectez doivent se trouver sur le système sur lequel l'agent s'exécute.

Les versions de Java suivantes sont prises en charge :

- Oracle Corporation Java version 5 ou ultérieure
- IBM Corporation Java version 5 ou ultérieure

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, cliquez sur **Données d'un serveur** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **JDBC**.
3. Cliquez sur **Suivant**.
4. Dans la zone **Informations JDBC** de la fenêtre **Informations JDBC**, cliquez sur **Parcourir** pour vous connecter à une base de données et générer votre requête SQL.

   Utilisez la navigateur JDBC pour vous connecter à une base de données et afficher ses tables pour créer une requête SQL qui collecte les données dont vous avez besoin. Lorsque vous sélectionnez une table et des colonnes, une requête est générée automatiquement et des attributs sont ajoutés pour chacune des colonnes renvoyées par la requête. Vous pouvez modifier et tester la requête générée, afin de vous assurer que les données renvoyées correspondent à celles dont vous avez besoin.

   Remarque : Vous pouvez également créer manuellement la source de données JDBC sans cliquer sur **Parcourir**. Si vous voulez créer manuellement la source de données, indiquez la requête, puis cliquez sur **Suivant**. Vous devez définir un attribut pour chaque colonne renvoyée par la requête, dans l'ordre dans lequel les colonnes sont renvoyées.

   Le fournisseur de données JDBC permet d'exécuter des requêtes SQL et des procédures stockées au niveau d'une base de données pour collecter des données de surveillance. Lorsque vous indiquez une requête SQL pour collecter des données, vous pouvez inclure une clause WHERE dans votre instruction SQL afin de filtrer les données renvoyées. L'instruction SQL peut également joindre des données de plusieurs tables. Outre les instructions SQL SELECT, le fournisseur de données JDBC peut exécuter des procédures stockées. Pour plus d'informations sur l'exécution de procédures stockées, voir «Procédures stockées», à la page 1331.
5. Lors de la première ouverture du navigateur, la fenêtre Navigateur JDBC (Java Database Connectivity) indique qu'aucune connexion n'est sélectionnée. Vous devez ajouter une connexion. Cliquez sur **Ajouter** et suivez les étapes pour ajouter une connexion.

   Si vous avez déjà défini une connexion, celle-ci est utilisée et vous pouvez passer à l'étape «6», à la page 1327.

   Remarque : La zone **Statut** affiche le statut de la connexion en cours.

   Procédez comme suit pour ajouter une connexion :

   a) Sur la page **Connexions JDBC**, cliquez sur **Connexion JDBC** puis sur **Suivant**.

   b) Sur la page **Propriétés de connexion**, renseignez les zones comme suit :

   Nom de connexion
   Nom de la connexion JDBC. Entrez un nom unique pour cette connexion. Ce nom sert à référencer la connexion dans le navigateur.

   Type de base de données
   Type de la base de données. Sélectionnez le produit de base de données auquel vous vous connectez. Par exemple, pour vous connecter à la base de données IBM DB2, sélectionnez **DB2**.

   Nom d'utilisateur
   Doit être défini avec au moins des droits en lecture à la base de données, mais ne doit pas s'agir nécessairement de l'administrateur de base de données.

   Mot de passe
   Doit être défini avec au moins des droits en lecture à la base de données, mais ne doit pas s'agir nécessairement de l'administrateur de base de données.

Nom d'hôte
Nom de l'hôte sur lequel le serveur de base de données est en cours d'exécution. Avec JDBC, vous pouvez surveiller des bases de données distantes, de sorte que vous n'êtes pas limité à la surveillance de bases de données sur le système local.

Port
Port de l'hôte sur lequel le serveur de base de données est en mode écoute.

Détails des
Nom de la base de données à laquelle vous vous connectez.

Répertoire jar
Répertoire contenant les fichiers JAR JDBC utilisés pour la connexion à la base de données. Tapez le nom de chemin ou cliquez sur **Parcourir** pour localiser le répertoire.

c) Facultatif : Cochez la case **Sauvegarder le mot de passe dans l'espace de travail Agent Builder** si vous souhaitez sauvegarder le mot de passe pour cette connexion.

d) Facultatif : Cochez la case **Définir comme valeurs par défaut de la configuration de l'agent** si vous voulez que les valeurs par défaut de ce type de serveur d'applications soient copiées à partir de ces propriétés.

Si vous générez l'agent sur un système similaire aux systèmes surveillés, cochez cette case. Si vous ne cochez pas cette case, l'utilisateur qui configure l'agent voit une zone vide. L'utilisateur doit alors déterminer les valeurs de toutes les informations sans valeurs par défaut.

e) Cliquez sur **Tester la connexion** pour créer une connexion à la base de données qui utilise les paramètres de configuration que vous avez indiqués.

Un message sur la page **Propriétés de connexion** indique si la connexion aboutit.

f) Une fois que la connexion fonctionne, cliquez sur **Terminer**.

6. Dans la fenêtre **Navigateur JDBC (Java Database Connectivity)**, une connexion à la base de données configurée est établie. Les tables contenues dans la base de données s'affichent dans la zone **Tables de base de données**. Sélectionnez une table de base de données pour que les colonnes contenues dans cette table s'affichent dans la zone **Colonnes de la table sélectionnée**.

Remarque :

a. Cliquez sur l'icône représentant des jumelles pour rechercher une table dans la liste **Tables de base de données**.

b. Toutes les tables s'affichent par défaut. Vous pouvez filtrer les tables affichées, en sélectionnant une option de filtre différente. Les options de filtre disponibles sont présentées dans le Tableau 267, à la page 1327.

Tableau 267. Options de filtre

Option de filtre	Description
Tous	Afficher toutes les tables
Utilisateur	Afficher uniquement les tables utilisateur
System	Afficher uniquement les tables système
Visualiser	Afficher uniquement les vues de base de données

Remarque : Pour récupérer des colonnes spécifiques, sélectionnez uniquement ces colonnes. Si vous sélectionnez la table, Agent Builder génère automatiquement une requête collectant toutes les colonnes de la table et crée des attributs pour toutes les colonnes qui se trouvent actuellement dans la table.

Vous pouvez sélectionner des colonnes en procédant comme suit :

- Sélectionnez la table et obtenez la requête par défaut pour toutes les colonnes.
- Sélectionnez des colonnes pour extraire uniquement ces colonnes.

7. Facultatif : Modifiez les valeurs d'énumération définies pour Erreur, Données manquantes et Aucune valeur dans la page **Informations d'attribut**.

   Modifiez les valeurs pour éviter tout chevauchement avec les valeurs légitimes qui risquent d'être renvoyées par les colonnes des tables de base de données.
8. Facultatif : Cliquez sur **Tester** dans la fenêtre **Navigateur JDBC (Java Database Connectivity)** pour tester et modifier l'instruction SQL.

   La fenêtre **Exécuter l'instruction SQL** s'affiche.

   a) Entrez ou modifiez l'instruction SQL dans la zone **Instruction SQL**.

   b) Cliquez sur **Exécuter** pour exécuter l'instruction SQL.

      Les résultats s'affichent dans la zone **Résultats**. Continuez de modifier et tester l'instruction jusqu'à ce que vous soyez satisfait des données renvoyées.

   c) Cliquez sur **OK** pour sauvegarder l'instruction, créez les attributs appropriés et revenez à la fenêtre **Informations JDBC**.
9. Facultatif : Cliquez sur **Tester** dans la fenêtre **Informations JDBC** pour tester le groupe d'attributs dans un environnement d'agent plus réaliste. Pour plus d'informations sur la procédure de test des groupes d'attributs JDBC, voir «Test des groupes d'attributs JDBC», à la page 1332. Si vous modifiez l'instruction JDBC au cours de ce test, vous devez également ajuster les attributs de sorte à inclure un attribut par colonne renvoyée par l'instruction JDBC, dans l'ordre correct.
10. Facultatif : Vous pouvez créer un filtre pour limiter les données renvoyées par ce groupe d'attributs en cliquant sur **Avancé**. Pour plus d'informations sur le filtrage de données à partir d'un groupe d'attributs, voir «Filtrage des groupes d'attributs», à la page 1237.
11. Sur la page **Informations JDBC**, dans la section **Systèmes d'exploitation**, sélectionnez les systèmes d'exploitation, puis cliquez sur **Suivant**. Voir «Spécification des systèmes d'exploitation», à la page 1249 pour déterminer les systèmes d'exploitation à sélectionner.

    Remarque : Cliquez sur **Insérer une propriété de configuration** pour sélectionner une propriété à insérer. Pour plus d'informations, voir «Personnalisation de la configuration de l'agent», à la page 1404.
12. Sur la page **Sélectionner les attributs clés**, sélectionnez les attributs de clé ou indiquez que la source de données génère uniquement une ligne de données. Pour plus d'informations, voir «Sélection des attributs de clé», à la page 1206.
13. Si vous voulez tester une source de données précédemment définie, dans la fenêtre de l'éditeur d'agent, sélectionnez l'onglet **Sources de données** et une source de données JDBC. Dans la zone **Informations de groupe d'attributs JDBC**, cliquez sur **Tester**. Pour plus d'informations sur la procédure de test, voir «Test des groupes d'attributs JDBC», à la page 1332.
14. Pour afficher les sections de configuration qui ont automatiquement été générées, cliquez sur l'onglet **Insérer une propriété de configuration** de l'éditeur d'agent.

    Vous pouvez modifier les libellés et les valeurs par défaut de ces propriétés de configuration de sorte qu'ils correspondent aux valeurs par défaut présentées aux utilisateurs lors de la configuration initiale de l'agent.
15. Facultatif : Effectuez les opérations de la page **Information d'attribut** ; pour plus d'informations, voir «Zones et options de définition des attributs», à la page 1232. Effectuez cette étape si vous avez choisi de créer manuellement la source de données JDBC sans cliquer sur Parcourir à l'étape «4», à la page 1326.

    La source de données JDBC d'Agent Builder prend en charge la collecte de données de la plupart des types SQL. Le Tableau 268, à la page 1329 décrit le type d'attribut créé par le navigateur JDBC lorsqu'il détecte une colonne d'un de ces types. Il s'agit des types de données pris en charge pour une utilisation avec un agent de surveillance.

Tableau 268. Types de données SQL pris en charge pour utilisation avec un agent de surveillance

Type de données SQL	Attribut IBM Tivoli Monitoring créé
BIGINT	Ce type de données est une valeur de jauge 64 bits dans IBM Tivoli Monitoring. Si vous sélectionnez la compatibilitéIBM Tivoli Monitoring V6.2, il s'agit d'une jauge 32 bits.
DECIMALDOUBLEFLOATNUMERICREAL	Ces types SQL sont créés sous forme d'attributs de jauge 64 bits dans IBM Tivoli Monitoring. Si les métadonnées de base de données contiennent une valeur de type échelle, cette valeur est utilisée ; dans le cas contraire, l'échelle est paramétrée sur 1. Si vous sélectionnez la compatibilité IBM Tivoli Monitoring V6.2, l'attribut est une jauge 32 bits.
BITINTEGERSMALLINTTINYINT	Les types SQL suivants sont créés sous forme d'attributs de jauge 32 bits dans IBM Tivoli Monitoring.
BOOLEAN	Cette valeur est une jauge 32 bits dans IBM Tivoli Monitoring avec des énumérations pour TRUE et FALSE.
TIMESTAMP	Les données des colonnes de ce type sont converties en attribut d'horodatage IBM Tivoli Monitoring de 16 octets.
TIMEDATECHARLONGVARCHARVARCHAR	Ces types SQL sont tous traités sous forme d'attributs de chaîne par le navigateur. La taille de colonne est utilisée comme taille d'attribut jusqu'à 256, ce qui correspond à la taille d'attribut de chaîne par défaut pour le navigateur JDBC.

Remarque : Si vous collectez des données d'un type de données non répertorié, un attribut de chaîne est utilisé par défaut. L'agent tente également de collecter les donnés de la base de données sous la forme d'une chaîne.

Modifiez les valeurs d'énumération définies pour Erreur, Données manquantes et Aucune valeur dans la page **Informations d'attribut**, si nécessaire. Modifiez les valeurs pour éviter tout chevauchement avec les valeurs légitimes qui risquent d'être renvoyées par les colonnes des tables de base de données.

Configuration JDBC

Lorsque vous définissez une source de données JDBC dans l'agent, des propriétés de configuration sont créées automatiquement.

Si vous définissez une source de données JDBC dans votre agent, celui-ci doit utiliser Java pour se connecter au serveur de base de données JDBC. Les propriétés de configuration Java s'ajoutent automatiquement à l'agent. Les propriétés de configuration Java suivantes sont propres à la configuration d'exécution de l'agent :

- *Répertoire de base Java* : Chemin complet pointant vers le répertoire d'installation Java.
- *Arguments JVM* : Ce paramètre permet d'indiquer une liste facultative d'arguments pour la machine virtuelle Java.
- *Niveau de trace* : Ce paramètre définit la quantité d'informations à écrire dans le fichier journal de trace Java. Par défaut, seules les données d'erreur sont écrites dans le fichier journal.

Remarque : Agent Builder n'a pas besoin des propriétés Java, dans la mesure où il utilise sa propre JVM et sa propre consignation qui sont configurées via le plug-in JLog.

Si vous définissez une source de données JDBC dans votre agent, les zones de configuration courantes obligatoires suivantes s'ajoutent automatiquement à l'agent :

- *Type de base de données JDBC* : Type de la base de données à laquelle vous vous connectez : IBM DB2, Microsoft SQL Server ou serveur de base de données Oracle.
- *Nom d'utilisateur JDBC* : nom d'utilisateur servant à l'authentification sur le serveur de base de données.
- *Mot de passe JDBC* : mot de passe servant à l'authentification sur le serveur de base de données.
- *Chemins de base* : liste des répertoires dans lesquels les fichiers JAR nommés dans la zone *Chemin d'accès aux classes* doivent être recherchés ou répertoires indiqués dans la zone *Répertoires JAR* qui ne sont pas complètement qualifiés. Les noms de répertoire sont séparés par un point-virgule (`;`) sur Windows, et par un point virgule ((`;`) ou deux points (`:`) sur les systèmes UNIX.
- *Chemin d'accès aux classes* : fichiers JAR nommés explicitement dans lesquels l'agent doit effectuer la recherche. Les répertoires qui ne sont pas complètement qualifiés s'ajoutent à chacun des chemins de base tant que le répertoire n'est pas trouvé.
- *Répertoires JAR* : liste des répertoires dans lesquels les fichiers JAR sont recherchés. Les noms de répertoire sont séparés par un point-virgule (`;`) sur Windows, et par un point virgule ((`;`) ou deux points (`:`) sur les systèmes UNIX. Les fichiers JAR de ces répertoires n'ont pas besoin d'être identifiés explicitement ; ils seront détectés, car ils se trouvent dans l'un de ces répertoires. La recherche ne s'applique pas aux sous-répertoires de ces répertoires. Les répertoires qui ne sont pas complets s'ajoutent à chacun des chemins de base tant que le répertoire n'est pas trouvé.

La configuration d'exécution exige également que vous indiquiez quelques détails supplémentaires pour vous connecter à la base de données. Vous pouvez choisir comment spécifier les éléments de configuration restants, sous la forme d'une adresse URL JDBC ou de propriétés de configuration de base (spécification par défaut) :

- Option de configuration d'adresse URL
  - Adresse URL de connexion JDBC : adresse URL de connexion spécifique du fournisseur qui fournit des informations sur l'hôte hébergeant la base de données et sur le numéro de port de connexion. Le format d'adresse URL se présente généralement comme suit :

    ```
    jdbc:identificateur://serveur:port/base de données
    ```

    Voir la documentation du fournisseur de pilote JDBC pour les différents formats d'adresse URL.
- Option de propriétés de base JDBC (par défaut)

  Nom du serveur JDBC : Nom de l'hôte sur lequel le serveur de base de données est en cours d'exécution.

  Nom de base de données JDBC : Nom de la base de données sur l'hôte sur lequel la connexion est établie.

  Numéro de port JDBC : Numéro du port d'écoute du serveur de base de données.

Remarque : Le fournisseur de données JDBC vous permet de surveiller plusieurs types de base de données dans le même agent à l'aide de sous-noeuds. Pour ce faire, vous devez soigneusement définir les substitutions de configuration de sous-noeud. Si vous surveillez plusieurs types de base de données, les paramètres de configuration suivants seront sûrement différents :

- Type de base de données JDBC
- Nom d'utilisateur JDBC
- Mot de passe JDBC

Si vous utilisez l'option de configuration de base, vous devez également définir des substitutions pour les propriétés suivantes sur la page **Substitutions de configuration de sous-noeud** :

- Nom du serveur JDBC

- Numéro de port JDBC
- Nom de base de données JDBC

Pour définir les substitutions de configuration pour votre sous-noeud, voir «Utilisation des sous-noeuds», à la page 1386 pour en savoir plus sur l'accès à la page **Substitutions de configuration de sous-noeud**. Lorsque vous configurez l'agent au moment de l'exécution, toutes ces propriétés doivent être configurées pour chaque instance de sous-noeud créée.

Outre les substitutions de sous-noeud, l'agent doit également pointer vers des pilotes JDBC pour chaque type de base de données auquel vous allez vous connecter depuis les sous-noeuds. Le paramètre *Répertoires JAR* constitue le moyen le plus pratique pour pointer vers les pilotes JDBC. Répertoriez les répertoires contenant les pilotes JDBC à l'aide d'un point-virgule pour séparer chaque répertoire. Par exemple, si vous vous connectez à des bases de données DB2 et Oracle avec l'agent, vous devez spécifier une valeur *Répertoires JAR* comme suit : `C:\Program Files\IBM\SQLLIB\java;C:\oracle\jdbc`.

Procédures stockées
Exemples de procédures stockées SQL et DB2 que vous pouvez utiliser avec le fournisseur de données JDBC.

Le fournisseur de données JDBC peut traiter les ensembles de résultats renvoyés par une procédure mémorisée. Les paramètres d'entrée de type chaîne ou entier peuvent être transmis à la procédure mémorisée. La syntaxe suivante exécute une procédure mémorisée :

```
call[:index] nom_procédure [argument] ...
```

Où :

index
Entier facultatif indiquant l'ensemble de résultats à utiliser par le fournisseur de données. Ce paramètre est utile lorsque la procédure stockée renvoie plusieurs ensembles de résultats et que vous voulez uniquement collecter les valeurs à partir d'un des ensembles de résultats. Si aucun index n'est indiqué, les données provenant de chaque ensemble de résultats sont collectées et renvoyées.

nom_procédure
Nom de la procédure mémorisée à exécuter par le fournisseur de données JDBC.

argument
Argument d'entrée de la procédure mémorisée. Si vous indiquez plusieurs arguments, séparez-les par un espace. Si l'argument contient un espace, placez la totalité de l'argument entre guillemets doubles. Si l'argument peut être analysé sous forme d'entier, il est transmis à la procédure mémorisée sous la forme d'un argument entier. Tout argument placé entre guillemets doubles est transmis sous la forme d'un argument de chaîne.

Exemples SQL Server
`call sp_helpdb`

Exécute la procédure `call sp_helpdb` qui ne nécessite aucun argument. Les données provenant de tous les ensembles de résultats renvoyés sont incluses dans les données renvoyées par le fournisseur de données.

`call:2 sp_helpdb master`

Exécute la procédure `sp_helpdb` avec l'argument principal. Cet argument est une argument d'entrée de chaîne. Seules les données provenant du second ensemble de résultats renvoyés par la procédure stockée sont incluses dans les données renvoyées par le fournisseur de données.

Lorsque l'index n'est pas indiqué, les données provenant de tous les ensembles de résultats renvoyés sont collectées. Vous devez vous assurer que les données renvoyées dans ces cas sont compatibles avec les attributs que vous définissez. Agent Builder crée des attributs à partir du premier ensemble de résultats renvoyés, et il est prévu que tous les autres ensembles de résultats attendus soient compatibles avec le premier.

Procédure mémorisée DB2

Voici un exemple de fonction DB2 écrite en SQL. Cette fonction explique comment renvoyer des résultats qui peuvent être traités par le fournisseur de données JDBC d'Agent Builder :

```
-- Run this script as follows:
-- db2 -td# -vf db2sample.sql

-- Procedure to demonstrate how to return a query from
-- a DB2 stored procedure, which can then be used by
-- an Agent Builder JDBC provider. The stored procedure
-- returns the following columns:
-- Name               Description              Data Type
-- current_timestamp  The current system time  timestamp
-- lock_timeout       The lock timeout         numeric scale 0
-- user               The user for the session String 128 characters long
DROP procedure db2sample#

CREATE PROCEDURE db2sample()
  RESULT SETS 1
  LANGUAGE SQL
BEGIN ATOMIC

  -- Define the SQL for the query
  DECLARE c1 CURSOR WITH HOLD WITH RETURN FOR
  SELECT CURRENT TIMESTAMP as current_timestamp,
CURRENT LOCK TIMEOUT as lock_timeout, CURRENT USER as user
  FROM sysibm.sysdummy1;

  -- Issue the query and return the data
  OPEN c1;
END#
```

Cette fonction peut être appelée à partir d'Agent Builder à l'aide de la même syntaxe que celle définie pour les autres procédures stockées. Dans ce cas, vous définissez `call db2sample` comme votre instruction JDBC afin d'exécuter cette procédure stockée.

Procédures stockées Oracle

Les procédures stockées Oracle ne renvoient pas d'ensembles de résultats. En revanche, vous devez écrire une fonction renvoyant un curseur de référence Oracle. Voici un exemple de fonction Oracle écrite en PL/SQL expliquant comment renvoyer des résultats qui peuvent être traités par le fournisseur de données JDBC d'Agent Builder :

```
CREATE OR REPLACE FUNCTION ITMTEST
RETURN SYS_REFCURSOR
IS
        v_rc SYS_REFCURSOR;
BEGIN
  OPEN v_rc FOR SELECT * FROM ALL_CLUSTERS;
  RETURN v_rc;
END;
```

Cette fonction peut être appelée à partir d'Agent Builder à l'aide de la même syntaxe que celle définie pour les autres procédures stockées. Dans ce cas, vous définissez `call ITMTEST` comme instruction JDBC afin d'exécuter cette procédure stockée. Dans la mesure où la fonction Oracle doit renvoyer une référence de curseur, un seul ensemble de résultats peut être traité par les fonctions Oracle. En d'autres termes, l'option d'index n'est pas prise en charge pour Oracle car il n'existe aucun moyen pour renvoyer plusieurs ensembles de résultats.

Test des groupes d'attributs JDBC

Vous pouvez tester le groupe d'attributs JDBC que vous avez créé, dans Agent Builder.

Procédure

1. Vous pouvez démarrer la procédure de test de l'une des manières suivantes :
   - Lors de la création de l'agent, cliquez sur **Tester** à la page **Informations JDBC**.

- Après la création de l'agent, sélectionnez un groupe d'attributs à la page **Définition de la source de données** de l'éditeur d'agent et cliquez sur **Tester**. Pour plus d'informations sur l'éditeur d'agent, voir «Utilisation de l'éditeur d'agent pour modifier l'agent», à la page 1207.

Après avoir cliqué sur **Tester** dans l'une des deux étapes précédentes, la fenêtre **Test de l'instruction JDBC** s'affiche.

2. Facultatif : Avant de démarrer le test, vous pouvez définir les variables d'environnement, les propriétés de configuration, ainsi que des informations Java.

   Pour plus d'informations, voir «Test des groupes d'attributs», à la page 1420. Pour plus d'informations sur les propriétés de configuration JDBC, voir («Configuration JDBC», à la page 1329).
3. Cliquez sur l'option de **démarrage de l'agent**.

   Une fenêtre indique que l'agent est en cours de démarrage.
4. Pour simuler une demande de données d'agent provenant de Tivoli Enterprise Portal ou de SOAP, cliquez sur **Collecte de données**.

   L'agent interroge la base de données avec la requête SQL spécifiée. La fenêtre **Test de l'instruction JDBC** collecte et affiche toutes les données du cache de l'agent depuis son dernier démarrage.

   Remarque : L'ordre des données renvoyées est significatif. Par exemple, la valeur figurant dans la première colonne renvoyée est toujours affectée au premier attribut. Si vous modifiez l'instruction JDBC, vous devez ajouter, supprimer ou réorganiser les attributs de sorte qu'ils correspondent aux colonnes renvoyées par l'instruction.
5. Facultatif : Cliquez sur **Vérifier les résultats** si les données renvoyées ne sont pas celles que vous attendez.

   La fenêtre **Statut de la collecte de données** affiche des informations supplémentaires sur les données. Les données collectées et affichées par la fenêtre Statut de la collecte de données sont décrites dans «Noeud de statut d'objet de performances», à la page 1466
6. Arrêtez l'agent en cliquant sur **Arrêter l'agent**.
7. Cliquez sur **OK** ou **Annuler** pour quitter la fenêtre **Test de l'instruction JDBC**. Cliquez sur **OK** pour sauvegarder les modifications que vous avez apportées.

Concepts associés

«Test de votre agent dans Agent Builder», à la page 1420
Après avoir utilisé Agent Builder pour créer un agent, vous pouvez tester l'agent dans Agent Builder.

Surveillance de la disponibilité du système avec des commandes Ping

Vous pouvez définir une source de données pour qu'elle teste la liste des périphériques réseau à l'aide de la commande PING (echo) d'ICPM (Internet Control Message Protocol). Les noms d'hôte ou adresses IP des périphériques à tester sont répertoriés dans un ou plusieurs des fichiers de la liste des périphériques. Un fichier de configuration Ping distinct spécifie le chemin d'accès de chaque fichier de la liste des périphériques. Le nom du fichier de configuration Ping est ensuite défini dans la configuration d'exécution de l'agent. Les résultats incluent le statut de chaque périphérique réseau.

Avant de commencer

Créez les fichiers de la liste des périphériques et un fichier de configuration ping (voir «Fichiers de configuration», à la page 1334).

Pourquoi et quand exécuter cette tâche

Une partie de la gestion de réseau consiste à déterminer si les systèmes répondent à une commande Ping ICMP (Internet Control Message Protocol). Utilisez cette source de données afin de surveiller le statut de base en ligne et hors ligne d'un ensemble de serveurs ou d'autres périphériques critiques dans votre environnement. La surveillance avec Ping est simple et ne surcharge que très peu le système. Pour surveiller une liste de périphériques, ajoutez le collecteur de données Ping à votre agent.

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, cliquez sur **Données de gestion de réseau** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **Ping**.
3. Cliquez sur **Suivant**.
4. Dans la zone **Systèmes d'exploitation** de la fenêtre **Informations sur le Ping**, sélectionnez les systèmes d'exploitation.
5. Facultatif : Vous pouvez tester ce groupe d'attributs en cliquant sur **Tester**. Pour plus d'informations sur le test, voir «Test des groupes d'attributs Ping», à la page 1335.
6. Facultatif : Vous pouvez créer un filtre pour limiter les données renvoyées par ce groupe d'attributs en cliquant sur **Avancé**. Pour plus d'informations sur le filtrage de données à partir d'un groupe d'attributs, voir «Filtrage des groupes d'attributs», à la page 1237.
7. Effectuez l'une des opérations suivantes :

   a) Si vous utilisez l'assistant **d'agent**, cliquez sur **Suivant**.

   b) Cliquez sur **Terminer** pour sauvegarder la source de données et ouvrir l'éditeur d'agent.
8. Pour plus d'informations sur l'ajout d'attributs, voir («Création d'attributs», à la page 1229).

Résultats

Pour plus d'informations sur le groupe d'attributs relatif au Ping, voir «Groupe d'attributs Ping», à la page 1495.

Fichiers de configuration

Vous fournissez à l'agent la liste des unités auxquelles une commande ping doit être envoyée, à l'aide de fichiers de configuration.

L'agent requiert deux types de fichier de configuration.

Fichier de la liste des unités

Inclut une liste des unités auxquelles une commande ping doit être envoyée. Si vous avez plusieurs unités, vous pouvez les répartir dans plusieurs fichiers de liste d'unités. L'agent démarre une unité d'exécution distincte pour chaque fichier de liste d'unités et les parcourt en parallèle. Il parcourt chaque fichier toutes les 60 secondes ou toutes les 30 secondes auxquelles est ajouté le temps d'exécution de la commande ping sur la liste, le temps le plus long étant retenu.

La syntaxe du fichier de la liste des unités est la suivante :

```
LISTNAME=nom_liste
nom_unité ou nom_hôte
nom_unité ou nom_hôte
nom_unité ou nom_hôte nom_unité ou nom_hôte
```

Où *nom_liste* est une description des unités dans ce fichier. Si aucun nom de liste n'est défini, le nom du fichier liste de périphériques est utilisé. Il n'est pas nécessaire que le nom de liste soit la première entrée du fichier. Toutefois, si le fichier contient plusieurs définitions de nom de liste, la dernière définition est utilisée.

Le nombre d'unités que vous pouvez inclure dans un fichier de liste d'unités n'est pas limité. Toutefois, le fait d'inclure trop d'entrées diminue l'intérêt d'avoir une liste ciblée de périphériques critiques et augmente la charge de travail globale. Il risque d'être plus difficile d'extraire le statut de chaque unité dans l'intervalle de surveillance de 60 secondes.

Au début de chaque cycle, l'agent vérifie l'heure de la dernière modification du fichier de liste d'unités. Si l'heure de la dernière modification du fichier est plus récente que la dernière lecture du fichier par l'agent, l'agent relit le fichier sans avoir à redémarrer.

Fichier de configuration de Ping

Indique l'emplacement du fichier de liste d'unités. Utilisez le chemin complet ou un chemin relatif à l'emplacement du fichier de configuration ping. Le fichier de configuration ping est transmis comme paramètre de configuration d'exécution à l'agent.

Exemple

Dans l'exemple ci-après, les périphériques sont divisés en deux fichiers.
Le fichier `/data/retailList.txt` contient les entrées suivantes :

```
LISTNAME=Retail
frontend.mycompany.com
productdb.mycompany.com
```

Le fichier `/data/manufacturingList.txt` contient les entrées suivantes :

```
LISTNAME=Manufacturing systems
manufloor.mycompany.com
stats.supplier.com
```

Le fichier ping, `/data/pinglists.txt`, contient les entrées suivantes :

```
/data/retailList.txt
/data/manufacturingList.txt
```

Propriété de configuration de la gestion de réseau

Une fois qu'une source de données est ajoutée, la configuration apparaît sur la page **Configuration d'exécution** de l'éditeur d'agent.

La section **Gestion de réseau** de la page **Informations de configuration d'exécution** contient les propriétés suivantes :

Tableau 269. Propriétés de configuration de la gestion de réseau

Nom	Valeurs admises	Obligatoire	Description
`Fichier de configuration de Ping`	Chemin de fichier	Non. Si ce fichier n'est pas fourni, le fichier `KUMSLIST` situé dans le répertoire bin de l'agent est utilisé.	Chemin d'accès au fichier contenant une liste de fichiers qui, eux-mêmes, contiennent une liste d'hôtes à surveiller via des pings ICMP.

Test des groupes d'attributs Ping
Vous pouvez tester le groupe d'attributs Ping que vous avez créé dans Agent Builder.

Procédure

1. Vous pouvez démarrer la procédure de test de l'une des manières suivantes :
   - Lors de la création de l'agent, cliquez sur **Tester** sur la page **Informations sur le Ping**.
   - Après la création de l'agent, sélectionnez un groupe d'attributs à la page **Définition de la source de données** de l'éditeur d'agent et cliquez sur **Tester**. Pour plus d'informations sur l'éditeur d'agent, voir «Utilisation de l'éditeur d'agent pour modifier l'agent», à la page 1207.

   Lorsque vous cliquez sur **Tester** dans l'une des deux étapes précédentes, la fenêtre **Tester les paramètres** s'affiche.
2. Facultatif : Avant de démarrer le test, vous pouvez définir des variables d'environnement et des propriétés de configuration. Pour plus d'informations, voir «Test des groupes d'attributs», à la page 1420.
3. Cliquez sur **Parcourir** pour sélectionner un fichier de configuration de Ping. Pour plus d'informations sur les fichiers de configuration de Ping, voir «Fichiers de configuration», à la page 1334.
4. Cliquez sur l'option de **démarrage de l'agent**. Une fenêtre indique que l'agent est en cours de démarrage.

5. Pour simuler une demande de données d'agent provenant de l'environnement de surveillance, cliquez sur **Collecter des données**. L'agent envoie une commande Ping aux périphériques spécifiés dans le fichier de liste de périphériques, référencé à partir du fichier de configuration de Ping.
6. La fenêtre **Paramètres de test** collecte et affiche toutes les données du cache de l'agent depuis son dernier démarrage.
7. Facultatif : Cliquez sur **Vérifier les résultats** si les données renvoyées ne sont pas celles que vous attendez.

   La fenêtre **Statut de la collecte de données** affiche des informations supplémentaires sur les données. Les données collectées et affichées dans la fenêtre Statut de la collecte de données sont décrites dans «Noeud de statut d'objet de performances», à la page 1466.
8. Arrêtez l'agent en cliquant sur **Arrêter l'agent**.
9. Cliquez sur **OK** ou sur **Annuler** pour quitter la fenêtre **Tester les paramètres**. Cliquez sur **OK** pour sauvegarder les modifications que vous avez apportées.

Concepts associés

«Test de votre agent dans Agent Builder», à la page 1420
Après avoir utilisé Agent Builder pour créer un agent, vous pouvez tester l'agent dans Agent Builder.

Surveillance de la disponibilité et du temps de réponse HTTP

Vous pouvez configurer une source de données pour qu'elle surveille la disponibilité et le temps de réponse des URL sélectionnées. Utilisez un fichier de configuration pour définir la liste des URL. Définissez le nom du fichier dans la configuration d'exécution de l'agent. Dans IBM Tivoli Monitoring, vous pouvez également utiliser des commandes Action pour ajouter et supprimer des URL surveillées. Le statut de chaque URL est ajouté sous la forme d'une ligne dans l'ensemble de données obtenu.

Pourquoi et quand exécuter cette tâche

Pour chaque URL surveillée, les résultats fournissent des informations générales sur la réponse HTTP à la requête HTTP. Ces résultats précisent notamment s'il est possible de l'extraire, la durée de l'extraction et la taille de la réponse. Si le contenu de la réponse est HTML, des informations sont également fournies sur les objets de page dans l'URL.

Vous pouvez surveiller les URL qui utilisent les protocoles HTTP, HTTPS, FTP et de fichier. Vous devez indiquer les URL à surveiller dans le fichier d'URL HTTP ou via les options Action.

Important : Au moment de la publication, les commandes Action ne sont pas disponibles dans un environnement IBM Cloud Application Performance Management. Elles sont uniquement disponibles dans un environnement Tivoli Monitoring.

Cette source de données nécessite un environnement d'exécution Java. Les versions de Java suivantes sont prises en charge :

- Oracle Corporation Java version 5 ou ultérieure
- IBM Corporation Java version 5 ou ultérieure

Pour créer un groupe d'attributs afin de surveiller une liste d'URL, procédez comme suit :

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, cliquez sur **Données d'un serveur** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **HTTP**.
3. Cliquez sur **Suivant**.
4. Sur la page **Informations HTTP**, sélectionnez un ou plusieurs systèmes d'exploitation dans la zone **Systèmes d'exploitation**.
5. Facultatif : Cliquez sur **Tester** pour tester ce groupe d'attributs. Pour plus d'informations sur le test, voir «Test des groupes d'attributs HTTP», à la page 1343.

6. Facultatif : Cliquez sur **Avancé** pour créer un filtre afin de limiter les données renvoyées par ce groupe d'attributs. Pour plus d'informations sur le filtrage de données à partir d'un groupe d'attributs, voir «Filtrage des groupes d'attributs», à la page 1237.
7. Effectuez l'une des opérations suivantes :
   a) Si vous utilisez l'assistant **d'agent**, cliquez sur **Suivant**.
   b) Cliquez sur **Terminer** pour sauvegarder la source de données et ouvrir l'éditeur d'agent.

Résultats
La source de données HTTP crée deux groupes d'attributs : URL gérées et objets URL. Vous pouvez ajouter, modifier ou supprimer des attributs.

Tâches associées
«Création d'attributs», à la page 1229
Vous pouvez ajouter de nouveaux attributs à un ensemble de données.

Référence associée
«Groupes d'attributs HTTP», à la page 1498
Les deux groupes d'attributs HTTP, `URL gérées` et `Objets d'URL`, permettent de recevoir des informations depuis les URL et les objets qu'elles contiennent.

Tables HTTP
Informations de référence sur les groupes d'attributs HTTP par défaut.

La source de données HTTP crée les deux groupes d'attributs suivants :

`URL gérées`
La table des URL gérées fournit des données sur la disponibilité et le temps de réponse de chaque URL surveillée.

`Objets d'URL`
Le tableau des objets d'URL contient une entrée d'URL séparée pour chaque objet intégré. Par exemple, les fichiers `.gif` et `.jpg` sont susceptibles d'être utilisés dans le site Web indiqué sur le rapport relatif aux URL gérées.

Pour plus d'informations sur la syntaxe utilisée dans les tables des URL gérées et des objets d'URL, voir («Zones spécifiques des attributs HTTP», à la page 1338).

Lorsque vous devez surveiller le temps de réponse et la disponibilité d'objets spécifiques dans un site Web, révisez le contenu de la table des objets d'URL. La table des objets URL permet de surveiller une liste spécifiques d'objets détectés dans les fichiers HTML téléchargés. La table répertorie les éléments HTML où sont recherchés les objets à surveiller et les attributs qui désignent ces objets au sein de ces éléments :

Tableau 270. Eléments HTML sur lesquels les objets à surveiller sont recherchés

Elément HTML	**Attribut contenant l'objet à surveiller**
`img`	`src`
`script`	`src`
`embed`	`src`
`object`	`codebase` ou `data`
`body`	`background`
`input`	`src`

Dans l'extraction HTML de l'exemple suivant, l'objet surveillé est l'image désignée par l'attribut `src` de l'élément `img`.

```
<img src="/v8/images/id-w3-sitemark-simple.gif" alt="" width="54" height="33" />
```

Une adresse URL complète d'accès à l'image est définie en fonction de l'URL d'accès au document source.

Remarque : Si vous ne souhaitez pas surveiller les objets trouvés sur une page Web, dans la section de configuration de la surveillance des URL, définissez la propriété **collecte d'objets de la page** sur **Non**.

Zones spécifiques des attributs HTTP

Sur la page **Information d'attribut**, deux zones pour les attributs HTTP permettent de définir le mode de collecte des données à partir de l'URL. La zone **Type d'attribut** peut comprendre toute valeur d'une liste qui contrôle les informations sur l'URL renvoyée. Certains types d'attribut nécessitent une valeur dans la zone **Valeur du type**.

La table suivante décrit tous les types d'attribut du groupe d'attributs des URL gérées et la valeur du type lorsqu'elle doit être précisée :

Tableau 271. Informations d'attributs HTTP - URL gérées

Type d'attribut	Description	Valeur du type	Type de données renvoyées	Différences avec les protocoles FTP et de fichier
`Requête XPath`	Permet d'exécuter une requête XPath sur le contenu renvoyé depuis une connexion d'URL. La requête doit être écrite pour renvoyer des données utiles à un attribut, et non une liste de noeuds.	Requête XPath à exécuter sur le contenu obtenu d'une connexion à l'URL.	Les données renvoyées peuvent être une chaîne, une valeur numérique ou une valeur d'horodatage. Si les données sont au format XML DateTime, vous pouvez spécifier horodatage comme type d'attribut. L'agent convertit la valeur en horodatage Candle.	Aucun
`Temps de réponse`	Quantité de temps en millisecondes pris par le téléchargement du contenu depuis l'URL demandée.	Aucun	Entier (nombre de millisecondes)	Aucun
`Message de réponse`	Message de réponse HTTP renvoyé par le serveur.	Aucun	Chaîne	Le message de réponse s'applique uniquement si l'URL utilise les protocoles HTTP ou HTTPS.

Tableau 271. Informations d'attributs HTTP - URL gérées (suite)

Type d'attribut	Description	Valeur du type	Type de données renvoyées	Différences avec les protocoles FTP et de fichier
`Code de réponse`	Code de réponse HTTP renvoyé par serveur.	Aucun	Entier	Le code de réponse s'applique uniquement si l'URL utilise les protocoles HTTP ou HTTPS. Il est toujours de 0 pour les URL de fichier ou de protocole FTP.
`Longueur de la réponse`	Taille du contenu en octets qui a été téléchargé depuis l'URL demandée	Aucun	Entier (taille en octets)	Aucun
`En-tête de réponse`	L'en-tête de réponse permet d'extraire une valeur depuis l'une des zones d'en-tête de réponse d'URL. L'argument indique quelle est la zone demandée.	En-tête de réponse à collecter.	Chaîne	Généralement, les protocoles FTP et de fichier ne comportent pas d'en-têtes à collecter.
`URL de demande`	La connexion à cette URL est établie. Tous les mots clés de réponse fournissent des informations sur la connexion à cette URL. La requête XPath permet d'obtenir des informations provenant du contenu renvoyé par l'accès à cette URL.	Aucun	Chaîne	Aucun
`Objets de page`	Nombre d'objets reconnus sur la page HTML surveillée et qui sont eux-mêmes surveillés par le groupe d'attributs d'objets d'URL.	Aucun	Entier	Aucun

Tableau 271. Informations d'attributs HTTP - URL gérées (suite)				
Type d'attribut	**Description**	**Valeur du type**	**Type de données renvoyées**	**Différences avec les protocoles FTP et de fichier**
`Taille totale des objets`	Taille totale des objets surveillés dans le groupe d'attributs d'objets d'URL pour cette page Web.	Aucun	Entier (en octets)	Aucun
`Alias`	Alias spécifié par l'utilisateur pour cette URL.	Aucun	Chaîne	Aucun
`Utilisateur`	Données spécifiées par l'utilisateur pour cette URL.	Aucun	Chaîne	Aucun

La table suivante décrit les types d'attribut du groupe d'attributs d'objets d'URL :

Tableau 272. Informations d'attributs HTTP - Objets URL				
Type d'attribut	**Description**	**Valeur du type**	**Type de données renvoyées**	**Différences avec les protocoles FTP et de fichier**
`URL`	URL surveillée dans la table des URL gérées.	Aucun	Chaîne	Aucun
`Nom d'objet`	URL de l'objet qui est surveillé dans la page **HTML**.	Aucun	Chaîne	Aucun
`Taille de l'objet`	Taille en octets du contenu téléchargé depuis l'URL du nom d'objet.	Aucun	Numérique	Aucun
`Temps de réponse de l'objet`	Temps en millisecondes pris par le téléchargement de l'objet de page.	Aucun	Numérique	Aucun

Surveillance d'une URL

Vous pouvez commencer à surveiller n'importe quelle URL en l'incluant dans le fichier d'URL ou en utilisant l'option d'ajout d'URL HTTP.

Fichier d'URL

Le fichier d'URL spécifié dans la configuration peut se trouver dans n'importe quel répertoire. Si ce fichier n'existe pas ou s'il est vide, vous pouvez démarrer la surveillance d'URL à l'aide des commandes Action. Pour plus d'informations, voir «Option Action», à la page 1341. Si vous disposez déjà d'un agent Tivoli Universal Agent utilisant le fournisseur de données Tivoli Universal Agent HTTP, vous pouvez réutiliser le fichier KUMPURLS. Lorsque vous configurez l'agent, pointez vers votre fichier KUMPURLS.

Le tableau suivant fournit des exemples montrant comment les URL sont saisies dans le fichier d'URL, en fonction de la méthode avec laquelle elles ont été ajoutées.

Tableau 273. Entrées de fichiers d'URL

URL	Ajoutée par

`www.bbc.co.uk`
`http://weather.com`
`www.ibm.com`
	Ajout manuel d'entrées dans le fichier. Si aucun protocole n'est spécifié comme dans l'exemple `www.ibm.com`, http est considéré comme le protocole par défaut.

`ftp://userid:password@ftpserver/index.html`	Ajout manuel par protocole FTP (File Transfer Protocol)
`http://www.ibm.com USER=ibm ALIAS=ibm`	Action d'ajout d'URL HTTP
`file:/tmp/samples.html USER=samples \` `ALIAS=samples`	Action d'ajout d'URL HTTP par FTP
`http://google.com INTERVAL=60 CACHE=50 \` `USER=google ALIAS=search`	Exemple du fichier KUMPURLS de Tivoli Universal Agent

Lorsque vous éditez directement le fichier d'URL, vos changements sont mis en oeuvre dès la prochaine collecte de données par l'agent.

Option Action

Vous pouvez également indiquer des URL à surveiller via une option Action appelée `Ajouter une URL HTTP`.

Restriction : Cette option n'est pas disponible dans l'édition actuelle d'IBM Cloud Application Performance Management, car vous ne pouvez pas lancer de commandes Action manuellement.

Lorsque cette option est sélectionnée, une fenêtre permettant d'indiquer les paramètres suivants s'affiche :

URL
Paramètre obligatoire représentant l'URL elle-même. Vous pouvez entrer ce paramètre avec ou sans le préfixe `http://` ou le préfixe `https://`.

Alias
Paramètre facultatif que vous pouvez indiquer pour associer un nom plus significatif à une URL. Aucun espace n'est autorisé dans ce paramètre. Si ce paramètre n'est pas indiqué, la zone du nom d'alias est vide par défaut.

Données_Utilisateur
Paramètre facultatif que vous pouvez indiquer pour entrer des données sur l'URL. Si ce paramètre n'est pas indiqué, la valeur par défaut de `Données_Utilisateur` est `INITCNFG`.

Après avoir fourni toutes les informations et fermé la fenêtre, affectez l'action `Ajouter une URL HTTP` au système géré de destination associé à l'agent. La surveillance commence immédiatement pour la nouvelle URL. L'URL est également ajoutée au fichier d'URL et reste ainsi surveillée pendant tous les redémarrages de l'agent.

Une option Action correspondante est nommée `Supprimer une URL HTTP`. Utilisez l'action `Supprimer une URL HTTP` pour arrêter immédiatement la surveillance d'une URL particulière. L'URL est également supprimée du fichier d'URL. La fenêtre de **suppression d'URL HTTP** demande uniquement les valeurs URL et `Données_Utilisateur`. Les valeurs URL et `Données_Utilisateur` doivent correspondre aux valeurs affichées dans Tivoli Enterprise Portal. Sinon, l'action de suppression échoue. Par exemple, si vous avez omis le préfixe `http://` dans la zone URL de l'action d'ajout, vous devez l'inclure dans la zone URL de l'action de suppression. Si vous n'avez pas indiqué de `données_utilisateur`, vous devez indiquer `INITCNFG` comme dans Tivoli Enterprise Portal.

Si une URL est ajoutée manuellement au fichier d'URL, vous pouvez la supprimer à l'aide de la commande Action, à condition de fournir les valeurs déjà indiquées dans Tivoli Enterprise Portal. Par exemple, si vous avez ajouté `www.ibm.com` à votre fichier d'URL, Tivoli Enterprise Portal affiche `http://www.ibm.com` comme URL et `INITCNFG` comme `données_utilisateur`. Pour supprimer l'URL à l'aide de la commande Action, vous devez utiliser les valeurs affichées dans Tivoli Enterprise Portal.

Après avoir fourni toutes les informations et fermé la fenêtre, affectez l'action `Supprimer une URL` HTTP au système géré de destination associé à l'agent.

Surveillance des URL `https://`
La source de données HTTP permet de surveiller uniquement les URL `https://` sécurisées ne nécessitant pas d'accès par script ou d'invite interactive.

Si l'URL `https://` peut être extraite avec un appel HTTP Get standard, elle peut aussi être surveillée.

Serveur proxy
Si le système où l'agent s'exécute nécessite un proxy pour accéder au fournisseur de données SOAP, vous devez indiquer les propriétés de configuration du serveur proxy.

Pour plus d'informations, voir «Configuration du serveur proxy», à la page 1342.

Configuration HTTP
Informations de référence sur la configuration HTTP.

Après l'ajout d'une source de données HTTP, la configuration apparaît sur la page **Configuration d'exécution** de l'éditeur d'agent. Des sections de configuration sont ajoutées pour la surveillance d'URL, pour l'authentification du serveur proxy et pour Java.

Configuration de surveillance des URL

La section de configuration de surveillance des URL contient les propriétés suivantes :

Tableau 274. Propriétés de configuration de surveillance des URL

Nom	Valeurs admises	Obligatoire	Description
Fichier d'URL HTTP	Chemin de fichier	Oui	Chemin d'accès au fichier contenant une liste des URL.
Page de collecte d'objets	Oui, Non La valeur par défaut est Oui.	Non	Indique s'il est nécessaire de télécharger les objets trouvés dans une page Web et de collecter des données à partir de ces derniers.

Configuration du serveur proxy

La section de configuration du serveur proxy contient les propriétés suivantes :

Tableau 275. Propriétés de configuration du serveur proxy

Nom	Valeurs admises	Obligatoire	Description
Nom d'hôte du proxy	Chaîne	Non	Nom d'hôte du proxy à utiliser pour les connexions HTTP.
Nom de l'utilisateur du proxy	Chaîne	Non	Nom d'utilisateur du serveur proxy.

Tableau 275. Propriétés de configuration du serveur proxy (suite)			
Nom	**Valeurs admises**	**Obligatoire**	**Description**
Port Proxy	Entier positif La valeur par défaut est 80.	Non	Numéro de port HTTP du serveur proxy.
Mot de passe du proxy	Mot de passe	Non	Mot de passe du serveur proxy.

Remarque : Si la propriété **Nom d'hôte du Proxy** n'est pas indiquée, aucun proxy n'est utilisé.

Configuration Java

Si vous définissez une source de données HTTP dans votre agent, celui-ci doit utiliser Java pour se connecter au serveur HTTP. Les propriétés de configuration Java s'ajoutent automatiquement à l'agent. Les propriétés de configuration Java suivantes sont propres à la configuration d'exécution de l'agent. Agent Builder n'a pas besoin des propriétés Java, dans la mesure où il utilise sa propre JVM et sa propre consignation qui sont configurées via le plug-in JLog :

Tableau 276. Propriétés de configuration Java			
Nom	**Valeurs admises**	**Obligatoire**	**Description**
Répertoire de base Java	Chemin complet d'accès à un répertoire	Non	Chemin complet pointant vers le répertoire d'installation Java.
Niveau de trace	Choix (La valeur par défaut est Erreur)	Oui	Cette propriété permet d'indiquer le niveau de trace utilisé par les fournisseurs Java.
Arguments JVM	Chaîne	Non	Utilisez cette propriété pour indiquer une liste facultative d'arguments pour la machine virtuelle Java.

Test des groupes d'attributs HTTP

Vous pouvez tester le groupe d'attributs HTTP que vous avez créé, dans Agent Builder.

Procédure

1. Démarrez la procédure de test de l'une des manières suivantes :
   - Lors de la création de l'agent, cliquez sur **Tester** à la page **Informations HTTP**.
   - Après la création de l'agent, sélectionnez un groupe d'attributs à la page **Définition de la source de données** de l'éditeur d'agent et cliquez sur **Tester**. Pour plus d'informations sur l'éditeur d'agent, voir «Utilisation de l'éditeur d'agent pour modifier l'agent», à la page 1207.

   Après avoir cliqué sur **Tester** dans l'une des deux étapes précédentes, la fenêtre **Test HTTP** s'affiche.
2. Cliquez sur **Parcourir** pour sélectionner le fichier d'URL HTTP. Pour plus d'informations sur les fichiers d'URL, voir «Fichier d'URL», à la page 1340.
3. Facultatif : Définissez les variables d'environnement, les propriétés de configuration, ainsi que des informations Java avant de démarrer le test.

   Pour plus d'informations, voir «Test des groupes d'attributs», à la page 1420. Pour plus d'informations sur la configuration HTTP, voir «Configuration HTTP», à la page 1342.

4. Cliquez sur l'option de **démarrage de l'agent**.

   Une fenêtre indique que l'agent est en cours de démarrage.
5. Pour simuler une demande de données d'agent provenant de Tivoli Enterprise Portal ou de SOAP, cliquez sur **Collecte de données**.

   L'agent surveille les URL définis dans le fichier d'URL HTTP. La fenêtre **Test HTTP** affiche les données qui sont renvoyées.
6. Facultatif : Cliquez sur **Vérifier les résultats** si les données renvoyées ne sont pas celles que vous attendez.

   La fenêtre **Statut de la collecte de données** affiche des informations supplémentaires sur les données. Les données collectées et affichées par la fenêtre Statut de la collecte de données sont décrites dans «Noeud de statut d'objet de performances», à la page 1466
7. Arrêtez l'agent en cliquant sur **Arrêter l'agent**.
8. Cliquez sur **OK** ou **Annuler** pour quitter la fenêtre **Test HTTP**. Cliquez sur **OK** pour sauvegarder les modifications que vous avez apportées.

Concepts associés

«Test de votre agent dans Agent Builder», à la page 1420
Après avoir utilisé Agent Builder pour créer un agent, vous pouvez tester l'agent dans Agent Builder.

Surveillance des données à partir d'une source de données SOAP ou d'une autre source de données HTTP

Vous pouvez définir une source de données pour qu'elle reçoive les données d'un serveur HTTP (par exemple via le protocole SOAP). La source de données envoie une demande HTTP à une URL et analyse la réponse (aux formats XML, HTML ou JSON) au niveau des attributs du jeu de données obtenu. Vous pouvez sélectionner les données extraites de la demande.

Pourquoi et quand exécuter cette tâche

A l'aide de la source de données SOAP, vous pouvez indiquer une URL HTTP et envoyer une demande GET, POST ou PUT. Pour les demandes POST ou PUT, vous pouvez spécifier les données POST associées. Une réponse XML, HTML ou JSON est extraite et analysée ; les données sont exposées à l'environnement de surveillance dans des attributs. Vous pouvez définir les attributs de toutes les valeurs dans un élément donné. Sinon, vous pouvez définir des valeurs XPath personnalisées pour indiquer la manière de remplir les attributs individuellement. Vous pouvez également combiner les deux mécanismes.

Pour collecter et analyser des réponses XML, HTML ou JSON à partir d'une URL, procédez comme suit :

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, cliquez sur **Données d'un serveur** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **SOAP**.
3. Cliquez sur **Suivant**.
4. Sur la page **Informations SOAP**, entrez une URL.

   La valeur par défaut est :

   ```
   http://${KQZ_HTTP_SERVER_NAME}:${KQZ_HTTP_PORT_NUMBER}
   ```

   Remarque : Vous pouvez utiliser une ou plusieurs variables de configuration permettant une résolution en URL. Cliquez sur **Insérer une propriété de configuration** pour sélectionner une propriété à insérer. Pour plus d'informations, voir «Personnalisation de la configuration de l'agent», à la page 1404.
5. Sélectionnez un type de demande. Le type de demande par défaut est Get. Pour les demandes Post et Put, entrez les données à traiter.

Remarque : Pour les demandes Post et Put, l'option **Insérer une propriété de configuration** est activée. Cliquez sur **Insérer une propriété de configuration** pour inclure une variable de configuration dans les données à traiter. Pour plus d'informations, voir «Personnalisation de la configuration de l'agent», à la page 1404.

6. Cliquez sur **Parcourir**.

   Remarque : Si, après avoir entré une URL et sélectionné un type de demande, vous ne souhaitez pas utiliser le navigateur SOAP pour générer la définition, entrez une **expression XPath de sélection de ligne**. Vous entrez l'**expression XPath de sélection de ligne** dans la fenêtre **Informations SOAP**. Ensuite, définissez tous les attributs du groupe d'attributs.

7. Dans la fenêtre de **navigateur SOAP**, procédez comme suit :

   a) Entrez une URL et sélectionnez un type de demande, si ce n'est pas déjà fait.

   b) Cliquez sur **Configuration** pour définir les propriétés de configuration référencées dans l'URL ou dans d'autres zones.

   c) Cliquez sur **Connecter** pour obtenir des données du fournisseur SOAP.

      Lorsque vous vous connectez à l'URL, la liste des éléments XML de l'URL s'affiche dans une arborescence DOM (Document Object Model). Une réponse HTML ou JSON est convertie au format XML et s'affiche sous forme d'une arborescence DOM. Pour plus de détails sur la conversion d'une réponse JSON en XML, voir «Représentation XML de données JSON», à la page 1347. Dans l'exemple de WebSphere Application Server de la (Figure 44, à la page 1345), l'URL suivante a été entrée :

      ```
      http://nc053011.tivlab.raleigh.ibm.com:9080/wasPerfTool/servlet
      /perfservlet?module= \threadPoolModule
      ```

      L'élément XML `PerformanceMonitor` est indiqué. Il s'agit de l'élément XML de niveau supérieur du document XML renvoyé par le fournisseur SOAP.

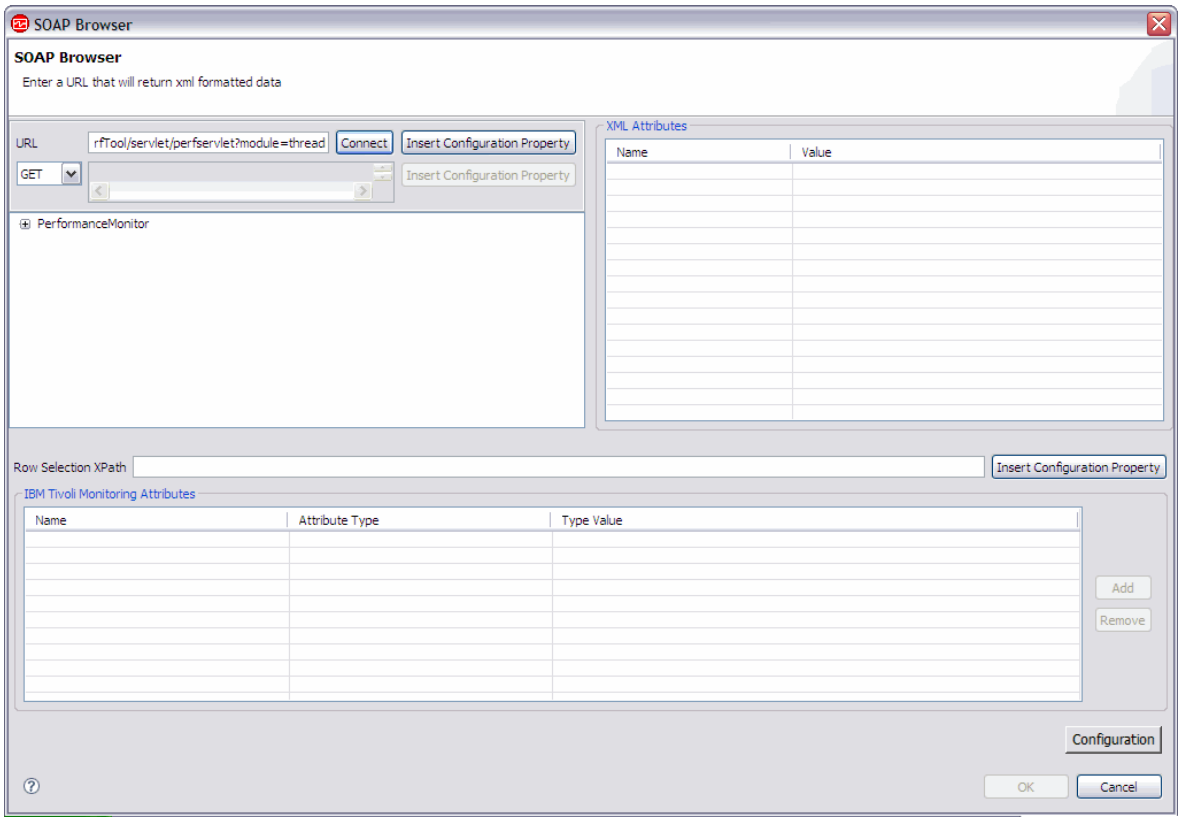


*Figure 44. Fenêtre **Navigateur SOAP***

   d) Dans l'arborescence DOM, recherchez et sélectionnez le noeud XML à définir comme **Expression XPath de sélection de ligne**.

Dans l'exemple de WebSphere Application Server de la (Figure 45, à la page 1346), le noeud `PerformanceMonitor/Node/Server/Stat/Stat/Stat` est sélectionné. Ce noeud représente une ligne de données dans le groupe d'attributs. Lorsque vous sélectionnez un noeud dans l'arborescence DOM et cliquez sur **Ajouter**, vous disposez de tous les attributs et éléments définis sur ce noeud de l'arborescence. (Vous cliquez sur **Ajouter** dans la zone **Attributs d'agent**).

Lorsqu'un noeud est sélectionné, la zone d'**attributs XML** affiche tous les attributs XML définis pour le noeud. Sélectionnez un attribut XML et cliquez sur **Ajouter** pour inclure cet attribut dans la liste des attributs d'agent.

Remarque : Si plusieurs lignes de données sont attendues, l'expression XPath doit être mappée à un ensemble de noeuds. Lorsque l'expression XPath de sélection de ligne renvoie un ensemble de noeuds comportant un seul élément, le groupe d'attributs contient une seule ligne.

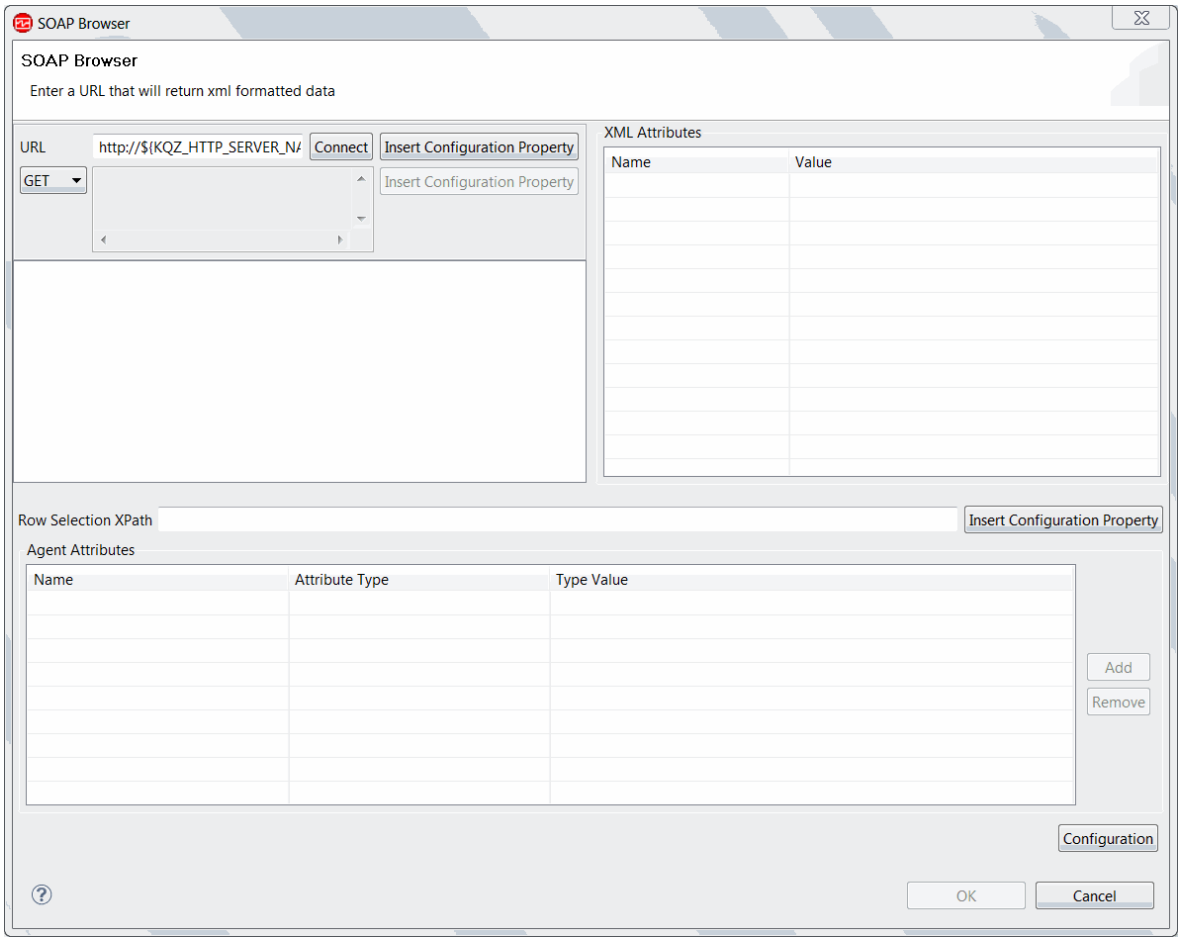


*Figure 45. Fenêtre **Navigateur SOAP***

e) Cliquez sur **Ajouter** dans la zone Attributs d'agent.

La liste des attributs d'agent apparaît et la zone **Expression XPath de sélection de lignes** est renseignée.

L'expression XPath de chaque attribut d'agent permet de mapper des noeuds ou des éléments XML aux attributs d'agent. Dans l'exemple de WebSphere Application Server de la Figure 46, à la page 1347, le premier attribut de la liste des attributs d'agent, `Stat`, n'est pas utilisé et doit être supprimé.

Vous pouvez modifier le nom et l'expression XPath d'un attribut d'agent dans la zone **Valeur du type**. Pour plus d'informations sur l'utilisation d'expressions XPath, voir «Options XPath», à la page 1350

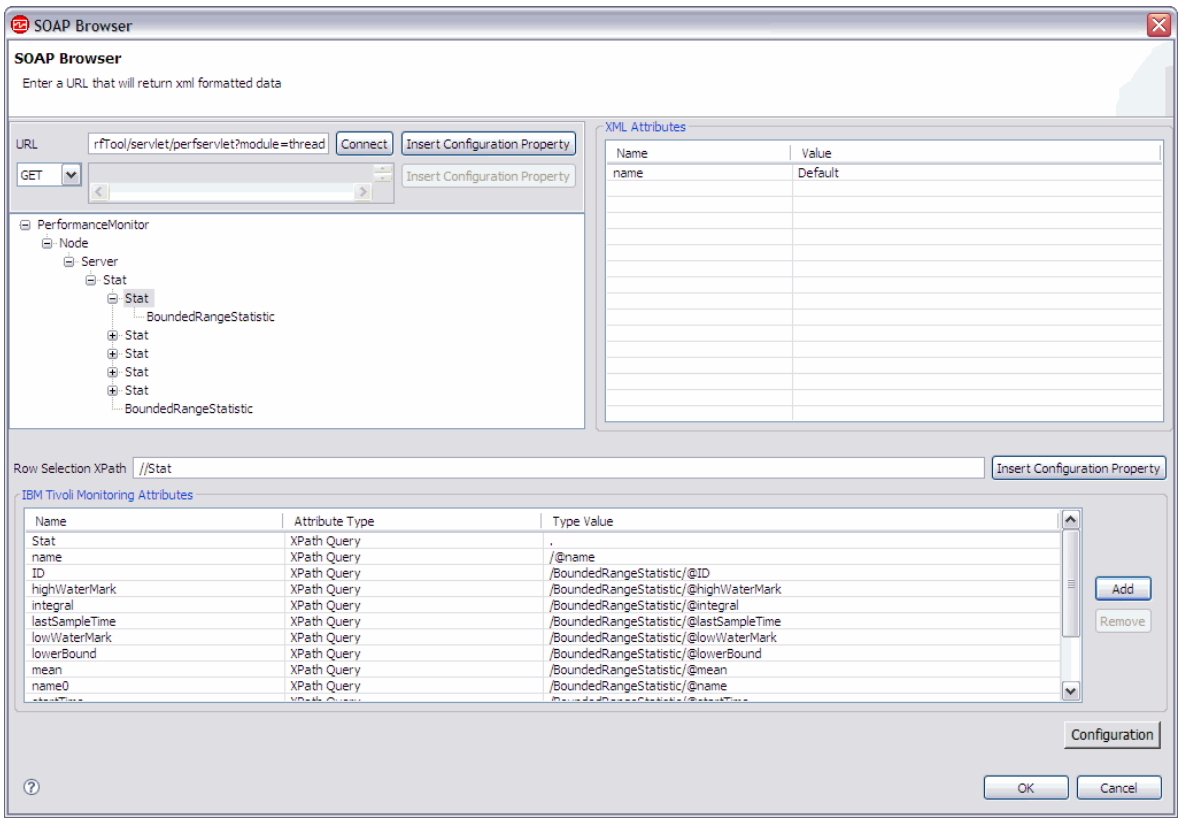


*Figure 46. Fenêtre **Navigateur SOAP***

f) Dans la fenêtre **Navigateur SOAP**, cliquez sur **OK** pour sauvegarder vos modifications et revenir à la fenêtre d'**Informations SOAP**.

8. Dans la fenêtre d'**Informations SOAP**, cliquez sur **Suivant**.
9. Si vous n'avez pas utilisé la fonction **Parcourir** et que vous avez entré l'**URL** et l'**expression XPath de sélection de ligne** dans la fenêtre d'**Informations SOAP**, la page **Informations d'attribut** s'affiche. Indiquez le premier attribut sur cette page et cliquez sur **Terminer**. Vous pouvez indiquer ensuite des attributs supplémentaires à l'aide de l'éditeur d'agent. Pour plus d'informations sur la création d'attributs, voir («Création d'attributs», à la page 1229).
10. Si vous avez utilisé la fonction **Parcourir** à l'étape «6», à la page 1345, la page **Sélectionner les attributs clés** s'affiche. Sur la page **Sélectionner les attributs clés**, sélectionnez les attributs de clé ou indiquez que la source de données génère uniquement une ligne de données. Pour plus d'informations, voir «Sélection des attributs de clé», à la page 1206.
11. Facultatif : Vous pouvez tester ce groupe d'attributs en cliquant sur **Tester**. Pour plus d'informations sur le test, voir «Test des groupes d'attributs SOAP», à la page 1351.
12. Facultatif : Vous pouvez créer un filtre pour limiter les données renvoyées par ce groupe d'attributs en cliquant sur **Avancé**. Pour plus d'informations sur le filtrage de données à partir d'un groupe d'attributs, voir «Filtrage des groupes d'attributs», à la page 1237.
13. Effectuez l'une des opérations suivantes :
    a) Si vous utilisez l'assistant **d'agent**, cliquez sur **Suivant**.
    b) Cliquez sur **Terminer** pour sauvegarder la source de données et ouvrir l'éditeur d'agent.

Représentation XML de données JSON

Si la requête HTTP renvoie des données JSON, le fournisseur de données les convertit en XML.

Le fournisseur de données convertit le nom d'un attribut JSON en nom de l'élément. Pour un attribut JSON d'un type simple, il convertir la valeur en données texte au sein de l'élément. Les objets JSON imbriqués sont convertis en éléments XML imbriqués. Tous les attributs subordonnés sont convertis en éléments subordonnés.

L'élément XML racine est `document_JSON`.

Si un nom d'attribut JSON contient des caractères non valides dans un nom d'élément, le fournisseur de données le modifie pour créer un nom d'élément valide. Le fournisseur de données ajoute également un attribut `nom_JSON` à l'élément. La valeur de l'attribut est le nom d'attribut JSON original.

Pour chaque élément d'un tableau JSON, le fournisseur de données créé un élément XML `élémént_tableau_`*`xxx`*`_JSON`, où *xxx* est le nom du tableau. La valeur de l'élément de tableau est convertie en texte au sein de l'élément XML. Un attribut `index_JSON` est ajouté à chaque élément XML ; la valeur de l'attribut est l'index de l'élément de tableau au sein du tableau.

Le fournisseur de données ajoute les attributs suivants à chaque élément :

- `niveau_JSON` : niveau du noeud au sein du fichier JSON. La racine de l'arborescence, représentée par la balise `document_JSON`, est au niveau 1.
- `type_JSON` : type de noeud JSON (objet, tableau, chaîne ou nombre).

Zones spécifiques des attributs SOAP
Dans la fenêtre **Informations d'attribut**, deux zones pour les attributs SOAP permettent de définir le mode de collecte des données à partir de la réponse SOAP.

La zone **Type d'attribut** peut comprendre toute valeur d'une liste qui contrôle les informations sur la réponse renvoyée. Certains types d'attribut nécessitent une valeur dans la zone **Valeur du type**. Le type d'attribut par défaut correspond à une requête XPath exécutée sur le contenu de la réponse du serveur SOAP. La valeur de type est la requête XPath exécutée. La table suivante décrit tous les types d'attribut et la valeur du type lorsqu'elle doit être précisée :

Tableau 277. Informations d'attributs SOAP

Type d'attribut	Description	Valeur du type	Type de données renvoyées	Différences avec les protocoles FTP et de fichier
`Requête XPath`	Permet d'exécuter une requête XPath sur le contenu renvoyé depuis une connexion d'URL. La requête doit être écrite pour renvoyer des données utiles à un attribut, et non une liste de noeuds.	Requête XPath à exécuter sur le contenu obtenu d'une connexion à l'URL. Si une requête de sélection de ligne a été définie, la requête XPath doit être relative à la requête.	Les données renvoyées peuvent être une chaîne, une valeur numérique ou une valeur d'horodatage. Le navigateur Agent Builder pour SOAP détecte généralement le type de données approprié de l'attribut dans les données explorées. Si les données ont le format XML DateTime, vous pouvez spécifier horodatage comme type d'attribut et l'agent convertit la valeur en horodatage Candle.	Aucun

Tableau 277. Informations d'attributs SOAP (suite)

Type d'attribut	Description	Valeur du type	Type de données renvoyées	Différences avec les protocoles FTP et de fichier
`Temps de réponse`	Quantité de temps en millisecondes pris par le téléchargement du contenu depuis l'URL demandée.	Aucun	Entier (nombre de millisecondes)	Aucun
`Message de réponse`	Message de réponse HTTP renvoyé par le serveur.	Aucun	Chaîne	Le message de réponse s'applique uniquement si l'URL utilise les protocoles HTTP ou HTTPS.
`Code de réponse`	Code de réponse HTTP renvoyé par serveur.	Aucun	Entier	Le code de réponse s'applique uniquement si l'URL utilise les protocoles HTTP ou HTTPS. Il est toujours de 0 pour les URL de fichier ou de protocole FTP.
`Longueur de la réponse`	Taille du contenu en octets qui a été téléchargé depuis l'URL demandée	Aucun	Entier (taille en octets)	Aucun
`En-tête de réponse`	L'en-tête de réponse permet d'extraire une valeur depuis l'une des zones d'en-tête de réponse d'URL. L'argument indique quelle est la zone demandée.	Zone d'en-tête de réponse à collecter.	Chaîne	Généralement, les protocoles FTP et de fichier ne comportent pas d'en-têtes à collecter.

Tableau 277. Informations d'attributs SOAP (suite)				
Type d'attribut	**Description**	**Valeur du type**	**Type de données renvoyées**	**Différences avec les protocoles FTP et de fichier**
URL de demande	Connexion qui a été établie à cette URL. Tous les mots clés de réponse fournissent des informations sur la connexion à cette URL. La requête XPath permet d'obtenir des informations provenant du contenu renvoyé par l'accès à cette URL.	Aucun	Chaîne	Aucun

Options XPath

Le langage XML Path vous permet de sélectionner des noeuds à partir d'un document XML. Voici quelques utilisations possibles d'expressions XPaths pour les sources de données SOAP :

- Utilisation de prédicats dans le langage XPath pour identifier les éléments XML qui correspondent à des lignes de données dans le groupe d'attributs IBM Tivoli Monitoring. Vous pouvez utiliser des prédicats dans l'expression XPath qui mappe des éléments ou des attributs XML sur des attributs Tivoli Monitoring, comme dans l'exemple suivant :

  ```
  Stat[@name="URLs"]/CountStatistic[@name="URIRequestCount"]/@count
  ```

  Lorsque l'expression XPath comprend plusieurs tranches d'emplacement, chacune d'entre elles peut contenir plusieurs prédicats. Les prédicats peuvent être complexes et contenir des valeurs booléennes ou des opérateurs de formule. Par exemple :

  ```
  //PerformanceMonitor/Node/Server[@name="server1"]/Stat/Stat/Stat[@name="Servlets"]/Stat
  ```

- Inclusion de fonctions d'ensembles de noeuds dans XPath, si une ligne contient plusieurs éléments XML de même type et si la position d'un élément XML de la liste de noeuds détermine l'attribut Tivoli Monitoring auquel l'élément est mappé. Exemples de fonctions de groupe de noeuds : `position()`, `first()`, `last()` et `count()`.
- Simple transformation de données, comme une sous-chaîne. Si vous indiquez la sous-chaîne suivante :

  ```
  substring(myXMLElement,1,3)
  ```

  Le langage XPath renvoie les trois premiers caractères de l'élément XML, myXMLElement.

Vous pouvez indiquer des éléments hors contexte de l'expression de sélection de ligne XPath à l'aide de deux points (`..`, comme dans l'exemple suivant :

```
/../OrganizationDescription/OrganizationIdentifier
```

Configuration SOAP

Une fois qu'une source de données SOAP est ajoutée, la configuration apparaît sur la page **Configuration d'exécution** de l'éditeur d'agent.

Des sections de configuration sont ajoutées pour serveur HTTP, pour serveur proxy et pour Java. Pour plus d'informations sur la configuration du serveur proxy, voir («Configuration du serveur proxy», à la page 1342). Pour plus d'informations sur la configuration Java, voir «Configuration Java», à la page 1343.

HTTP Server

La section de configuration du serveur HTTP Server contient les propriétés suivantes :

Tableau 278. Propriétés de configuration HTTP Server

Nom	Valeurs admises	Obligatoire	Description
Nom d'utilisateur HTTP	Chaîne	Non	Utilisateur HTTP
Mot de passe HTTP	Mot de passe	Non	Mot de passe du serveur HTTP
Nom du serveur HTTP	Chaîne (La valeur par défaut est localhost)	Non	Hôte ou adresse IP du serveur HTTP
numéro de port HTTP	Numérique (La valeur par défaut est 80)	Non	Hôte ou adresse IP du serveur HTTP
Validation de certificat activée	True, False (La valeur par défaut est True)	Oui	La désactivation de la validation de certificat présente des risques
Fichier de clés de confiance HTTP	Chemin de fichier	Non	Fichier de clés de confiance HTTP
Mot de passe du magasin de clés de confiance HTTP	Mot de passe du magasin de clés de confiance HTTP	Non	Mot de passe du magasin de clés de confiance HTTP

Serveur proxy

Si le système où l'agent s'exécute nécessite un proxy pour accéder au fournisseur de données SOAP, vous devez indiquer les propriétés de configuration du serveur proxy. Pour plus d'informations, voir «Configuration du serveur proxy», à la page 1342.

Test des groupes d'attributs SOAP

Vous pouvez tester le groupe d'attributs SOAP que vous avez créé, dans Agent Builder.

Procédure

1. Vous pouvez démarrer la procédure de test de l'une des manières suivantes :
   - Lors de la création de l'agent, cliquez sur **Tester** à la page **Informations SOAP**.
   - Après la création de l'agent, sélectionnez un groupe d'attributs à la page **Définition de la source de données** de l'éditeur d'agent et cliquez sur **Tester**. Pour plus d'informations sur l'éditeur d'agent, voir «Utilisation de l'éditeur d'agent pour modifier l'agent», à la page 1207.

   Après avoir cliqué sur **Tester** dans l'une des deux étapes précédentes, la fenêtre **Test de la collecte SOAP** s'affiche.

2. Facultatif : Avant de démarrer le test, vous pouvez définir les variables d'environnement, les propriétés de configuration, ainsi que des informations Java.

   Pour plus d'informations, voir «Test des groupes d'attributs», à la page 1420. Pour plus d'informations sur la configuration SOAP, voir «Configuration SOAP», à la page 1351.
3. Modifiez l'URL, l'expression XPath de sélection de ligne et le type de demande.
4. Cliquez sur l'option de **démarrage de l'agent**.

   Une fenêtre indique que l'agent est en cours de démarrage.
5. Pour simuler une demande de données d'agent provenant de Tivoli Enterprise Portal ou de SOAP, cliquez sur **Collecte de données**. Cette action renseigne la table des résultats et vous permet de prévisualiser la façon dont les données sont analysées et affichées dans les colonnes de Tivoli Enterprise Portal.

   Dans la zone des résultats, vous pouvez modifier les définitions d'attribut, puis recharger les données pour identifier l'impact des modifications sur les données qui seront stockées dans le groupe d'attributs. Vous pouvez cliquer avec le bouton droit de la souris dans une zone de résultats de colonne pour afficher les options permettant de modifier l'attribut. Les options de modification d'attribut sont les suivantes :

   - **Modifier l'attribut**
   - **Masquer l'attribut**
   - **Insérer un attribut avant**
   - **Insérer un attribut après**
   - **Supprimer**
   - **Supprimer les attributs suivants**
   - **Supprimer tout**
6. Facultatif : Cliquez sur **Vérifier les résultats** si les données renvoyées ne sont pas celles que vous attendez.

   La fenêtre **Statut de la collecte de données** affiche des informations supplémentaires sur les données. Les données collectées et affichées dans la fenêtre **Statut de la collecte de données** sont décrites dans «Noeud de statut d'objet de performances», à la page 1466.
7. Arrêtez l'agent en cliquant sur **Arrêter l'agent**.
8. Cliquez sur **OK** ou **Annuler** pour quitter la fenêtre **Test de la collecte SOAP**. Cliquez sur **OK** pour sauvegarder les modifications que vous avez apportées.

Concepts associés

«Test de votre agent dans Agent Builder», à la page 1420
Après avoir utilisé Agent Builder pour créer un agent, vous pouvez tester l'agent dans Agent Builder.

Surveillance de données à l'aide d'un socket

Vous pouvez définir une source de données pour qu'elle collecte les données d'une application externe à l'aide d'un socket TCP. L'application doit établir la connexion TCP à l'agent et envoyer les données au format XML structuré. Selon l'application, la source de données peut produire un ensemble de données comprenant une ligne, plusieurs lignes ou des données d'événement.

Pourquoi et quand exécuter cette tâche

Utilisez la source de données du socket pour fournir des données à l'agent à partir d'une application externe qui s'exécute sur le même système que l'agent. L'application externe peut envoyer des données à l'agent à tout moment. Par exemple, vous pouvez développer une interface de ligne de commande qui permet à un utilisateur de publier des données dans un groupe d'attributs lors de son exécution. L'autre option consiste à modifier une application surveillée de manière à envoyer des mises à jour à l'agent. L'agent ne démarre pas ou n'arrête pas l'application qui envoie des données au socket ; cette opération est contrôlée par l'utilisateur.

Il existe certaines limitations avec la source de données du socket :

- Par défaut, vous ne pouvez établir des connexions qu'à l'hôte local (127.0.0.1). Pour plus d'informations sur la façon de configurer votre agent pour accepter les connexions à partir d'un hôte distant, voir «Connexion de port de socket distant», à la page 1361.
- L'interface de programme d'application du socket n'intègre aucun mécanisme permettant au client de déterminer quels sous-noeuds sont disponibles. Le client peut envoyer des données pour un sous-noeud spécifique, mais il doit déjà connaître le nom du sous-noeud.

Pour créer un groupe d'attributs afin de collecter des données à l'aide d'un socket TCP (Transmission Control Protocol), procédez comme suit.

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, cliquez sur **Programmes personnalisés** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **Socket**.
3. Cliquez sur **Suivant**.
4. Dans la page **Informations relatives au socket**, entrez un nom de groupe d'attributs.
5. Entrez un texte d'aide pour le groupe d'attributs.
6. Indiquez si le groupe d'attributs **Génère une ligne de données unique**, **Peut générer plusieurs lignes de données** ou **Génère des événements**. Pour plus d'informations, voir «Envoi de données», à la page 1355.
7. Dans la section Informations relatives au socket, sélectionnez une **page de codes**. Pour plus d'informations, voir «Jeux de caractères», à la page 1358.
8. Facultatif : Cliquez sur **Avancé** pour modifier les propriétés avancées du groupe d'attributs. L'option **Avancé** est active lorsque vous indiquez que le groupe d'attributs **Peut générer plusieurs lignes de données** ou **Génère des événements**.
9. Cliquez sur **Suivant**.
10. Sur la page **Informations d'attribut**, indiquez le premier attribut du groupe d'attributs. Pour plus d'informations sur la création d'attributs, voir «Création d'attributs», à la page 1229.
11. Cliquez sur **Suivant**.
12. Facultatif : Sur la page **Informations globales relatives à la source de données du socket**, dans la section des **codes d'erreur**, vous pouvez définir les codes d'erreur que le client du socket peut envoyer lorsqu'il n'arrive pas à collecter des données. Pour plus d'informations, voir «Envoi d'erreurs au lieu de données», à la page 1356. Pour définir un code d'erreur, procédez comme suit :
    a) Dans la section des **codes d'erreur**, cliquez sur **Ajouter**. Un code d'erreur est limité à 256 caractères. Seuls les lettres, les chiffres et les traits de soulignement ASCII sont admis. Les espaces ne sont pas autorisés.
    b) Dans la fenêtre **Définition du code d'erreur du socket**, entrez la valeur qui s'affichera dans le groupe d'attributs **Statut de l'objet de performances**.
    c) Entrez une valeur interne. La valeur interne doit être un entier compris entre 1 000 et 2 147 483 647.
    d) Vous devez définir un texte de message pour chaque erreur. Vous pouvez utiliser un texte précédemment entré en le sélectionnant dans la liste. Cliquez sur **OK** pour revenir à la page **Informations globales relatives à la source de données du socket**. Le texte du message est utilisé dans le fichier journal de l'agent.

    Si aucun texte de message approprié n'est disponible, cliquez sur **Parcourir** pour définir le texte du message. La fenêtre (liste) Messages s'ouvre. La zone de messages montre les messages définis dans l'agent. La liste reste vide jusqu'à ce que vous définissiez des messages. Vous pouvez utiliser **Modifier** pour modifier un message défini et **Supprimer** pour supprimer un ou plusieurs messages que vous avez définis.
    e) Dans la fenêtre (liste) Messages, cliquez sur **Ajouter** pour afficher une fenêtre **Définition de message**. Dans la fenêtre **Définition de message**, tapez le texte indiquant la signification du nouveau message et sélectionner le type du message.

Remarque : L'identificateur de message est automatiquement généré pour vous.

f) Cliquez sur **OK**.

g) La fenêtre (liste) Messages s'affiche avec le nouveau message. Pour vérifier le message et revenir à la page **Informations globales relatives à la source de données du socket**, cliquez sur **OK**.

13. Facultatif : Dans la section **Fichiers supplémentaires** de la page **Informations globales relatives à la source de données du socket**, vous pouvez ajouter des fichiers qui sont intégrés à l'agent. Ces fichiers sont copiés dans le système d'agent une fois l'agent installé.

    La colonne **Type de fichier** décrit comment chaque fichier doit être utilisé. Trois utilisations possibles sont décrites dans le tableau suivant :

Tableau 279. Types des fichiers supplémentaires	
Type de fichier	**Description**
Exécutable	Sélectionnez cette option pour inclure un fichier exécutable à l'agent. L'agent n'utilise pas ces fichiers.
Bibliothèque	Sélectionnez cette option si vous voulez inclure une bibliothèque à l'agent. L'agent n'utilise pas ces fichiers.
Ressource Java	Sélectionnez cette option pour inclure des ressources Java à l'agent. L'agent n'utilise pas ces fichiers.

    Pour plus d'informations sur l'emplacement où sont installés les fichiers supplémentaires avec l'agent, voir («Nouveaux fichiers sur votre système», à la page 1438).

    Cliquez sur **Modifier** pour modifier le fichier importé. Pour plus d'informations, voir «Modification d'une définition de fichier de commandes», à la page 1319.

14. Facultatif : Vous pouvez tester ce groupe d'attributs en cliquant sur **Tester**. Pour plus d'informations sur le test, voir «Test des groupes d'attributs de socket», à la page 1362.

15. Facultatif : Si la source de données est échantillonnée, vous pouvez créer un filtre pour limiter les données renvoyées par ce groupe d'attributs en cliquant sur **Avancé**. La source de données est échantillonnée si vous n'avez pas sélectionné "Génère des événements" dans la page **Informations relatives au socket**. Pour plus d'informations sur le filtrage de données à partir d'un groupe d'attributs, voir «Filtrage des groupes d'attributs», à la page 1237.

16. Effectuez l'une des opérations suivantes :

    a) Si vous utilisez l'assistant d'**agent**, cliquez sur **Suivant**.

    b) Cliquez sur **Terminer** pour sauvegarder la source de données et ouvrir l'éditeur d'agent.

    Sélectionnez les systèmes d'exploitation sur lesquels l'agent est en écoute des données provenant des clients du socket dans la section **Systèmes d'exploitation** de la page **Paramètres du fournisseur du socket**. Pour ouvrir cette page, cliquez sur **Paramètres du fournisseur du socket** dans la vue Structure ou sur **Paramètres globaux** dans l'éditeur d'agent de n'importe quelle page de groupe d'attributs du socket.

    Remarque : Les codes d'erreurs et les fichiers supplémentaires peuvent être mis à jour dans les sections **Codes d'erreur** et **Fichiers supplémentaires** de la page **Paramètres du fournisseur du socket**.

Envoi d'informations de socket à l'agent

Lorsque l'agent contient un ou plusieurs groupes d'attributs du socket, il ouvre un socket et se met à l'écoute des données provenant des clients.

L'application qui envoie des données socket à l'agent se connecte à un port défini dans l'agent. Ce port correspond à la valeur définie par une propriété de configuration d'agent ou est un port éphémère alloué

automatiquement par TCP/IP. Pour plus d'informations sur les ports et la configuration de socket, voir «Configuration du socket», à la page 1360.

Les données reçues doivent être au format XML. Les flux d'informations XML suivants sont possibles en utilisant la source de données du socket :

- Envoi d'une ou plusieurs lignes de données à l'agent pour un groupe d'attributs échantillonnés
- Envoi d'une ligne de données à l'agent pour un groupe d'attributs qui génère des événements
- Envoi d'un code d'erreur à l'agent à la place de données
- Envoi d'un enregistrement de préfixe de tâche à l'agent
- Réception d'une requête de tâche provenant de l'agent
- Envoi d'une réponse de tâche à l'agent

Envoi de données

Un groupe d'attributs est défini pour recevoir des données échantillonnées ou des données d'événements. Lors de la création du groupe d'attributs, vous spécifiez une option qui indique si les données à recevoir :

- génèrent une ligne de données unique ;
- génèrent plusieurs lignes de données ;
- génèrent des événements.

Si vous sélectionnez **Génère une ligne de données unique** ou **Peut générer plusieurs lignes de données**, il s'agit d'un groupe d'attributs échantillonnés. Si vous sélectionnez **Génère des événements**, votre groupe d'attributs envoie un événement à l'environnement de surveillance à chaque réception d'une ligne.

Lorsque vous affichez des données échantillonnées dans Tivoli Enterprise Portal ou dans la console IBM Cloud Application Performance Management, vous visualisez la dernière série de lignes collectées. Les données affichées pour un groupe d'attributs d'événement correspondent au contenu d'un cache local qui est géré par l'agent. Pour les données d'événements, l'agent ajoute la nouvelle entrée dans le cache, jusqu'à ce que la taille maximale du cache soit atteinte et que l'entrée la plus ancienne soit supprimée. Pour les données échantillonnées, l'agent remplace le contenu du cache chaque fois que vous envoyez des données.

Si vous sélectionnez **Génère des événements** ou **Génère une ligne de données unique**, vous ne devez envoyer à l'agent qu'une seule ligne de données pour ce groupe d'attributs dans chaque message. Vous pouvez envoyer autant d'événements que vous le souhaitez, en envoyant chaque événement dans un message distinct.

En général, les données échantillonnées sont collectées par l'agent sur requête, mais le client du socket fournit des données échantillonnées mises à jour selon sa propre planification. Vous pouvez mettre à jour un groupe d'attributs échantillonné (une seule ligne ou plusieurs) aussi souvent que vous le souhaitez. Lorsque les données sont demandées par Tivoli Monitoring ou IBM Cloud Application Performance Management, l'agent fournit les données les plus récentes.

S'il manque des lignes de données pour le groupe d'attributs de socket dans Tivoli Enterprise Portal ou dans la console IBM Cloud Application Performance Management, vérifiez les erreurs dans le fichier journal. De plus, si les données du groupe d'attributs ne sont pas celles escomptées, vérifiez les erreurs dans le fichier journal. Le source de données du socket tente de traiter tout élément possible reçu en entrée. Par exemple, si le client envoie trois lignes correctes et une non valide (par exemple, format XML syntaxiquement incorrect), les informations suivantes s'affichent :

- Trois lignes de données dans le groupe d'attributs
- Une erreur est consignée dans le fichier journal de l'agent pour la ligne syntaxiquement incorrecte
- Des lignes correctes ayant été renvoyées, le statut de l'objet de performances affiche `NO_ERROR`

Les données d'événements comme les données échantillonnées sont envoyées à l'agent sous forme de flux de données XML unique à partir du client du socket. Les données envoyées à partir d'un client du

socket doivent toujours se terminer par un caractère de retour à la ligne : '\n'. L'agent lit les données jusqu'au caractère de retour à la ligne, puis tente de traiter les éléments reçus. Toutes les données reçues impossibles à traiter sont supprimées. Voici un exemple qui montre comment envoyer deux lignes de donnés à l'agent pour un groupe d'attributs nommé abc :

```
<socketData><attrGroup name="abc"><in><a v="1"/><a v="no"/><a v="5"/></in><in> \
<a v="3"/><a v="yes"/><a v="5"/></in></attrGroup></socketData>\n
```

Cet exemple envoie à l'agent deux lignes de données qui contiennent chacune trois attributs. L'ordre des attributs est important et doit respecter celui qui est défini dans le groupe d'attributs. La seule exception à cette règle est que les attributs dérivés doivent être ignorés, quel que soit l'endroit où ils apparaissent dans le groupe d'attributs.

Si le groupe d'attributs est défini dans un sous-noeud, l'ID d'instance du sous-noeud doit être identifié lorsque les données sont envoyées à l'agent. L'ID instance de sous-noeud est identifié à l'aide de l'attribut de sous-noeud dans l'élément socketData. Vous devez adopter une convention de configuration des ID d'instance de sous-noeud que le client du socket utilisera puisque ce dernier n'a pas accès aux propriétés de configuration ou d'ID d'instance. Les données envoyées à un sous-noeud non configuré sont ignorées.

Exemple :

```
<socketData subnode="app1"><attrGroup name="abc"><in><a v="1"/><a v="no"/><a v="5"/>
</in><in> \<a v="3"/><a v="yes"/><a v="5"/></in></attrGroup></socketData>\n
```

Dans cet exemple, les données sont envoyées au sous-noeud dont l'ID d'instance ID est "app1". "app1" n'est pas le nom du système géré, mais l'identificateur d'instance spécifié lors de la configuration de l'instance de sous-noeud.

Les données du socket sont constituées des éléments XML suivants :

socketData
Elément racine. Il comporte un attribut facultatif nommé sous-noeud qui indique l'ID d'instance de sous-noeud.

attrGroup
Elément qui identifie le groupe d'attributs auquel sont destinées les données du socket. L'attribut name est obligatoire ; il permet d'indiquer le nom du groupe d'attributs.

in
Elément obligatoire pour identifier une nouvelle ligne de données. Toutes les valeurs d'attribut d'une ligne de données doivent être des enfants du même élément in.

a
L'élément a identifie une valeur d'attribut. L'attribut v est obligatoire ; il permet de spécifier la valeur d'attribut.

Envoi d'erreurs au lieu de données

Parfois, l'application qui envoie des données de socket n'est pas à même de collecter les données nécessaires pour un groupe d'attributs. Dans ce cas, au lieu d'envoyer des données à l'agent, elle renvoie un code d'erreur. Ce code d'erreur fournit des informations sur le problème à l'environnement de surveillance. Exemple d'erreur :

```
<socketData><attrGroup name="abc"/><error rc="1000"/></attrGroup></socketData>\n
```

Le code d'erreur doit être défini dans l'agent dans une liste commune à tous les groupes d'attributs du socket. Lorsque l'agent reçoit un code d'erreur, le message d'erreur défini est consigné dans le fichier journal de l'agent. En outre, le groupe d'attributs Statut d'objet de performances contient un attribut Code d'erreur mis à jour avec le type de code d'erreur. Le type de code d'erreur est défini pour le code d'erreur que vous envoyez.

Pour l'exemple ci-dessus, vous devez définir la valeur de code d'erreur 1000 dans l'agent. Exemple de définition de code d'erreur :

Tableau 280. Exemple de code d'erreur		
Valeur du code d'erreur	**Type du code d'erreur**	**Message**
1000	APP_NOT_RUNNING	L'application ne s'exécute pas

Lorsque le code d'erreur est envoyé, un message semblable au suivant est consigné dans le fichier journal de l'agent :

```
(4D7FA153.0000-5:customproviderserver.cpp,1799,"processRC") Code d’erreur 1000 reçu du client.
\Message : K1C0001E L'application ne s'exécute pas
```

Si vous sélectionnez la requête Statut de l'objet de performances à partir de Tivoli Enterprise Portal, la colonne **Code d'erreur** pour la ligne **abc** du groupe d'attributs affiche la valeur APP_NOT_RUNNING dans cette table.

L'envoi d'un code d'erreur à un groupe d'attributs échantillonnés efface toutes les données précédemment reçues pour ce groupe d'attributs. L'envoi de données au groupe d'attributs supprime l'affichage du code d'erreur dans le groupe d'attributs Statut d'objet de performances. Vous pouvez également envoyer un code d'erreur 0 pour effacer le code d'erreur de la table.

L'envoi d'une erreur à un groupe d'attributs qui génère des événements n'efface pas le cache des événements précédemment envoyé.

Traitement des demandes Action

Le client de socket peut s'inscrire pour recevoir des demande `Action` de l'agent lorsque la commande Action correspond à un certain préfixe. Toute action sans correspondance avec ce préfixe est gérée par l'agent. Le préfixe ne devant générer aucun conflit avec des actions prévues pour être gérées par l'agent, utilisez le code produit de l'agent comme préfixe. Les `actions` fournies avec l'Agent Builder sont nommées d'après la source de données que l'`action` utilise. Par exemple, l'`action JMX_INVOKE` intervient sur la source de données JMX. SSHEXEC est un autre exemple d'action qui utilise le fournisseur de données de script SSH. Ces actions n'utilisant pas le code produit, vous pouvez en toute sécurité l'utiliser comme préfixe `action`.

Le client de socket doit s'exécuter sur une longue durée et laisser le socket ouvert. Il doit envoyer une demande d'enregistrement pour le préfixe et écouter les demandes du socket. L'agent s'assure qu'aucune expiration de délai ne se produit dans le socket d'un client à exécution longue, même si aucune donnée ne transite. Voici un exemple de requête d'enregistrement :

```
<taskPrefix value="K42"/>\n
```

Dans cet exemple, la commande `Action` reçue par l'agent qui commence par `"K42"` est envoyée au client du socket qui a lancé l'enregistrement. Voici un exemple de demande d'`action` pouvant être reçue par le client du socket :

```
<taskRequest id="1"><task command="K42 refresh" user="sysadmin"/></taskRequest>\n
```

L'`id` est un identificateur unique utilisé par l'agent pour le suivi des demandes envoyées aux clients. Lorsque le client de socket répond à la tâche, il doit fournir cet identificateur dans l'attribut `id` de l'élément `taskResponse`.

Le client de socket doit traiter l'action et envoyer une réponse. Exemple de réponse :

```
 <taskResponse id="1" rc="1"/>\n
```

Si l'action se termine avec succès, un attribut `rc` avec la valeur `0` est renvoyé. La valeur `rc` doit être un entier, où toute valeur différente de 0 indique un échec. La valeur du code retour de la tâche est consignée dans le fichier journal de l'agent et s'affiche dans la requête Statut d'action incluse à l'agent. La boîte de dialogue qui s'ouvre dans Tivoli Enterprise Portal après l'exécution d'une action n'affiche pas le code retour. La boîte de dialogue indique si la commande `Action` a retourné un succès ou un échec. Vous

devez afficher le journal de l'agent ou la requête Statut d'action pour connaître le code retour précis en cas d'échec.

Il est de la responsabilité du développeur d'agent de documenter, créer et importer toutes les actions prises en charge par les clients de socket utilisés par un agent. Le client de socket doit être développé de manière à pouvoir gérer de manière appropriée les scénarios dans lesquels des utilisateurs lui envoient des actions non prises en charge. Si les utilisateurs définissent des actions supplémentaires commençant par le préfixe enregistré, ils sont transmis au client. Le client doit être développé de manière à gérer ces scénarios de manière appropriée.

Un délai d'attente, qui contrôle la durée pendant laquelle l'agent attend une réponse du client de socket, est défini. Il s'agit d'une variable d'environnement définie dans l'agent, nommée `CDP_DP_ACTION_TIMEOUT`, dont la valeur par défaut est 20 secondes.

Remarque : Les messages de code d'erreur définis pour les groupes d'attributs de la source de données du socket ne sont pas utilisés pour les commandes `Action`. Vous pouvez retourner les mêmes valeurs de code de retour. Cependant, l'agent ne consigne pas le message défini et ne modifie pas la zone `Code d'erreur` du groupe d'attributs Statut de l'objet de performances.

Codage des données du socket

Le client du socket code les données envoyées à l'agent.

Il est essentiel de bien comprendre comment le client du socket code les données envoyées à l'agent.

Caractères spéciaux

Les données envoyées à l'agent ne doivent contenir aucun caractère de retour à la ligne sauf à la fin de chaque événement ou donnée échantillonnée. Les caractères de retour à la ligne présents dans des valeurs d'attribut doivent être remplacés par un autre caractère ou codés selon le (Tableau 281, à la page 1358) ci-dessous. Vous devez également veiller à ne pas rompre la syntaxe XML avec les valeurs d'attribut. Le tableau répertorie les caractères qui doivent être codés s'ils font partie des valeurs d'attribut :

Tableau 281. Caractères à coder dans des valeurs d'attributs

Caractère	**En-tête**
&	`&`
<	`<`
>	`>`
“	`"`
'	`'`
\n	`
`

Remarque : L'agent utilise le caractère de retour à la ligne pour séparer les réponses reçues d'un client. Tout caractère de retour à la ligne inattendu nuit à la bonne analyse des données.

L'agent n'étant pas doté d'un analyseur syntaxique XML complet, n'utilisez pas de codage spécial pour les caractères qui ne se trouvent pas dans le (Tableau 281, à la page 1358). Par exemple, ne codez pas avec `¢` ou `&cent` le signe centime ¢.

Jeux de caractères

Outre le codage des caractères spéciaux, l'agent doit savoir quelle page de codes a été utilisée pour coder vos données. Définissez chaque groupe d'attributs du socket pour indiquer si vous envoyez les données à l'agent comme données **UTF-8** ou **page de codes locale**. Soyez conscient de la manière dont votre client envoie les données. Si vous utilisez un client écrit en Java, indiquez **UTF-8** comme codage dans le programme d'écriture utilisé pour envoyer les données à l'agent. Définissez **UTF-8** comme **page de codes** du groupe d'attributs. **Page de codes locale** correspond à la page de codes locale de l'agent. Si les

données sont envoyées sur un socket distant, elles doivent se conformer à la page de codes locale de l'agent ou utiliser UTF-8.

Données numériques

Soyez conscient de la manière dont vous formatez vos valeurs d'attributs numériques. Les valeurs numériques envoyées à l'agent ne doivent contenir aucun caractère spécial. Le séparateur de milliers est un exemple. Entre autres exemples, citons les symboles de devises ou les caractères qui décrivent l'unité d'une valeur. Lorsque l'agent ne parvient pas à analyser des données numériques, il consigne une erreur indiquant l'anomalie. Le code d'erreur du statut de l'objet de performances n'est pas défini lorsque l'analyse d'un attribut échoue. Voici un exemple de message d'erreur consigné dans le journal de l'agent :

```
(4D3F1FD6.0021-9:utilities.cpp,205,"parseNumericString") Caractères incorrects :00:04 \
détectés lors de l'extraction de valeur numérique à partir de 00:00:04, avec retour de 0.000000
```

Remarque : Pour en savoir plus sur le mode de formatage d'un attribut d'horodatage, voir («Horodatage», à la page 1234).

Erreurs de socket

Des erreurs sont consignées dans le fichier journal de l'agent pour les incidents liés à la réception de données provenant d'un client du socket.

Les autres erreurs consignées concernent les commandes `Actions` qui renvoient une autre valeur que `0`. Les valeurs d'erreur que le client du socket envoie sont consignées avec le message associé au code d'erreur.

Le statut de l'objet de performances du groupe d'attributs est défini lorsque le client du socket envoie un code de retour d'erreur à l'agent. Outre les valeurs définies par l'agent, certaines autres valeurs peuvent s'afficher. Le tableau suivant présente les autres valeurs de “code d'erreur” possibles avec les groupes d'attributs de socket :

Tableau 282. Valeurs du statut de l'objet de performances

Code d'erreur	Description
NO_ERROR	Aucune erreur. Indique qu'aucune erreur n'est associée au groupe d'attributs. Incidents liés à une ligne de données échantillonnées ne provoquant pas le remplacement de l'état NO_ERROR. Vous devez valider le nombre de lignes affichées et les valeurs d'attribut, même si le code d'erreur renvoyé est NO_ERROR.
NO_INSTANCES_RETURNED	Un client de socket n'a envoyé aucune ligne de données pour un groupe d'attributs échantillonnés. Aucune erreur. Indique qu'il n'existe aucune instance des ressources que surveille ce groupe d'attributs.
XML_PARSE_ERROR	L'agent n'a pas réussi à analyser les données reçues du client. Consultez le journal de l'agent pour plus de détails.
OBJECT_CURRENTLY_UNAVAILABLE	Le client a envoyé à l'agent un code d'erreur non défini dans la liste des codes d'erreur.

Tableau 282. Valeurs du statut de l'objet de performances (suite)	
Code d'erreur	**Description**
GENERAL_ERROR	Un incident s'est produit lors de la collecte de données à partir du client, généralement parce que le client n'a pas répondu à la requête dans le délai imparti. Consultez le journal de trace de l'agent pour plus de détails. Le client peut également spécifier GENERAL_ERROR comme code d'erreur, mais il est préférable de définir un code d'erreur plus détaillé.

Configuration du socket
Après avoir ajouté une source de données de socket à votre agent, configurez votre agent pour qu'il accepte des données à partir d'un port de socket.

Pourquoi et quand exécuter cette tâche

Une fois qu'une source de données est ajoutée, la configuration apparaît dans la page **Configuration d'exécution** de l'éditeur d'agent. La section Configuration du socket contient la propriété suivante :

Tableau 283. Propriété de configuration du socket			
Nom	**Valeurs admises**	**Obligatoire**	**Description**
Numéro de port	0 ou tout entier positif La valeur par défaut est 0	Oui	Port sur lequel l'agent écoute les données provenant des clients du socket. La valeur 0 indique qu'un port éphémère doit être utilisé.

L'agent écrit la valeur du port utilisé dans un fichier. Les clients du socket qui s'exécutent sur l'ordinateur agent peuvent ensuite lire ce fichier pour savoir à quel port se connecter. Le fichier dans lequel la valeur du port est enregistrée s'appelle *kxx_instanceName*_cps.properties, où : *kxx* est le code produit de trois caractères de l'agent et *instanceName* le nom d'instance d'un agent multi-instance. S'il ne s'agit pas d'un agent multi-instance, cette partie du nom est omise et le nom du fichier est simplement *kxx*_cp.properties.

Sous Windows, le fichier est enregistré dans le répertoire %CANDLE_HOME%\TMAITM6 pour les installations 32 bits et dans %CANDLE_HOME%\TMAITM6_x64 pour les installations 64 bits. Sous UNIX, le fichier est enregistré dans le répertoire /tmp.

Procédure

1. Facultatif : Définissez la variable d'environnement CDP_DP_HOSTNAME sur le nom d'hôte ou l'adresse IP de votre interface réseau, si votre système possède plusieurs interfaces :
   a) Accédez à la vue **Informations sur l'agent** de l'éditeur d'agent, puis sélectionnez **Variables d'environnement**.
   b) Cliquez sur **Ajouter** et sélectionnez CDP_DP_HOSTNAME dans la liste des variables d'environnement à l'aide de la zone Nom.
   c) Définissez le nom d'hôte ou l'adresse IP dans la zone Valeur.
2. Démarrez l'agent.

Lorsque l'agent est démarré, il se connecte à l'interface définie par la variable d'environnement CDP_DP_HOSTNAME. Si CDP_DP_HOSTNAME n'a pas été définie, l'agent se connecte au nom d'hôte par défaut.

Si vous souhaitez que l'agent se connecte à un port défini à la place d'un port temporaire, vous pouvez définir la propriété de configuration **Numéro de port** (CP_PORT).

Pour définir la propriété de configuration du numéro de port, procédez comme suit :

a) Affichez la vue **Configuration d'exécution** de l'éditeur d'agent.

b) Dans le panneau **Informations sur la configuration d'exécution**, sélectionnez **Configuration du socket** > **Socket** > **Numéro de port**.

c) Entrez un numéro de port dans **Valeur par défaut**.

Si vous ne spécifiez pas de valeur, la valeur 0 est utilisée. La valeur 0 indique qu'un port temporaire est utilisé.

Connexion de port de socket distant

Vous pouvez configurer votre agent pour qu'il accepte les données à partir d'un port de socket distant. L'agent doit s'exécuter sur un système qui dispose d'une connexion d'interface réseau à un système distant.

Procédure

1. Réglez la variable d'environnement CDP_DP_ALLOW_REMOTE sur YES en effectuant les étapes suivantes.
   a) Accédez à la page **Informations sur l'agent** de l'éditeur d'agent, puis sélectionnez **Variables d'environnement**.
   b) Cliquez sur **Ajouter** et sélectionnez CDP_DP_ALLOW_REMOTE dans la liste des variables d'environnement à l'aide de la zone **Nom**.
   c) Définissez la zone **Valeur** sur YES.
2. Suivez la procédure décrite dans «Configuration du socket», à la page 1360.

   Restriction :

   - Les données envoyées entre l'application socket et l'agent :
     - Doivent être conformes à la syntaxe XML définie pour un fournisseur de données de socket. Pour plus d'informations, voir « Codage des données du socket», à la page 1358.
     - Doivent être encodées au format UTF-8.
     - Sont en texte clair (non chiffrées). Si les données contiennent des informations sensibles, la communication doit être sécurisée via un tunnel SSH ou un autre mécanisme extérieur à l'agent.
   - L'agent traite les données reçues de tout hôte distant afin que l'environnement soit sécurisé avec le pare-feu ou les filtres de trafic réseau appropriés.

Résultats

Vous pouvez exécuter le code qui implémente un fournisseur de données de socket sur un système pouvant se connecter au système sur lequel l'agent est en cours d'exécution.

Exemple de script pour socket

Ces exemples de scripts montrent comment un client de socket peut être écrit.

Exemple Perl

L'exemple de script Perl suivant permet d'établir une connexion à un socket et d'envoyer des données. Cet exemple a été écrit pour un agent qui s'exécute sous UNIX avec le code produit `k00` et un groupe d'attributs nommé `SocketData`.

```
#!/usr/bin/perl -w
# SocketTest.pl
# Client de socket Agent Builder simple qui utilise IO:Socket
#------------------------

use strict;
use IO::Socket;

# Initialisation de la connexion de socket à l'agent
#-----------------------
my $host = '127.0.0.1';
my $port = 0;
# Cet exemple est valable pour un agent ayant le code produit k00.  Le code produit
# est utilisé dans la ligne suivante pour rechercher le fichier contenant le numéro de port à
utiliser.
open PORTFILE, "/tmp/k00_cps.properties" || die "Port file not found $!\n";
while (<PORTFILE>) {
    if (/^CP_PORT=([0-9]+)/) {
        $port = $1;
    }
}

if ($port == 0) {
    die "Could not find port to use to connect to agent.\n";
}

my $sock = new IO::Socket::INET( PeerAddr => $host, PeerPort => $port,
Proto => 'tcp'); $sock or die "no socket :$!";

# L'appel suivant envoie 2 lignes de données à l'agent.  Chaque ligne contient 1
# attribut de chaîne et 3 attributs numériques.
syswrite $sock, "<socketData><attrGroup name=\"SocketData\"><in><a v=\"A message
from perl\"/>  \<a v=\"1\"/><a v=\"2\"/><a v=\"123\"/></in><in><a v=\"More from
perl\"/><a v=\"456\"/>  \<a v=\"123\"/><a v=\"789\"/></in></attrGroup>
</socketData>\n";

close $sock;
```

Test des groupes d'attributs de socket

Vous pouvez tester le groupe d'attributs de socket que vous avez créé, dans Agent Builder.

Avant de commencer

Pour tester le groupe d'attributs, vous devez disposer d'un client de socket pour envoyer des données. Un client de socket exemple écrit avec un script perl est visible dans «Exemple de script pour socket», à la page 1362.

Restriction : Contrairement à la plupart des autres groupes d'attributs, vous ne pouvez pas tester le groupe d'attributs du socket lorsqu'il est en cours de création. Vous pouvez tester le groupe d'attributs lorsque vous avez terminé sa création.

Procédure

1. Après la création de l'agent, sélectionnez un groupe d'attributs sur la page **Définition de la source de données** de l'éditeur d'agent et cliquez sur **Tester**. Pour plus d'informations sur l'éditeur d'agent, voir «Utilisation de l'éditeur d'agent pour modifier l'agent», à la page 1207.

   Après avoir cliqué sur **Tester** dans l'une des deux étapes précédentes, la fenêtre de **test du client socket** s'affiche.
2. Facultatif : Avant de démarrer le test, définissez des variables d'environnement et des propriétés de configuration.

Pour plus d'informations, voir «Test des groupes d'attributs», à la page 1420.

3. Cliquez sur l'option de **démarrage de l'agent**. Une fenêtre indique que l'agent est en cours de démarrage.
4. Lorsque l'agent démarre, il écoute les données du socket en fonction de sa configuration.
5. Pour tester la collecte de données de l'agent, vous pouvez désormais générer des données de socket correspondant à la configuration des agents.

   Vous pouvez générer des données de socket à l'aide d'un client de socket.

   Lorsque l'agent reçoit les données de socket correspondant à sa configuration, il les ajoute à son cache interne.
6. Pour simuler une demande de données d'agent provenant de Tivoli Enterprise Portal, cliquez sur **Collecte de données**.

   La fenêtre **Tester le client du socket** collecte et affiche les données figurant dans la mémoire cache de l'agent depuis son dernier démarrage.
7. Cliquez sur **Vérifier les résultats** si vous constatez que quelque chose ne fonctionne pas correctement.

   La fenêtre **Statut de la collecte de données** affiche des informations supplémentaires sur les données. Les données collectées et affichées par la fenêtre Statut de la collecte de données sont décrites dans «Noeud de statut d'objet de performances», à la page 1466
8. Arrêtez l'agent en cliquant sur **Arrêter l'agent**.
9. Cliquez sur **OK** ou **Annuler** pour quitter la fenêtre **Tester le client socket**. Cliquez sur **OK** pour sauvegarder les modifications que vous avez apportées.

Concepts associés

«Test de votre agent dans Agent Builder», à la page 1420
Après avoir utilisé Agent Builder pour créer un agent, vous pouvez tester l'agent dans Agent Builder.

Utilisation de l'API Java pour surveiller des données

Vous pouvez définir une source de données pour qu'elle utilise l'API Java en vue d'interagir avec une application à exécution longue sur la plateforme Java. L'agent lance l'application au moment du démarrage et interagit régulièrement avec elle. Lorsque vous générez l'agent, Agent Builder crée le code source pour l'application. Vous devez personnaliser le code pour regrouper les données correctes. Selon le code, la source de données peut produire plusieurs jeux de données contenant une ligne, plusieurs lignes ou des données d'événement.

Pourquoi et quand exécuter cette tâche

Utilisez la source de données de l'API Java et le langage de programmation Java pour collecter des données qui ne peuvent pas l'être avec d'autres sources de données d'Agent Builder. L'agent démarre l'application Java et envoie une requête d'arrêt au moment opportun. L'application Java ne doit se fermer qu'au moment demandé.

Un agent qui contient des groupes d'attributs d'interface de programme d'application Java sert d'interface avec le processus d'application Java. L'application Java utilise l'interface de programme d'application du client du fournisseur Java comme interface avec l'agent. Pour plus d'informations sur l'interface de programme d'application, voir le Javadoc sur le Knowledge Center de Tivoli Monitoring. L'API Java vous permet d'effectuer les actions suivantes :

- Connexion au processus d'agent et enregistrement des groupes d'attributs pris en charge par l'application Java
- Réception et réponse à une requête de données échantillonnées
- Envoi de données de manière asynchrone pour un groupe d'attributs qui génère des événements
- Envoi d'une erreur pour un groupe d'attributs dont une collection de données est défaillante
- Prise en charge des groupes d'attributs dans des sous-noeuds avec des instances de sous-noeuds configurées

- Réception et réponse à une requête "Action"

Pour créer un groupe d'attributs qui collecte des données dans une application Java et les envoie à l'aide de l'API Java, suivez la procédure ci-dessous. Celle-ci détaille la création d'un exemple d'application Java à utiliser comme point de départ de votre application Java.

Procédure

1. Sur la page **Source de données initiale de l'agent** ou **Emplacement de la source de données**, cliquez sur **Programmes personnalisés** dans la zone **Catégories de données de surveillance**.
2. Dans la zone **Sources de données**, cliquez sur **Interface de programme d'application Java**.
3. Cliquez sur **Suivant**.
4. Dans la page **Informations relatives à l'interface de programme d'application Java**, entrez un nom de groupe d'attributs.
5. Entrez un texte d'aide pour le groupe d'attributs.
6. Indiquez si le groupe d'attributs **Génère une ligne de données unique**, **Peut générer plusieurs lignes de données** ou **Génère des événements**. Ce choix affecte l'exemple d'application Java créé à la fin de l'exécution de l'assistant. Pour plus d'informations, voir «Envoi de données», à la page 1355.
7. Facultatif : Cliquez sur **Avancé** pour modifier les propriétés avancées du groupe d'attributs. L'option **Avancé** apparaît lorsque vous indiquez que le groupe d'attributs **Peut générer plusieurs lignes de données** ou **Génère des événements**.
8. Cliquez sur **Suivant**.
9. Sur la page **Informations d'attribut**, indiquez le premier attribut du groupe d'attributs. Pour plus d'informations sur la création d'attributs, voir («Création d'attributs», à la page 1229).
10. Sélectionnez **Ajouter des attributs supplémentaires** et cliquez sur **Suivant** pour ajouter d'autres attributs à l'agent. Les références aux attributs sont incorporées dans l'exemple d'application Java qui est créé à la fin de l'exécution de l'assistant.
11. Cliquez sur **Suivant**.
12. Dans la page **Informations globales relatives à la source de données de l'interface de programme d'application Java**, entrez un nom de classe et un nom de fichier JAR.

    Le nom de classe est un nom de classe qualifié complet dont la méthode principale est appelée au démarrage de Java. L'exemple d'application Java est créé avec la méthode Java principale dans cette classe.

    Le fichier JAR est l'archive qui contient les classes Java comprenant l'application Java. Le fichier JAR est intégré à l'agent et installé avec lui.
13. Facultatif : Définissez les codes d'erreur que l'application Java peut envoyer, sur la page **Informations globales relatives à la source de données de l'API Java**, dans la section **Codes d'erreur**. Ces codes sont envoyés par l'application Java lorsqu'elle ne parvient pas à collecter des données.

    Restriction : Un code d'erreur est limité à 256 caractères. Seuls les lettres, les chiffres et les traits de soulignement ASCII sont admis. Les espaces ne sont pas autorisés.

    a) Cliquez sur **Ajouter** dans la section Codes d'erreur.

    b) Dans la fenêtre **Définition du code d'erreur d'interface de programme d'application Java**, entrez une valeur d'affichage.

    c) Entrez une valeur interne. La valeur interne doit être un entier compris entre 1 000 et 2 147 483 647.

    d) Définissez un texte de message pour chaque erreur. Vous pouvez utiliser un texte précédemment entré en le sélectionnant dans la liste. Cliquez sur **OK** pour revenir à la page **Informations globales relatives à la source de données de l'interface de programme d'application Java**.

    Le message est consigné dans le fichier journal de l'agent.

    e) Si aucun texte de message approprié n'est disponible, cliquez sur **Parcourir** pour définir le texte du message.

La fenêtre (liste) Messages s'affiche. La zone de messages montre les messages définis dans l'agent. La liste reste vide jusqu'à ce que vous définissiez des messages. Vous pouvez utiliser **Modifier** pour modifier un message défini et **Supprimer** pour supprimer un ou plusieurs messages que vous avez définis.

f) Dans la fenêtre (liste) Messages, cliquez sur **Ajouter** pour afficher une fenêtre **Définition de message**. Dans la fenêtre **Définition de message**, tapez le texte indiquant la signification du nouveau message et sélectionnez le type du message.

Remarque : L'identificateur de message est automatiquement généré pour vous.

g) Cliquez sur **OK**.

h) La fenêtre (liste) Messages s'affiche avec le nouveau message. Pour vérifier le message et revenir à la page **Informations globales relatives à la source de données de l'interface de programme d'application Java**, cliquez sur **OK**.

14. Facultatif : Dans la section **Fichiers supplémentaires** de la page **Informations globales relatives à la source de données de l'interface de programme d'application Java**, vous pouvez ajouter des fichiers qui sont intégrés à l'agent et copiés sur le système d'agent au moment de l'installation de l'agent. Le fichier JAR de l'API client du fournisseur Java n'est pas répertorié ici ; il est automatiquement copié sur le système d'agent. La colonne **Type de fichier** décrit comment chaque fichier doit être utilisé. Trois utilisations possibles sont décrites dans le tableau suivant (Tableau 284, à la page 1365). Cliquez sur **Modifier** pour modifier le fichier importé. Pour plus d'informations, voir «Modification d'une définition de fichier de commandes», à la page 1319.

Tableau 284. Types des fichiers supplémentaires

Type de fichier	**Description**
Exécutable	Sélectionnez cette option pour inclure un fichier exécutable à l'agent. L'agent n'utilise pas ce fichier, mais il est intégré au chemin d'accès pour être utilisé par l'application Java.
Bibliothèque	Sélectionnez cette option si vous voulez inclure une bibliothèque à l'agent. L'agent n'utilise pas ce fichier, mais il est intégré au chemin d'accès de bibliothèque pour être utilisé par l'application Java.
Ressource Java	Sélectionnez cette option pour inclure des ressources Java à l'agent. L'agent n'utilise pas ce fichier, mais il est intégré au chemin d'accès aux classes pour être utilisé par l'application Java.

Remarque : Lorsqu'un fichier supplémentaire de ressource Java est ajouté à Agent Builder, il est automatiquement inséré dans le chemin d'accès des classes du projet. Cet ajout permet au compilateur Java de résoudre toutes les références figurant dans le code pour les classes dans la ressource.

Pour plus d'informations sur l'emplacement où sont installés les fichiers supplémentaires avec l'agent, voir («Nouveaux fichiers sur votre système», à la page 1438).

15. Facultatif : Créez un filtre pour limiter les données renvoyées par ce groupe d'attributs, si les données sont échantillonnées. Créez un filtre en cliquant sur **Avancé**.

Remarque : Les données sont échantillonnées si vous n'avez pas sélectionné **Génère des événements** sur la page **Informations relatives à l'API Java**.

Pour plus d'informations sur le filtrage des données à partir d'un groupe d'attributs, voir «Filtrage des groupes d'attributs», à la page 1237.

16. Facultatif : Ajoutez des propriétés de configuration au sous-noeud.

Si vous ajoutez cette source de données à un sous-noeud, la page **Substitutions de configuration de sous-noeud** apparaît et vous permet d'ajouter des propriétés de configuration à ce sous-noeud. Au moins une propriété de configuration est nécessaire sous le sous-noeud pour l'exemple d'application Java à créer, Au moins une propriété de configuration est nécessaire, car l'exemple s'en sert pour distinguer les instances de sous-noeud les unes des autres.

17. Effectuez l'une des opérations suivantes :
    a) Si vous utilisez l'assistant d'**agent**, cliquez sur **Suivant**. Exécutez l'assistant si nécessaire.
    b) Sinon, cliquez sur **Terminer** pour sauvegarder la source de données et ouvrir l'éditeur d'agent. Puis, dans le menu principal, sélectionnez **Fichier** > **Sauvegarder**.

    A ce point, Agent Builder crée le code source pour l'application de surveillance. Le code se trouve dans le sous-répertoire `src` du répertoire de projet. Editez ce code pour créer votre application de surveillance.

Que faire ensuite

Sélectionnez les systèmes d'exploitation appropriés dans la page **Paramètres d'API Java**. Sélectionnez cette option si ce groupe d'attributs et l'application Java doivent s'exécuter sur des systèmes d'exploitation différents de ceux définis pour l'agent. Pour ouvrir la page, cliquez sur **Paramètres d'API Java** dans la vue Structure ou sur **Paramètres globaux** dans l'éditeur d'Agent de n'importe quelle page de groupe d'attributs de l'interface de programme d'application Java.

Remarque : Les codes d'erreur et les fichiers supplémentaires peuvent être mis à jour ultérieurement dans les sections **Codes d'erreur** et **Fichiers supplémentaires** de la page **Paramètres d'API Java**.

Exécution de l'application Java
Informations sur l'initialisation de l'application Java et ses dépendances

Initialisation de l'application Java

L'agent démarre l'application Java pendant son démarrage et son initialisation. Des paramètres de configuration permettent de contrôler l'environnement d'exécution Java qui est utilisé pour lancer le processus. Des arguments de machine virtuelle Java et le niveau de consignation Java peuvent également être spécifiés dans la configuration. Pour plus d'informations sur la configuration de l'API Java, voir «Configuration de l'API Java», à la page 1376. Le processus Java hérite de toutes les variables d'environnement définies pour l'agent. Des paramètres de configuration d'exécution, également placés dans l'environnement, peuvent être interrogés via des appels API.

L'application Java doit être un processus qui s'exécute sur une longue durée. Elle ne doit pas s'arrêter à moins de recevoir une demande d'arrêt de l'API. Si l'application Java s'arrête après enregistrement auprès de l'agent, ce dernier tente de redémarrer l'application Java trois fois. Si la collecte des données reprend sans problème, ce compteur de redémarrage est réinitialisé. L'agent consigne une erreur lorsqu'une application Java s'arrête et qu'un redémarrage est initié.

Remarque : Si l'application Java s'arrête avant la fin de l'enregistrement du groupe d'attributs, aucune tentative de redémarrage n'est effectuée.

Dépendances

Une application Java doit utiliser un environnement d'exécution Java. Les versions de Java suivantes sont prises en charge :

- Oracle Corporation Java version 5 ou ultérieure
- IBM Corporation Java version 5 ou ultérieure

Java doit déjà être installé sur le système d'agent lorsque l'agent est configuré et démarré. Le fichier JAR qui contient l'API utilisée pour communiquer avec l'agent est inclus avec l'agent d'`exécution` et inclus dans le `chemin d'accès aux classes` de la JVM. Tous les fichiers JAR supplémentaires nécessaires à l'application Java doivent être définis en tant que fichiers supplémentaires des groupes d'attributs de l'API Java. Tous les fichiers supplémentaires dont le *Type de fichier* est *Ressource Java* sont ajoutés

automatiquement au `chemin d'accès aux classes` de base de l'application Java, avec le fichier JAR de l'API Java.

Tous les fichiers JAR qui sont nécessaires au fonctionnement de l'application Java, mais qui ne sont pas inclus dans l'agent, doivent être inclus dans le paramètre de configuration *Chemin d'accès aux classes pour les fichiers JAR externes*.

Application Java générée à titre d'échantillon
Informations de référence décrivant le code généré par Agent Builder et le code que vous devez ajouter ou remplacer pour les ressources à surveiller.

Lorsque vous créez un agent avec une ou plusieurs sources de données d'interface de programme d'application Java, Agent Builder génère le code source de l'application Java. Ce code est généré dans le projet de l'agent et suit la structure de ce dernier. Vous devez ajouter votre propre code Java à l'application générée. Il collecte des données pour des groupes d'attributs échantillonnés, gère les événements à envoyer à des groupes d'attributs basés sur des événements, signale les incidents détectés, et exécute les tâches. L'application générée fournit des données à l'agent mais il s'agit d'échantillons à remplacer par les données issues des ressources à surveiller.

Un exemple d'agent est supposé avoir les caractéristiques suivantes :

- Code produit : K91
- Classe principale d'interface de programme d'application Java : `agent.client.MainClass`
- Structure de la source de données de l'agent illustrée à la (Figure 47, à la page 1367) :

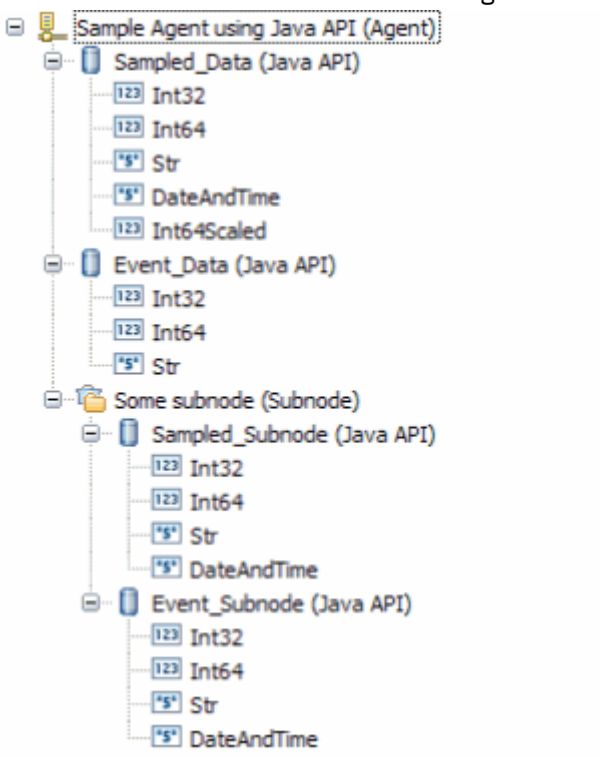


Figure 47. Structure de l'exemple d'agent

- Propriété de configuration de *certains sous-noeuds* : `K91_INSTANCE_KEY`

Structure des classes

L'application Java générée sépare, dans une proportion importante, le code qui sert d'interface avec l'agent du code d'interface avec les ressources surveillées. Il contient des fichiers que vous modifiez et d'autres que vous ne modifiez pas.

Les classes Java suivantes sont créées par Agent Builder :

`MainClass` (package `agent.client`)
Classe indiquée sur la page **Informations globales relatives à la source de données de l'API Java**. Elle contient une méthode principale et une méthode pour la gestion des requêtes de *commande Action*. Cette classe hérite de la classe auxiliaire décrite ci-après. Vous devez modifier cette classe pour l'interface avec les ressources à surveiller et les actions à exécuter.

`MainClassBase` (package `agent.client`)
Classe auxiliaire qui initialise la connexion au serveur, enregistre les groupes d'attributs et attend les requêtes provenant du serveur. Ne modifiez pas cette classe.

Classes `Sampled_Data`, `Sampled_Subnode`, `Event_Data` et `Event_Subnode` (package `agent.client.attributeGroups`)
Il existe une classe pour chaque groupe d'attributs de l'API Java qui gère des requêtes de collecte de données ou qui génère des événements pour le groupe d'attributs. Ces classes héritent chacune de l'une des classes auxiliaires décrites ci-après. Vous devez modifier ces classes pour regrouper les données issues des ressources à surveiller.

Classes `Sampled_DataBase`, `Sampled_SubnodeBase`, `Event_DataBase` et `Event_SubnodeBase` (package `agent.client.attributeGroups`)
Classes auxiliaires, une pour chaque groupe d'attributs de l'API Java, qui définissent la structure des attributs du groupe dans une classe interne. Ne modifiez pas ces classes.

Interface `ICustomAttributeGroup` (package `agent.client.attributeGroups`)
Interface qui définit les méthodes publiques de chaque classe de groupe d'attributs. Ne modifiez pas cette interface.

Agent Builder n'écrase jamais les classes que vous pouvez modifier. Il se contente de les créer si elles n'existent pas.

Les classes auxiliaires et l'interface sont écrasées à chaque sauvegarde d'Agent Builder. A mesure que vous modifiez et sauvegardez l'agent, les classes auxiliaires sont mises à jour afin de refléter tous les changements structurels apportés aux groupes d'attributs de l'API Java. L'interface et les classes auxiliaires contiennent un avertissement dans leur en-tête pour vous rappeler que vous devez modifier le fichier.

Initialisation et nettoyage

La méthode principale de la classe `MainClass` est appelée au démarrage de l'agent. Elle crée une instance `MainClass` puis lance la méthode à exécution longue pour recevoir et gérer les requêtes d'agent.

La majeure partie du code d'initialisation et de nettoyage doit être ajoutée à `MainClass`. Dans le constructeur, ajoutez le code d'initialisation requis pour créer vos ressources ou y accéder. Vous pouvez, si vous le souhaitez, ouvrir des connexions à des ressources distantes, créer des descripteurs ou initialiser des structures de données.

Avant l'arrêt de l'agent, la méthode `stopDataCollection` est appelée. Si vous devez fermer des connexions ou effectuer un nettoyage avant l'arrêt de l'application Java, ajoutez ce code à la méthode `stopDataCollection`.

Si une initialisation n'est requise que pour un groupe d'attributs particulier, vous pouvez ajouter cette initialisation au constructeur de la classe du groupe d'attributs. De même, si un nettoyage n'est requis que pour un groupe d'attributs particulier, vous pouvez ajouter ce code de nettoyage à la méthode `stopDataCollection` du groupe d'attributs.

Tout code de l'application Java peut utiliser l'objet consignateur pour inscrire des entrées de journal. (La classe auxiliaire principale crée un objet consignateur protégé dans son constructeur. Les objets auxiliaires de groupe d'attributs créent une référence protégée à ce consignateur dans leurs constructeurs). L'objet consignateur fait appel à l'utilitaire de consignation de trace de Java. Des informations détaillées relatives aux erreurs et aux traces sont accessibles dans le journal de trace que crée le consignateur. Ces informations sont essentielles pour l'identification des incidents avec le fournisseur.

Lors de l'appel de `stopDataCollection`, si vous transmettez la tâche de nettoyage à une autre unité d'exécution, attendez que cette unité d'exécution soit terminée avant le retour à la méthode `stopDataCollection`. Sinon, la tâche de nettoyage risque de s'arrêter brutalement lors de l'arrêt du processus suite à la fin de l'unité d'exécution.

L'un des paramètres de configuration d'agent est réservé au niveau de trace Java. Le tableau suivant indique les valeurs que vous pouvez définir dans la propriété de configuration JAVA_TRACE_LEVEL. Si l'API a créé le consignateur à votre intention, le tableau affiche le niveau qu'utilise ce consignateur.

Tableau 285. Options de niveau de trace Java

Niveau de trace configuré	Niveau de trace de consignation Java	Description
Arrêt	HORS FONCTION	Pas de consignation.
Erreur	GRAVE	Suivi des problèmes survenus dans l'application Java.
Avertissement	WARNING	Suivi des erreurs et des erreurs potentielles.
Informations	INFORMATION	Suivi des informations importantes concernant l'application Java.
Débogage minimum	FIN	Suivi des détails de niveau supérieur nécessaires à l'analyse du comportement de l'application Java.
Débogage moyen	PLUS FIN	Suivi des détails relatifs au flux du programme de l'application Java.
Débogage maximum	TRES FIN	Suivi de tous les détails concernant l'application Java.
Tous	TOUS	Suivi de tous les messages.

Dans cet exemple, l'application Java crée le fichier journal nommé `k91_trace0.log`. Si l'agent est multi-instance, le nom d'instance doit être inclus dans le nom du fichier journal.

Remarque : Ne pas écrire de messages vers une erreur ou une sortie standard. Sur les systèmes Windows, ces messages sont perdus. Sur les systèmes UNIX et Linux, ces données sont écrites dans un fichier sans boucle.

Collecte de données échantillonnées de groupe d'attributs

La classe d'un groupe d'attributs échantillonnés (qui collecte une ou plusieurs lignes de données) contient une méthode `collectData`, par exemple `Sampled_Data.collectData`. Cette méthode est appelée chaque fois que l'agent demande des données.

La classe auxiliaire du groupe d'attributs définit une classe interne nommée Attributs. Cette classe comporte une zone pour chaque attribut qui est défini dans votre groupe d'attributs. Les attributs dérivés ne sont pas inclus car ils sont calculés par l'agent. Les types de données des zones d'attribut sont des équivalents Java des types d'attributs Tivoli Monitoring, comme indiqué dans le (Tableau 286, à la page 1370).

Tableau 286. Types de données des zones d'attributs et leurs types d'attribut IBM Tivoli Monitoring équivalents

Type Tivoli Monitoring	**Type de données de la zone d'attribut**
Chaîne	Chaîne
Numérique, 32 bits, sans ajustement décimal	entier
Numérique, 64 bits, sans ajustement décimal	long
Numérique, ajustement décimal différent de zéro	double
Horodatage	Planification calendaire

La méthode `collectData` doit :

1. Collecter les données appropriées à partir de la ressource surveillée.
2. Créer un objet Attributs.
3. Ajouter les données aux zones de l'objet Attributs.
4. Appeler la méthode `Attributes.setAttributeValues` pour copier les données dans une mémoire tampon interne.
5. Répéter les étapes 1 à 4 pour chaque ligne de données. (Vous pouvez sauter les étapes 1 à 4 et ne renvoyer aucune ligne. Dans ce cas, la colonne Code d'erreur de la table Statut de l'objet de performances contient la valeur NO_INSTANCES_RETURNED. Pour plus d'informations sur les codes d'erreur, voir («Codes d'erreur», à la page 1373).
6. Appelez `AgentConnection.sendData` pour envoyer les données à l'agent ou appeler `sendError` pour supprimer les données copiées de tous les appels de `setAttributeValues` et envoyez à la place un code d'erreur.

Vous devez collecter les données à partir de votre ressource (étape 1), en remplaçant les données échantillonnées utilisées dans l'application générée.

Pour renseigner l'objet Attributs, vous pouvez transmettre les données à l'aide du constructeur d'attributs (comme dans l'application générée). Vous pouvez également utiliser le constructeur à zéro argument pour créer un objet Attributs puis affecter les zones de l'objet aux valeurs d'attribut collectées. Les zones portent le même nom que les attributs, mais commencent par une lettre en minuscule.

Collecte de données échantillonnées pour un sous-noeud

Lorsqu'un groupe d'attributs échantillonnés se trouve dans un sous-noeud, il est probable que vous surveilliez plusieurs ressources (une pour chaque sous-noeud). Vous devez déterminer les ressources à partir desquelles les données doivent être collectées. Une ou plusieurs propriétés de configuration doivent identifier la ressource surveillée.

Cet exemple part du principe qu'une propriété de configuration, `K91_INSTANCE_KEY`, contient une valeur qui identifie la ressource à partir de laquelle collecter des données.

Pour trouver la ressource appropriée, procédez comme suit :

1. Extrayez l'ID instance de tous les sous-noeuds configurés en appelant `AgentConnection.getConfiguredSubnodeInstanceIDs`. A chaque sous-noeud configuré correspond un ID instance unique.
2. Extrayez la propriété de configuration `K91_INSTANCE_KEY` de chaque ID instance en appelant `AgentConnection.getSubnodeConfigurationProperty`.
3. Recherchez la ressource représentée par la valeur de `K91_INSTANCE_KEY`.

Cette procédure peut être effectuée dans la méthode `collectData` avant les procédures détaillées dans «Collecte de données échantillonnées de groupe d'attributs», à la page 1369.

Vous pouvez également exécuter cette procédure dans le constructeur de classe de groupe d'attributs et effectuer un mappage direct de l'ID instance sur la ressource. Le constructeur `Sampled_Subnode` est un

exemple de constructeur de classe de groupe d'attributs. Cette procédure vous donne également la possibilité de créer des descripteurs ou d'ouvrir des connexions qui peuvent être utilisés dans toute la durée de vie de l'agent. La création de descripteurs ou l'ouverture de connexions peut optimiser l'accès à vos ressources.

Le code généré crée des exemples d'objet ressource de type `MonitoredEntity` dans le constructeur et les ajoute dans une mappe `configurationLookup`. Vous devez supprimer la classe interne `MonitoredEntity` et remplacer les objets `MonitoredEntity` qui accèdent à vos propres ressources. Si vous choisissez d'effectuer intégralement la procédure de recherche dans la méthode `collectData`, vous pouvez supprimer la mappe `configurationLookup` de la classe.

Si vous choisissez de faire appel au constructeur, avec mappage de l'ID instance de sous-noeud à votre ressource, les étapes à suivre dans la méthode `collectData` sont les suivantes :

1. Extraction de l'ID instance du sous-noeud à partir du paramètre de demande, par appel de `Request.getSubnodeInstanceID`.
2. Extraction de l'objet ressource à partir de la mappe créée dans le constructeur.
3. Exécution de la procédure décrite dans «Collecte de données échantillonnées de groupe d'attributs», à la page 1369 pour envoyer des données à l'agent.

Une propriété de sous-noeud est choisie arbitrairement dans l'exemple d'Agent Builder, ici`K91_INSTANCE_KEY`. Si la propriété est incorrecte, ou si plusieurs propriétés sont nécessaires pour identifier la ressource adéquate, vous devez choisir les propriétés correctes pour identifier la ressource.

Envoi d'événements

Pour les groupes d'attributs qui génèrent des événements, la méthode `collectData` n'est pas appelée régulièrement. Votre application envoie des événements à mesure que la ressource les transmet.

Ainsi, le code généré pour un groupe d'attributs basé sur des événements crée et démarre une unité d'exécution qui s'exécute à partir d'une classe interne nommée `SampleEventClass`. Le groupe d'attributs basé sur des événements, utilisé dans l'exemple, est la classe `Event_Data`. L'unité d'exécution se réveille régulièrement et envoie un événement. Si vous devez interroger périodiquement la ressource concernant des événements, vous pouvez utiliser la structure de la classe `Event_Data` qui a été générée :

1. Créez et démarrez une unité d'exécution à partir du constructeur `Event_Data`.
2. Dans la méthode d'exécution de l'unité d'exécution, générez une boucle jusqu'à ce que l'agent se termine.
3. Procédez à une mise en sommeil pendant un certain temps avant de vérifier la présence d'événements. Vous pouvez modifier l'intervalle d'interrogation de 5 000 millisecondes en une valeur plus adaptée à votre agent.
4. Déterminez si un ou plusieurs événements se sont produits. L'application générée n'effectue pas cette vérification et transmet toujours un seul événement.
5. Pour chaque événement à envoyer, extrayez les données à transmettre.
6. Créez et renseignez l'objet Attributs (comme l'a fait la méthode `collectData` pour un groupe d'attributs échantillonnés).
7. Appelez la méthode `Attributes.sendEventData`. Les événements constituant une ligne unique, vous ne pouvez envoyer qu'une seule ligne à la fois.

Par ailleurs, si vous travaillez avec une API Java qui signale les événements issus de sa propre unité d'exécution, vous pouvez initialiser cette unité d'exécution dans le constructeur `Event_Data`. Vous pouvez également enregistrer votre propre objet de gestion d'événement à l'aide du mécanisme de gestion des événements de votre ressource. Dans votre gestionnaire d'événements, procédez comme suit :

1. Extrayez les données d'événements à envoyer.
2. Créez et remplissez l'objet Attributs.

3. Appelez la méthode `Attributes.sendEventData`.

Dans ce cas, vous n'avez pas à créer votre propre unité d'exécution dans la classe `Event_Data` et vous n'avez pas besoin de la classe `SampleEventClass`.

Envoi d'événements dans un sous-noeud

Lorsqu'un événement est détecté pour un groupe d'attributs de sous-noeud, l'application Java doit envoyer l'événement au sous-noeud approprié.

Cet exemple part du principe qu'une propriété de configuration, `K91_INSTANCE_KEY`, contient une valeur qui identifie une instance de ressource pouvant générer des événements. Il présume également que la valeur de la propriété `K91_INSTANCE_KEY` est extraite avec les données à envoyer dans l'événement. Pour extraire la propriété et les données, l'application Java effectue les étapes suivantes :

1. Extraction des données d'événements à envoyer avec la “clé d'instance”.
2. Création et remplissage de l'objet Attributs.
3. Extraction de la liste de tous les ID d'instance de sous-noeud configurés par appel de `AgentConnection.getConfiguredSubnodeInstanceIDs`.
4. Pour chaque instance de sous-noeud, extraction de la valeur de `K91_INSTANCE_KEY` par appel de `AgentConnection.getSubnodeConfigurationProperty`.
5. A la détection d'une correspondance entre la valeur de `K91_INSTANCE_KEY` et la valeur obtenue avec les données d'événement, mémorisation de l'ID d'instance de sous-noeud correspondant.
6. Appel de `Attributes.sendSubnodeEventData`, avec transmission de l'ID d'instance de sous-noeud mémorisé.

L'application générée n'effectue pas la recherche décrite aux étapes 4 et 5, mais envoie un événement au groupe d'attributs de chaque sous-noeud. Ce comportement n'est probablement pas approprié pour un agent de production.

Commandes `Action`

Les commandes `Action` sont définies dans Tivoli Enterprise Portal ou à l'aide de la commande `tacmd createaction`. Les actions peuvent être importées dans le projet Agent Builder de l'agent de sorte qu'elles sont créées lors de l'installation de l'agent. Pour plus d'informations sur l'importation des commandes `Action`, voir («Importation des fichiers de prise en charge de l'application», à la page 1447).

L'application Java générée s'enregistre pour toutes les actions qui commencent par le code produit de l'agent, par exemple, `K91Refresh`. Cet enregistrement s'effectue dans la classe auxiliaire principale (`MainClassBase`) à partir de la méthode `registerActionPrefix`. Si vous souhaitez enregistrer d'autres préfixes ou ne pas vous enregistrer du tout pour les actions, redéfinissez `registerActionPrefix` dans `MainClassBase`.

Lorsque l'agent doit exécuter une action qui commence par un préfixe que votre agent a enregistré, la méthode `MainClass.takeAction` est appelée. Ajoutez du code pour appeler `Request.getAction()`, effectuez l'action appropriée, puis appelez `AgentConnection.sendActionReturnCode` pour envoyer le code retour de votre action. Le code retour `0` indique que l'action a abouti, tout autre code retour indique que l'action a échoué.

Gestion des exceptions

Les méthodes `collectData` et `takeAction` peuvent émettre n'importe quelle exception Java, vous pouvez donc autoriser votre code de collecte à émettre des exceptions sans les intercepter. La méthode `handleException` (pour `collectData`) ou la méthode `handleActionException` (pour `takeAction`) est appelée lorsque la classe auxiliaire reçoit l'exception.

Pour les exceptions `collectData`, vous devez appeler `AgentConnection.sendError` lorsqu'une exception se produit ou en cas de problème de collecte de données. L'application générée transmet un code d'erreur `GENERAL_ERROR`. Vous devez toutefois remplacer ce code d'erreur par un code défini par

votre agent et qui décrit mieux l'incident qui s'est produit. Pour plus d'informations sur l'ajout de codes d'erreur, voir l'étape («13», à la page 1364).

Pour les exceptions `takeAction`, vous devez appeler `AgentConnection.sendActionReturnCode` avec un code retour différent de zéro.

Certaines méthodes `AgentConnection` émettent des exceptions dérivées de `com.ibm.tivoli.monitoring.agentFactory.customProvider.CpciException`. La méthode `handleException` n'est pas appelée si une exception `CpciException` est émise lors de la collecte de données car la classe auxiliaire gère l'exception.

Remarque : Si vous choisissez d'intercepter vos exceptions dans la méthode `collectData` au lieu d'utiliser la méthode `handleException`, assurez-vous que toutes les exceptions `CpciException` sont renvoyées. Vous vérifiez le renvoi de l'exception `CpciException` pour qu'elle soit traitée par la classe de base.

Codes d'erreur

En réponse à une exception ou à toute autre erreur liée aux ressources, un code d'erreur est généralement transmis à l'agent par appel de la méthode `AgentConnection.sendError`. Une erreur liée à un groupe d'attributs basé sur des événements peut être envoyée à tout moment. Une erreur liée à un groupe d'attributs échantillonnés ne peut être envoyée qu'en réponse à une demande de collecte de données et à la place d'un appel `sendData`.

Lorsque vous envoyez une erreur à l'agent, les opérations suivantes s'exécutent :

1. Un message d'erreur est consigné dans le journal de trace de l'agent. Ce message d'erreur contient le code d'erreur et le message défini pour ce code d'erreur.
2. Une requête de statut d'objet de performances permettant d'obtenir des informations relatives au statut des groupes d'attributs s'affiche. La colonne Code d'erreur indique le type de code d'erreur défini pour l'erreur envoyée. Le statut d'erreur est effacé une fois que l'agent a correctement reçu les données du groupe d'attributs. Si vous répondez à une requête de collecte de données par un appel `sendData` sans avoir inclus de ligne de données, la colonne Code d'erreur affiche `NO_INSTANCES_RETURNED`.

Le tableau suivant décrit certains de codes d'erreur internes à l'agent que vous pouvez obtenir dans certaines situations :

Tableau 287. Codes d'erreur internes de l'agent

Code d'erreur	Description
`NO_ERROR`	Indique que le groupe d'attributs ne présente pas de problèmes.
`NO_INSTANCES_RETURNED`	L'application Java a répondu à une demande de collecte de données mais n'a fourni aucune donnée. Le fait de ne pas fournir de données ne constitue pas une erreur. Cela indique généralement qu'il n'existe aucune instance de la ressource que surveille le groupe d'attributs.
`OBJECT_NOT_FOUND`	L'agent a tenté de collecter des données pour un groupe d'attributs qui n'est pas enregistré via l'API client. Cette erreur peut signifier que l'application n'a pas réussi à démarrer ou n'a pas initié l'enregistrement du groupe d'attributs au moment où l'agent a tenté de collecter des données.
`OBJECT_CURRENTLY_UNAVAILABLE`	L'application a envoyé à l'agent un code d'erreur non défini dans la liste globale des codes d'erreur.

Tableau 287. Codes d'erreur internes de l'agent (suite)	
Code d'erreur	**Description**
GENERAL_ERROR	Un incident s'est produit lors de la collecte de données à partir de l'application, généralement parce que l'application n'a pas répondu à la requête dans le délai imparti. Consultez le journal de trace de l'agent pour plus de détails. L'application peut également spécifier GENERAL_ERROR comme code d'erreur, mais il est préférable de définir un code d'erreur plus détaillé.

Changements au niveau de l'agent

Certains des changements apportés à l'agent nécessitent les changements correspondants au niveau de l'application Java. Si les changements structurels sont complexes, vous pouvez supprimer certains ou la totalité des fichiers source Java avant de sauvegarder l'agent. Vous pouvez également supprimer les fichiers si vous souhaitez recommencer sans les personnalisations que vous avez apportées.

Le tableau suivant décrit les modifications à apporter aux fichiers source de l'application Java après certains changements dans Agent Builder lors de la sauvegarde de l'agent.

Tableau 288. Changements au niveau d'un agent nécessitant des modifications de la source Java		
Changement au niveau de l'agent	**Action d'Agent Builder**	**Modifications manuelles nécessaires au niveau du source Java**
Changement du nom du package de la classe principale	• Génère toutes les classes dans la nouvelle structure de package • Supprime toutes les classes auxiliaires de l'ancien package	• Portez le contenu de la classe principale et de la classe des groupes d'attributs depuis les classes de l'ancien package vers les classes du nouveau package. • Supprimez les classes de l'ancien package une fois la migration terminée.
Changement du nom de la classe principale	• Crée de nouvelles classes principales. • Supprime l'ancienne classe auxiliaire principale.	• Portez le contenu de la classe principale vers la nouvelle classe. • Mettez à jour les références au nom de la classe à partir des classes des groupes d'attributs.
Ajout d'un groupe d'attributs de l'API Java	• Crée des classes pour le nouveau groupe d'attributs. • Ajoute un enregistrement pour le nouveau groupe d'attributs dans la classe auxiliaire principale.	Remplacez l'exemple de code par la logique personnalisée dans la classe du groupe d'attributs.

Tableau 288. Changements au niveau d'un agent nécessitant des modifications de la source Java (suite)

Changement au niveau de l'agent	Action d'Agent Builder	Modifications manuelles nécessaires au niveau du source Java
Suppression d'un groupe d'attributs de l'API Java	Supprime l'enregistrement de la classe auxiliaire principale.	• Supprimez la classe du groupe d'attributs ou portez la logique personnalisée vers une autre classe. • Supprimez la classe auxiliaire du groupe d'attributs.
Changement de nom d'un groupe d'attributs de l'API Java	• Crée des classes pour le nouveau nom du groupe d'attributs. • Met à jour l'enregistrement pour le groupe d'attributs renommé dans la classe auxiliaire principale.	• Portez la logique personnalisée dans la classe du groupe d'attributs portant l'ancien nom vers la classe du groupe d'attributs portant le nouveau nom. • Supprimez la classe du groupe d'attributs portant l'ancien nom. • Supprimez la classe auxiliaire du groupe d'attributs portant l'ancien nom.
Ajout d'un attribut à un groupe d'attributs de l'API Java	Met à jour la classe interne Attributs dans la classe auxiliaire du groupe d'attributs.	Collectez des données pour le nouvel attribut dans la classe du groupe d'attributs.
Suppression d'un attribut d'un groupe d'attributs de l'API Java	Met à jour la classe Attributs dans la classe auxiliaire du groupe d'attributs.	Supprimez la collecte de données de l'ancien attribut dans la classe du groupe d'attributs.
Changement du nom d'un attribut d'un groupe d'attributs de l'API Java	Met à jour le nom d'attribut de la classe Attributs dans la classe auxiliaire du groupe d'attributs.	Mettez à jour toutes les références au nom de l'attribut dans la classe Attributs (généralement, ces références n'existent pas du fait de l'utilisation du constructeur d'attributs, avec arguments positionnels).
Réorganisation des attributs d'un groupe d'attributs de l'API Java	Met à jour l'ordre des attributs dans la classe Attributs dans la classe auxiliaire du groupe d'attributs.	Mettez à jour l'ordre des arguments dans tous les appels au constructeur d'attributs.

Certains des changements mentionnés dans le tableau précédent peuvent être rationalisés si vous utilisez l'action Rename d'Eclipse Refactor. Appliquez cette action sur tous les noms affectés (y compris les noms de classe auxiliaire) avant de sauvegarder l'agent modifié.

Utilisation de l'API Java

L'interface de programme d'application Java est utilisée dans l'ensemble de l'application Java générée pour communiquer avec l'agent. Le plus souvent, votre seule interaction directe avec l'API Java consiste à modifier un paramètre d'un appel de méthode existant. Par exemple, la modification d'un code d'erreur GENERAL_ERROR envoyé par un code d'erreur défini dans votre agent.

Si vous avez besoin d'effectuer une codification plus étendue avec l'API Java, vous pouvez afficher Javadoc depuis l'éditeur de texte Eclipse. Vous pouvez afficher Javadoc pendant l'édition du code Java en procédant comme suit :

1. Mettez en évidence un nom de package, de classe ou de méthode à partir de l'interface de programme d'application.
2. Appuyez sur **F1** pour ouvrir l'aide Eclipse.
3. Sélectionnez le lien Javadoc.

Vous pouvez également afficher une brève description issue de Javadoc en survolant un nom de classe ou de méthode. Le Javadoc de l'interface de programme d'application est également accessible dans le Knowledge Center de Tivoli Monitoring (voir Javadoc).

Les classes de l'interface de programme d'application Java figurent dans le fichier `cpci.jar`. Le fichier `cpci.jar` est automatiquement ajouté au chemin de génération Java du projet lorsqu'un agent qui contient un groupe d'attributs d'interface de programme d'application Java est créé. Ce fichier est également ajouté lors de l'importation d'un agent contenant un groupe d'attributs de l'API Java, et lorsqu'un groupe d'attributs de l'API Java est ajouté à un agent existant. Le fichier `cpci.jar` est également automatiquement ajouté à chaque agent contenant un groupe d'attributs d'interface de programme d'application Java et au chemin CLASSPATH de l'application Java.

Configuration de l'API Java
Lorsque vous définissez une source de données de l'API Java dans votre agent, des propriétés de configuration sont créées pour vous.

Si vous définissez une source de données de l'interface de programme d'application Java dans votre agent, celui-ci doit utiliser Java pour se connecter au serveur de l'interface de programme d'application Java. Les propriétés de configuration Java s'ajoutent automatiquement à l'agent. Les propriétés de configuration Java suivantes sont propres à la configuration d'exécution de l'agent :

Tableau 289. Propriétés de configuration Java

Nom	Valeurs admises	Obligatoire	Description
Répertoire de base Java	Chemin complet d'accès à un répertoire	Non	Chemin complet pointant vers le répertoire d'installation Java.
Niveau de trace Java	Choix	Oui	Cette propriété permet d'indiquer le niveau de trace utilisé par les fournisseurs Java.
Arguments JVM	Chaîne	Non	Utilisez cette propriété pour indiquer une liste facultative d'arguments pour la machine virtuelle Java.
Chemin d'accès aux classes pour les fichiers JAR	Chaîne	Non	Chemin contenant tous les fichiers JAR qui ne sont pas inclus dans l'agent, mais qui sont nécessaires au fonctionnement du client de l'environnement d'exécution.

Ces variables de configuration sont disponibles sur la page **Informations sur la configuration d'exécution** de l'éditeur d'agent, sous **Configuration de la machine virtuelle Java (JVM)** et **Configuration de l'API Java**.

Test des groupes d'attributs d'application Java

Vous pouvez tester le groupe d'attributs d'application Java que vous avez créé, dans Agent Builder.

Avant de commencer

Restriction : Contrairement à la plupart des autres groupes d'attributs, vous ne pouvez pas tester le groupe d'attributs de l'application Java lorsque celui-ci est en cours de création. Vous pouvez tester le groupe d'attributs lorsqu'il est ajouté à l'agent, l'agent est alors enregistré. Lors de l'enregistrement de l'agent, le code Java est généré pour le groupe d'attributs.

Procédure

1. Après la création de l'agent, sélectionnez un groupe d'attributs sur l'**éditeur d'agent** dans la page **Définition de la source de données** et cliquez sur **Tester**.

   Pour plus d'informations sur l'éditeur d'agent, voir «Utilisation de l'éditeur d'agent pour modifier l'agent», à la page 1207.

   Après avoir cliqué sur **Tester** dans l'une des deux étapes précédentes, la fenêtre **Tester le client Java** s'affiche.
2. Facultatif : Définissez les variables d'environnement, les propriétés de configuration, ainsi que des informations Java avant de démarrer le test. Pour plus d'informations, voir «Test des groupes d'attributs», à la page 1420. Pour plus d'informations sur les propriétés de configuration d'exécution Java par défaut, voir «Configuration de l'API Java», à la page 1376.
3. Cliquez sur l'option de **démarrage de l'agent**. Une fenêtre indique que l'agent est en cours de démarrage.
4. Pour simuler une demande de données d'agent provenant de Tivoli Enterprise Portal ou de SOAP, cliquez sur **Collecte de données**.

   L'agent recherche des données dans le client Java. La fenêtre de **test du client Java** affiche toutes les données renvoyées.
5. Facultatif : Cliquez sur **Vérifier les résultats** si les données renvoyées ne sont pas celles que vous attendez.

   La fenêtre **Statut de la collecte de données** affiche des informations supplémentaires sur les données. Les données collectées et affichées par la fenêtre Statut de la collecte de données sont décrites dans «Noeud de statut d'objet de performances», à la page 1466
6. Arrêtez l'agent en cliquant sur **Arrêter l'agent**.
7. Cliquez sur **OK** ou **Annuler** pour quitter la fenêtre **Tester le client Java**. Cliquez sur **OK** pour sauvegarder les modifications que vous avez apportées.

Concepts associés

«Test de votre agent dans Agent Builder», à la page 1420
Après avoir utilisé Agent Builder pour créer un agent, vous pouvez tester l'agent dans Agent Builder.

Création de jeux de données à partir de sources existantes

Quand au moins un jeu de données existe, vous pouvez en créer un nouveau à partir d'un jeu de données existant.

L'option de création d'un nouveau jeu de données est disponible sur la page **Source de données initiales de l'agent** et sur la page **Emplacement de la source de données**. Vous pouvez créer un groupe d'attributs à l'aide de sources de données existantes via l'une des méthodes suivantes :

1. Jointure des données à partir de deux jeux de données existants (groupes d'attributs). Pour plus d'informations, voir «Jointure de deux groupes d'attributs», à la page 1378.

2. Filtrage des données à partir d'un jeu de données existant (groupe d'attributs). Pour plus d'informations, voir «Création d'un groupe d'attributs filtré», à la page 1383.

Conseil : L'option permettant de joindre deux jeux de données est disponible seulement après la création d'au moins deux jeux de données.

Jointure de deux groupes d'attributs

Créez un groupe d'attributs à partir de deux autres groupes d'attributs.

Pourquoi et quand exécuter cette tâche

La jointure de groupes d'attributs est particulièrement utile lorsque l'agent collecte des données de deux types de sources de données différents. Par exemple, l'agent peut collecter les données WMI et PerfMon, ou SNMP et les sources de données de script. Chaque ensemble d'attributs peut s'avérer plus utile lorsqu'il est utilisé conjointement dans une seule vue Tivoli Enterprise Portal.

Par exemple, supposons que vos groupes d'attributs soient définis comme suit :

```
First_Attribute_Group
    index integer
    trafficRate    integer
    errorCount    integer
```

```
Second_Attribute_Group
    index2    integer
    name string
    traffic string
```

Une des définitions vous fournit des compteurs (comme Perfmon) et l'autre des informations d'identification. Aucun groupe d'attributs ne vous est utile seul. Toutefois, si vous combinez les deux groupes d'attributs à l'aide de l'index pour que les lignes appropriées de chaque groupe concordent, vous disposez alors d'un groupe d'attributs plus puissant. Vous pouvez utiliser le groupe d'attributs combinés pour afficher en même temps le nom, le type et les métriques.

Ce même mécanisme permet d'ajouter des balises aux informations collectées via des groupes d'attributs normaux. Les informations peuvent ensuite être corrélées plus aisément dans un système d'événements en cas de détection d'un incident. Par exemple, une société souhaite gérer tous ses serveurs en collectant des données communes et en utilisant des situations courantes pour surveiller l'état de santé des serveurs. Elle souhaite également être en mesure d'identifier les serveurs à l'aide d'informations supplémentaires indiquant quelle application est en cours d'exécution sur un serveur particulier. D'autre part, la société souhaite contrôler les valeurs utilisées sur chaque serveur, mais ne veut pas créer des agents différents pour chaque application. Pour cela, elle peut créer un groupe d'attributs supplémentaire dans son agent unique, en procédant comme suit :

```
Application_Information
    application_type     integer
    application_name    string
    application_group    string
```

Ce groupe d'attributs est défini sous la forme d'un groupe d'attributs de script qui collecte ses valeurs à partir de la configuration d'agent. Vous pouvez indiquer des valeurs différentes pour chaque instance d'agent et utiliser un seul agent pour gérer tous ses systèmes. Ce groupe d'attributs est ensuite joint à tous les groupes d'attributs source sur lesquels ces informations d'application peuvent être requises. Les informations sont ensuite disponibles dans Tivoli Enterprise Portal, dans les situations, dans les événements et dans les données entreposées.

Lors de la jointure de deux groupes d'attributs, un troisième groupe est créé. Ce groupe d'attributs contient tous les attributs contenus dans les groupes d'attributs source.

Les résultats d'une opération de jointure varient selon le nombre de lignes pris en charge par chaque groupe d'attributs source. Si les deux groupes d'attributs sont définis pour ne renvoyer qu'une seule ligne de données, le groupe d'attributs joint qui en résulte comporte une seule ligne de données. Cette ligne contient tous les attributs des deux groupes d'attributs source.

Tableau 290. Groupe d'attributs source 1 (ligne unique)		
Attribut1	**Attribut2**	**Attribut3**
16	texte	35

Tableau 291. Groupe d'attributs source 2 (ligne unique)			
Attribut4	**Attribut5**	**Attribut6**	**Attribut7**
5001	données supplémentaires	56	35

Tableau 292. Jointure résultante						
Attribut1	**Attribut2**	**Attribut3**	**Attribut4**	**Attribut5**	**Attribut6**	**Attribut7**
16	texte	35	5001	données supplémentaires	56	35

Supposons qu'un groupe d'attributs source soit défini pour ne renvoyer qu'une seule ligne (ligne unique), alors que l'autre peut en renvoyer plusieurs (multiligne). Le groupe d'attributs joint qui en résulte contient le même nombre de lignes que le groupe d'attributs source multiligne. Les données du groupe d'attributs à ligne unique s'ajoutent à chaque ligne du groupe d'attributs multiligne.

Tableau 293. Groupe d'attributs source 1 (ligne unique)		
Attribut1	**Attribut2**	**Attribut3**
16	texte	35

Tableau 294. Groupe d'attributs source 2 (plusieurs lignes)			
Attribut4	**Attribut5**	**Attribut6**	**Attribut7**
user1	path1	56	35
user2	path2	27	54
user3	path3	44	32

Tableau 295. Jointure résultante						
Attribut1	**Attribut2**	**Attribut3**	**Attribut4**	**Attribut5**	**Attribut6**	**Attribut7**
16	texte	35	user1	path1	56	35
16	texte	35	user2	path2	27	54
16	texte	35	user3	path3	44	32

Enfin, supposons que les deux groupes d'attributs source soient définis pour renvoyer plusieurs lignes. Vous devez identifier un attribut de chaque groupe d'attributs source sur lequel effectuer la jointure. Le groupe d'attributs résultant contient des lignes de données où la valeur de l'attribut du premier groupe d'attributs correspond à la valeur de l'attribut du deuxième groupe.

Tableau 296. Groupe d'attributs source 1 (plusieurs lignes)		
Attribut1	**Attribut2**	**Attribut3**
16	texte	35

Tableau 296. Groupe d'attributs source 1 (plusieurs lignes) (suite)		
Attribut1	**Attribut2**	**Attribut3**
27	texte supplémentaire	54
39	une autre chaîne	66

Tableau 297. Groupe d'attributs source 2 (plusieurs lignes)			
Attribut4	**Attribut5**	**Attribut6**	**Attribut7**
user1	path1	56	35
user2	path2	27	54
user3	path3	44	32

Tableau 298. Jointure résultante (jointure sur Attribut3 et Attribut7)						
Attribut1	**Attribut2**	**Attribut3**	**Attribut4**	**Attribut5**	**Attribut6**	**Attribut7**
16	texte	35	user1	path1	56	35
27	texte supplémentaire	54	user2	path2	27	54

Agent Builder permet également de joindre des groupes d'attributs utilisateur au groupe d'attributs Disponibilité, si des filtres de disponibilité sont définis dans votre agent. Pour plus d'informations sur les données contenues dans le groupe d'attributs Disponibilité, voir («Noeud de disponibilité», à la page 1461).

Vous pouvez créer ce type de groupe d'attributs en appelant le menu de l'arborescence des sources de données en cliquant à l'aide du bouton droit, puis en sélectionnant **Joindre des groupes d'attributs**.

Procédure

1. Sur la page **Définition de la source de données**, cliquez avec le bouton droit de la souris sur l'un des groupes d'attributs à joindre, puis sélectionnez **Joindre des groupes d'attributs**.

   Cette option n'est visible que s'il y a au moins deux groupes d'attributs définis. Un filtre de disponibilité défini compte comme un groupe d'attributs défini.

   La page **Informations sur le groupe d'attributs** s'ouvre.

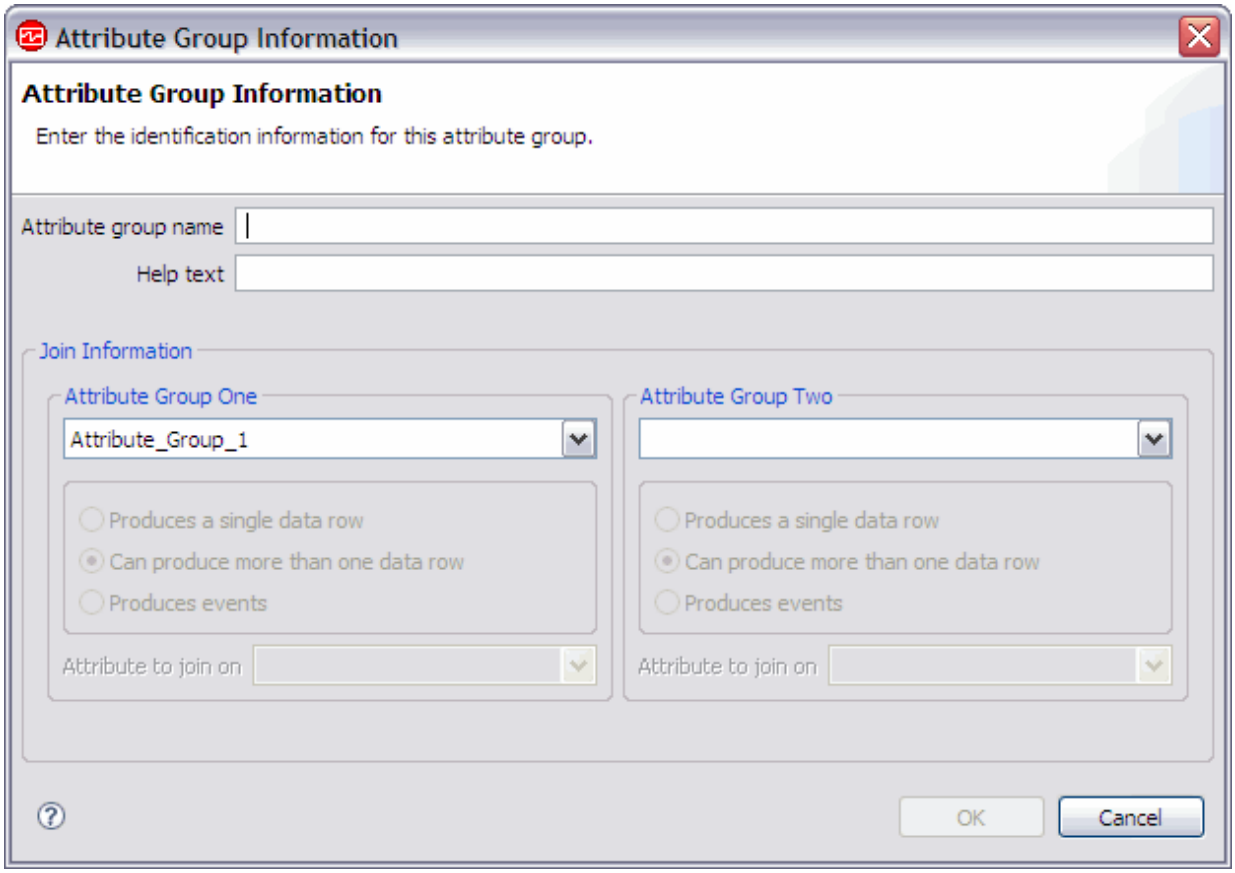


*Figure 48. Page **Informations sur le groupe d'attributs**Fenêtre Informations sur le groupe d'attributs*

2. Dans la zone **Informations de jointure**, sélectionnez les deux groupes d'attributs à joindre. Effectuez votre choix parmi les groupes disponibles dans les listes **Groupe d'attributs Un** et **Groupe d'attributs Deux**.

   Pour chaque groupe d'attributs, l'option **Génère une ligne de données unique** ou l'option **Peut générer plusieurs lignes de données** est sélectionnée. Cette sélection est verrouillée et dépend de la définition initiale des groupes d'attributs source.

   Remarque : Les restrictions suivantes s'appliquent aux jointures de groupes d'attributs :

   - Vous ne pouvez pas joindre un groupe d'attributs appartenant à un type de sous-noeud à un groupe d'attributs d'un autre type de sous-noeud.
   - Vous ne pouvez joindre un groupe d'attributs d'événement qu'à un groupe d'attributs à ligne unique, non basé sur des événements.

   a) Vous devez sélectionner, pour chaque attribut, l'attribut sur lequel effectuer la jointure dans **Peut générer plusieurs lignes de données,**, sous **Attribut sur lequel effectuer la jointure**.

   Les zones **Nom du groupe d'attributs** et **Aide** sont renseignées à l'aide des informations relatives aux groupes d'attributs sélectionnés. Si vous le souhaitez, vous pouvez les modifier.
3. Cliquez sur **OK**.

Résultats

Le groupe d'attributs joint que vous avez créé est ajouté à la zone **Informations sur le groupe d'attributs** de la page **Définition de la source de données**

Manipulation des attributs de groupes d'attributs joints

L'utilisation d'attributs dans des groupes d'attributs joints peut imposer des règles supplémentaires sur le mode de manipulation de ces attributs.

Suppression d'un groupe d'attributs

Un groupe d'attributs ne peut pas être supprimé s'il est référencé dans un groupe d'attributs joint, sauf si ce dernier est également en cours de suppression.

Suppression d'un attribut

Un attribut ne peut pas être supprimé si son groupe d'attributs parent est référencé dans un groupe d'attributs joint et qu'une des conditions suivantes est remplie :

- L'attribut est défini comme attribut de jointure dans le groupe d'attributs joint.
- L'attribut est utilisé dans un attribut dérivé du groupe d'attributs joint.

Les attributs joints ne peuvent pas être supprimés. Seuls les attributs dérivés, si certains sont ajoutés, peuvent être supprimés du groupe d'attributs joint.

Réorganisation d'attributs

L'ordre des attributs joints est fixé par l'ordre des attributs source. La liste d'attributs joints ne peut pas être réorganisée. Seuls les attributs dérivés, s'il y en a, peuvent être réorganisés.

Lorsque la version d'un agent est validée, les attributs source et dérivés ne peuvent être ni réorganisés, ni supprimés. Les attributs ajoutés dans une nouvelle version de l'agent, qu'il s'agisse d'attributs source ou d'attributs dérivés, viendront après tous les attributs validés. Pour plus d'informations, voir «Validation d'une version de l'agent», à la page 1225.

Ajout d'un attribut

Il n'est pas possible d'ajouter explicitement de nouveaux attributs joints. Seuls des attributs dérivés peuvent être créés explicitement.

Suppression de filtres de disponibilité

Le dernier filtre de disponibilité ne peut pas être supprimé si le groupe d'attributs Disponibilité est référencé dans un groupe d'attributs joint.

Attributs joints

Manipulez les informations associées à des attributs joints

Procédure

- Le nom et le texte d'aide d'un attribut joint peuvent être modifiés de sorte qu'ils soient différents de l'attribut source :
  a) Sélectionnez l'attribut dans le groupe d'attributs joint, sur le panneau **Informations sur le groupe d'attributs** de la page **Définition de la source de données**.
  b) Entrez le nouveau nom et le nouveau texte d'aide.
- L'attribut joint peut être affiché ou non dans Tivoli Enterprise Portal, selon que la case **Afficher l'attribut dans Tivoli Enterprise Portal** est, ou non, cochée. Cette case se trouve dans la section **Informations sur l'attribut joint** de la page **Définition de la source de données**. Cette option est tout à fait indépendante du fait que l'attribut source est, ou non, affiché dans Tivoli(r) Enterprise Portal.
- Tout attribut ou combinaison d'attributs (affichés dans Tivoli Enterprise Portal) peuvent être marqués comme étant des attributs de clé. Pour cela, cochez la case **Attribut de clé**. Cette option est indépendante du fait que les attributs sont des attributs de clé dans les groupes d'attributs source, ainsi que du fait que les attributs source sont, ou non, affichés dans Tivoli(r) Enterprise Portal.

- Les informations relatives au type d'attribut des attributs joints sont héritées des attributs source et ne peuvent pas être modifiées dans l'attribut joint. Dans la section **Informations de groupe d'attributs joint** de l'éditeur d'agent (Figure 49, à la page 1383), cliquez sur **Localiser l'attribut source** pour accéder à l'attribut source.

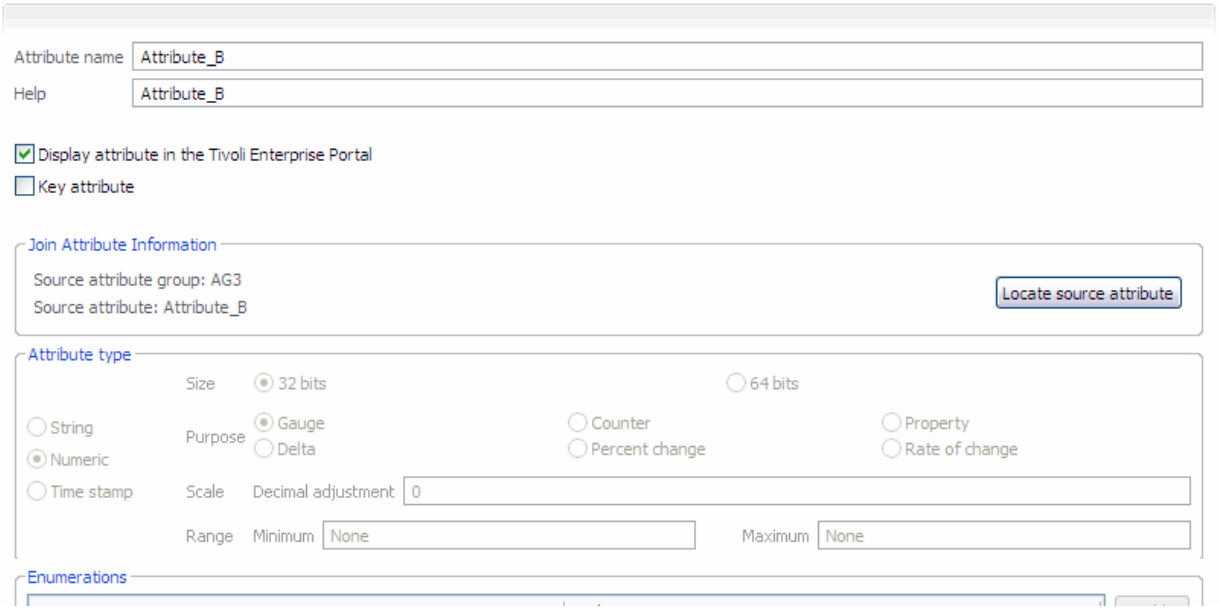


Figure 49. Localiser les informations de l'attribut source

Toute modification apportée aux groupes d'attributs source est répercutée dans les attributs joints. En cas de modification des groupes d'attributs source, ils sont automatiquement mis à jour dans le groupe d'attributs joint. Cette mise à jour automatique se produit également si un groupe d'attributs différent est défini comme groupe d'attributs source. Les modifications apportées à un type d'attribut source sont copiées dans l'attribut joint. Les modifications apportées à un nom ou à un texte d'aide d'attribut source sont reportées dans l'attribut joint. Toutefois, ces modifications ne sont plus copiées si le nom et le texte d'aide d'un attribut joint a été modifié.

Création d'un groupe d'attributs filtré

Créez un groupe d'attributs filtré (ensemble de données) en filtrant les lignes de données d'un groupe d'attributs existant. Si un ensemble de données renvoie plusieurs lignes, vous pouvez créer un groupe filtré qui renvoie une ligne utilisable avec IBM Cloud Application Performance Management.

Pourquoi et quand exécuter cette tâche

Un groupe d'attributs filtré contient les mêmes colonnes que le groupe d'attributs source mais peut exclure quelques lignes. Une formule de sélection est utilisée pour déterminer quelles lignes inclure.

Si vous souhaitez fournir des informations de récapitulatif et de statut pour Cloud APM, vous devez utiliser un ensemble de données qui renvoie une ligne unique. Pour plus de détails, voir «Préparation de l'agent pour Cloud APM», à la page 1417. Si les informations source se trouvent dans un ensemble de données qui renvoie plusieurs lignes, vous pouvez créer un groupe d'attributs filtré qui renvoie une ligne unique.

Par exemple, les sources de données de code retour de commande, de service Windows et de processus fournissent des informations sous forme de lignes dans l'ensemble de données de disponibilité unique. Vous pouvez créer un groupe d'attributs filtré en utilisant la zone NAME dans la formule de sélection. Le groupe inclut le statut de l'application nécessaire. Définissez-le comme renvoyant une seule ligne. Vous pourrez ensuite utiliser ce groupe d'attributs comme l'ensemble de données récapitulatives pour Cloud APM.

Un groupe d'attributs filtré est également très utile lorsqu'une requête de source de données de base renvoie des données que vous préférez scinder en groupes distincts. Windows Performance Monitor, SNMP et WMI sont autant d'illustrations de ces sources de données.

Par exemple, supposons qu'une source de données renvoie les données suivantes :

```
Name    Type  Size  Used  Free
Memory  MEM      8     4     4
Disk1   DISK   300   200   100
Disk2   DISK   500   100   400
```

Il s'agit d'une table qui génère un rapport concernant le stockage qui existe sur le système et qui inclut à la fois la mémoire et l'espace disque. Vous préférerez sans doute le diviser en deux tableaux séparés, à savoir un pour la mémoire et un autre pour le disque. Pour cela, vous créez deux groupes d'attributs de base qui collectent les mêmes données et filtre les lignes indésirables. Cependant, cette méthode n'est pas la plus efficace. A la place, définissez un groupe d'attributs de base qui renvoie les données sur l'utilisation du disque et de la mémoire sous forme regroupée. Définissez ensuite deux groupes d'attributs filtrés. Chacun d'eux utilise la même table de base comme source de données. L'un inclut un filtre avec `Type=="MEM"`, l'autre inclut un filtre avec `Type=="DISK"`.

Dans l'exemple, pour le groupe d'attributs filtré avec `Type=="MEM"`, les données renvoyées sont :

```
Name    Type  Size  Used  Free
Memory  MEM      8     4     4
```

et pour celui avec `Type=="DISK"`, les données renvoyées sont :

```
Name    Type  Size  Used  Free
Disk1   DISK  300   200   100
Disk2   DISK  500   100   400
```

Remarque : Les groupes d'attributs dont les données sont fondées sur des événements ne permettent pas de créer des groupes d'attributs filtrés. Seuls les groupes d'attributs dont les données sont échantillonnées peuvent être utilisés.

Procédure

1. Cliquez sur **Sources de données existantes** dans la zone **Catégories de données de surveillance** sur la page **Source de données initiale de l'agent** ou la page **Emplacement de la source de données**.

   Remarque :

   - vous accédez à la page **Source de données initiale de l'agent** à l'aide de l'assistant de création d'agent. Pour plus d'informations, voir «Création d'un agent», à la page 1204.
   - Vous pouvez accéder à la page **Emplacement de la source de données** en cliquant avec le bouton droit de la souris sur un agent dans la page **Définition de la source de données** de l'**Editeur d'agent** et en sélectionnant **Ajouter une source de données**.
2. Sélectionnez **Filtrer les lignes de données d'un groupe d'attributs** dans la zone **Sources de données**.
3. Cliquez sur **Suivant**

   La page **Filtrer les informations** s'affiche.
4. Sélectionnez un **Groupe d'attributs source** dans la liste.
5. Entrez une **Formule de sélection** pour filtrer les données du groupe d'attributs que vous avez sélectionné.
   Par exemple, dans la page **Filtrer les informations** présentée plus haut, la formule de sélection filtre les lignes de données sur lesquelles l'attribut `Type` est `"DISK"`. Les lignes de données dont l'attribut `Type` ne correspond pas à `"DISK"` sont supprimées. La formule de sélection entrée doit donner un résultat booléen, à savoir vrai ou faux.

Remarque : Dans la page **Filtrer les informations**, vous pouvez cliquer sur **Modifier** pour entrer ou modifier la formule à l'aide de l'éditeur de formule. Pour plus d'informations sur l'éditeur de formule, voir «Editeur de formule», à la page 1237.

6. Cliquez sur **Suivant**.
7. Sélectionnez **Génère une ligne de données unique** ou **Peut générer plusieurs lignes de données**.
   a) Si vous avez sélectionné **Peut générer plusieurs lignes de données**, choisissez un ou plusieurs attributs de clé dans la liste.
8. Cliquez sur **Terminer**.

Création d'un groupe de navigation

Dans un environnement IBM Tivoli Monitoring, les groupes de navigation servent à regrouper plusieurs sources de données associées (groupes d'attributs) afin de créer des espaces de travail affichant des vues des sources de données combinées. Vous pouvez créer un groupe de navigation lors de la création d'un agent à l'aide de l'assistant de création d'agent au niveau de l'agent de base. Vous pouvez également créer un groupe de navigation lors de la définition d'un sous-noeud à l'aide de l'assistant de création de composant d'agent.

Pourquoi et quand exécuter cette tâche

Par exemple, vous pourriez être amené à collecter des données de système de fichiers provenant de plusieurs sources de données. Il peut être utile de créer un espace de travail affichant des vues de toutes les données de système de fichiers issues de ces sources de données différentes.

Les groupes de navigation sont également un bon moyen pour "masquer" les sources de données sur Tivoli Enterprise Portal. Vous pouvez décider que certaines mesures collectées de deux sources de données sont très utiles lorsque les sources de données sont jointes pour créer une source de données combinée. Vous ne voulez voir que les données combinées dans la source de données jointe. Vous pouvez créer un groupe de navigation contenant toutes les trois sources de données et créer un espace de travail contenant des vues qui n'affichent que la source de données combinée. Les deux sources de données d'origine sont masquées dans Tivoli Enterprise Portal. Pour plus d'informations sur la jointure de sources de données, voir «Création de jeux de données à partir de sources existantes», à la page 1377.

Remarque : Lors du regroupement de sources de données dans un groupe de navigation, Tivoli Monitoring n'associe pas de requête au groupe de navigation. On part du principe que vous définissez un espace de travail par défaut pour que le groupe de navigation affiche les sources de données dans un format utile.

Un groupe de navigation peut être défini dans l'agent de base ou dans un sous-noeud. Un groupe de navigation ne peut pas contenir un autre groupe de navigation.

Les groupes de navigation n'ont aucun impact dans un environnement IBM Cloud Application Performance Management.

Procédure

1. Effectuez l'une des opérations suivantes :
   - Lors de la création d'un agent à l'aide de l'assistant d'**agent**, sur la page **Source de données initiale de l'agent**, cliquez sur **Regroupements de sources de données** dans la zone **Catégories de données de surveillance**.
   - Avec un agent existant, procédez comme suit dans l'éditeur d'agent :
     a. Cliquez sur l'onglet **Sources de données** pour ouvrir la page **Définition de la source de données**.
     b. Sélectionnez l'agent, puis cliquez sur **Ajouter à la sélection**.
     c. Sur la page **Emplacement de la source de données**, dans la zone **Catégories de données de surveillance**, cliquez sur **Regroupements de sources de données**.

2. Dans la zone **Sources de données**, cliquez sur **Un groupe de navigation**.
3. Cliquez sur **Suivant**.
4. Dans la fenêtre **Informations sur le groupe de navigation**, entrez le nom du groupe de navigation et le texte d'aide que vous voulez associer au nom, puis cliquez sur **Suivant**.

   Remarque : Agent Builder crée automatiquement des groupes de navigation dans certaines situations. Le nom de groupe de navigation suivant est réservé :

   - Disponibilité

   .
5. Sur la page **Première source de données du groupe de navigation**, sélectionnez la première source de données de surveillance pour le nouveau groupe de navigation. Cliquez sur une catégorie dans la liste **Catégories de données de surveillance** et une source de données dans la liste **Sources de données**. Cliquez ensuite sur **Suivant**.

   Conseil : Vous pouvez créer la source de données comme d'habitude. Vous pouvez également cliquer sur **Sources de données existantes** et choisir de déplacer une ou plusieurs sources de données déjà créées vers le groupe de navigation.
6. Pour créer une source de données dans un groupe de navigation, sélectionnez le groupe de navigation sur la page **Définition de la source de données**, puis cliquez sur **Ajouter à la sélection**.
7. Pour déplacer des sources de données existantes dans le groupe de navigation, sur la page **Définition de la source de données**, sélectionnez le groupe de navigation et cliquez sur **Ajouter à la sélection** et sur la page **Source de données de groupe de navigation**, sélectionnez **Sources de données existantes**. Sur la page **Sources de données actuellement définies**, sélectionnez les sources de données.
8. Pour supprimer une source de données d'un groupe de navigation, effectuez l'une des opérations suivantes sur la page **Définition de la source de données** :
   - Sélectionnez la source de données, puis faites-la glisser vers le niveau supérieur de l'arborescence des sources de données.
   - Sélectionnez la source de données, puis cliquez sur **Supprimer**.
9. Pour créer un groupe de navigation, effectuez l'une des opérations suivantes sur la page **Définition de la source de données** :
   - Cliquez sur **Ajouter à l'agent**.
   - Sélectionnez un sous-noeud et cliquez sur **Ajouter à la sélection**.

Utilisation des sous-noeuds

Les sous-noeuds permettent de surveiller plusieurs composants d'application à partir d'une seule instance de l'agent.

Vous pouvez générer un agent unique effectuant les tâches suivantes à l'aide de sous-noeuds :

- Il surveille chaque instance d'un serveur logiciel exécuté sur un système, au lieu d'avoir à utiliser des instances distinctes de l'agent, une par instance de serveur logiciel.
- Il surveille plusieurs systèmes distants différents, au lieu d'avoir à utiliser des instances distinctes de l'agent, une par système distant.
- Il surveille plusieurs types de ressource différents à partir d'un agent, au lieu d'avoir à générer et déployer plusieurs agents différents.
- Dans IBM Tivoli Monitoring, il affiche un niveau supplémentaire dans l'arborescence de navigation physique de Tivoli Enterprise Portal qui permet un regroupement et une personnalisation supplémentaires. De plus, vous pouvez définir des groupes de systèmes gérés pour obtenir un autre niveau de granularité dans le cadre de situations.
- Dans IBM Cloud Application Performance Management, il fournit des ressources différentes, en affichant divers tableaux de bord récapitulatifs et détaillés. Les ressources de sous-noeud peuvent être

affichées comme des homologues ou des sous-composants de la ressource d'agent. Vous pouvez les intégrer dans des applications indépendantes.

Vous pouvez créer des types de sous-noeud dans Agent Builder. Chaque type doit correspondre à un type de ressource différent pouvant être surveillé par un agent. Ajoutez des sources de données et des ensembles de données au type de sous-noeud pour une ressource surveillée spécifique.

Lorsque vous déployez l'agent sur un hôte surveillé et le configurez, vous pouvez créer une ou plusieurs instances de chaque type de sous-noeud. Chaque instance d'un sous-noeud doit correspondre à une instance d'un serveur, d'un système distant ou de toute ressource à surveiller par le type de sous-noeud. Toutes les instances de sous-noeud d'un type de sous-noeud unique comportent des groupes d'attributs et des espaces de travail dont la forme est identique. Toutefois, chaque instance de sous-noeud possède des données issues de la ressource particulière en cours de surveillance.

Lorsque vous configurez l'agent sur l'hôte surveillé, vous pouvez déterminer le nombre d'instances de sous-noeud. Certaines données de configuration peuvent s'appliquer à l'agent dans son ensemble, alors que d'autres données de configuration s'appliquent à une seule instance de sous-noeud. Configurez chaque instance de sous-noeud de façon différente de sorte qu'elles ne surveillent pas la même ressource et qu'elles n'affichent pas les mêmes données.

Dans un environnement IBM Tivoli Monitoring, une instance de sous-noeud s'affiche dans l'agent de la vue Navigation Physical dans Tivoli Enterprise Portal. Les espaces de travail affichent les données qui sont produites par une instance de sous-noeud et des situations peuvent être distribuées à une ou plusieurs instances d'un sous-noeud. Une liste de systèmes gérés est automatiquement créée ; elle contient toutes les instances du sous-noeud, à l'instar de la liste de systèmes gérés créée pour un agent.

Dans un environnement IBM Cloud Application Performance Management, vous pouvez afficher les instances d'agent et de sous-noeud en tant que ressources surveillées. Chaque instance de sous-noeud devient une ressource distincte. Pour plus de détails, voir «Sous-noeuds dans IBM Cloud Application Performance Management», à la page 1392.

Dans la mesure où les agents générés à l'aide d'Agent Builder créent les instances de sous-noeud en fonction des valeurs de configuration, ces sous-noeuds ont la même durée de vie que l'agent. Il ne reste qu'un seul signal de présence effectué pour l'agent, et non un signal de présence distinct pour chaque sous-noeud. Par conséquent, grâce aux sous-noeuds, vous pouvez considérablement augmenter l'éventuelle échelle de l'environnement de surveillance. L'autre solution consiste à utiliser plusieurs instances de l'agent, ce qui peut limiter l'ampleur potentielle de l'environnement IBM Tivoli Monitoring ou IBM Cloud Application Performance Management.

L'ajout ou la suppression d'un sous-noeud nécessite la reconfiguration de l'agent. Pour reconfigurer l'agent, vous devez l'arrêter et le redémarrer, une opération qui implique l'ensemble des sous-noeuds. Vous pouvez définir l'agent en tant qu'agent multi-instance ; dans ce cas, vous pouvez démarrer et arrêter une instance unique et laisser les autres instances s'exécuter.

Avec les ensembles de données dans les sous-noeuds, un agent peut définir des ensembles de données de niveau agent qui résident hors d'un sous-noeud.

Dans l'arborescence de navigation de Tivoli Enterprise Portal, un type de sous-noeud s'affiche sous le nom de l'agent et les instances de sous-noeud s'affichent sous un type de sous-noeud. A l'instar des agents, les sous-noeuds sont identifiés à l'aide d'un nom de système géré, par exemple, `94:Hill.cmn`.

Par exemple, dans l'arborescence de navigation de la Figure 50, à la page 1388, **Watching Over Our Friends** est un agent comportant trois ressources (**Boarders**, **Common Areas** et **Kennel Runs**) et deux types de sous-noeud (**Common Area** et **Kennel Run**). Des types de sous-noeud sont définis pour deux de ces ressources (**Common Area** et **Kennel Run**). Un sous-noeud n'est pas requis pour la troisième ressource (**Boarder**), qui est représentée par une ligne unique dans une table au niveau de l'agent de base. Le type de sous-noeud Common Area comporte trois instances de sous-noeud : `94:Hill:cmn`, `94:Meadow:cmn` et `94:Tree:cmn` représentant trois common areas dans le Kennel. Le type de sous-noeud Kennel Run comporte quatre instances de sous-noeud : `94:system1:run`, `94:system2:run`, `94:system4:run` et `94:system5:run` représentant quatre kennel runs.

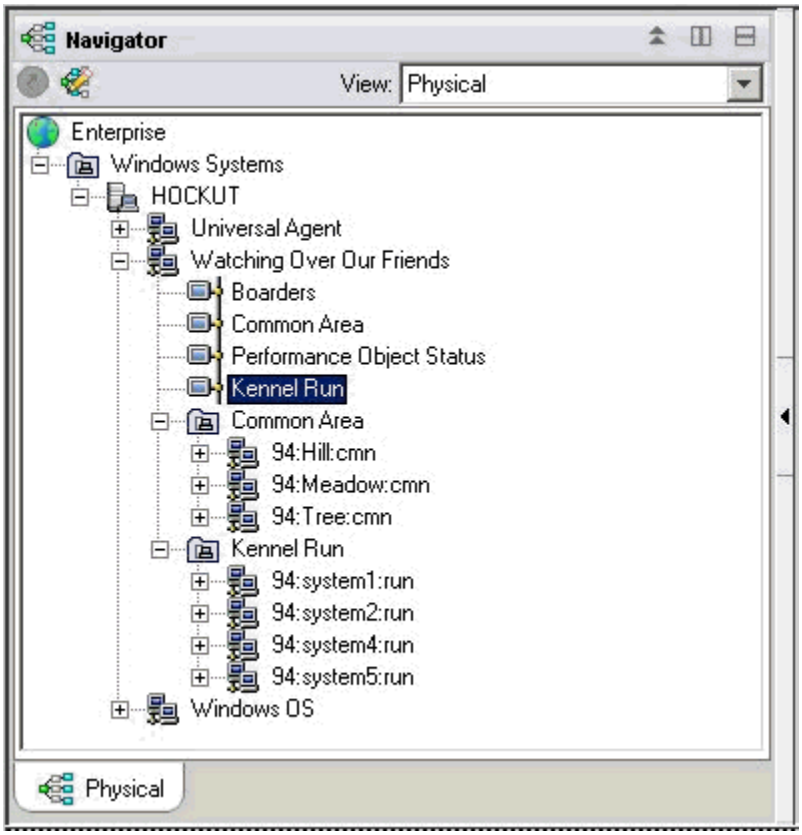


Figure 50. Sous-noeuds de l'arborescence du navigateur

Un agent unique peut utiliser des sous-noeuds selon l'une des méthodes suivantes :

- L'agent peut comporter des sous-noeuds différents du même type.
- L'agent peut comporter des sous-noeuds de types différents.

Sous-noeuds pour des mêmes données issues de sources différentes

Vous pouvez utiliser des sous-noeuds d'un même type pour représenter plusieurs instances d'un type de ressource surveillée. Chaque sous-noeud de même type inclut les mêmes groupes d'attributs et les valeurs correctes de cette instance de ressource surveillée. Le nombre de sous-noeuds varie selon la configuration de l'agent. L'exemple de la Figure 51, à la page 1389, présente la surveillance de systèmes différents.

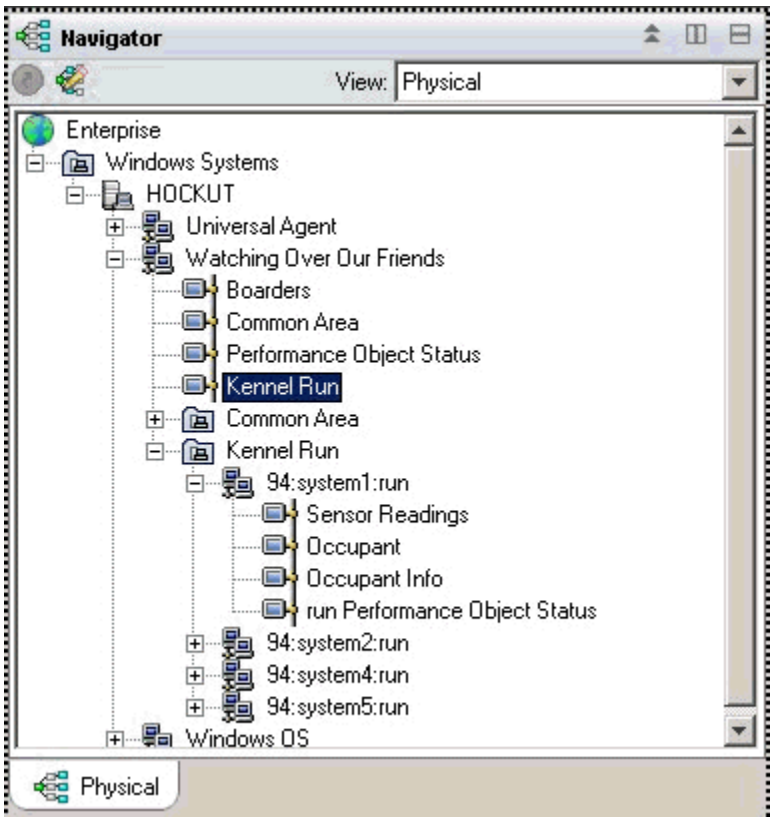


Figure 51. Sous-noeuds surveillant des systèmes différents

Sous-noeuds pour plusieurs types de données

Lorsqu'un agent surveille plusieurs types de ressources surveillées, vous pouvez créer un type de sous-noeud pour chaque type de ressource. Chaque sous-noeud inclut les informations définies dans ce type de sous-noeud. L'exemple ci-dessous présente deux types de sous-noeud. Chaque type surveille un type de ressource différent, des types de données différents étant disponibles pour chaque ressource :

- Common Area
- Kennel Run

L'agent présenté à la Figure 52, à la page 1390 exécute un exemplaire de chaque type de sous-noeud. Il se peut qu'un agent particulier crée un sous-ensemble des agents définis. Les sous-noeuds servent à refléter des profils V5 de Tivoli Monitoring.

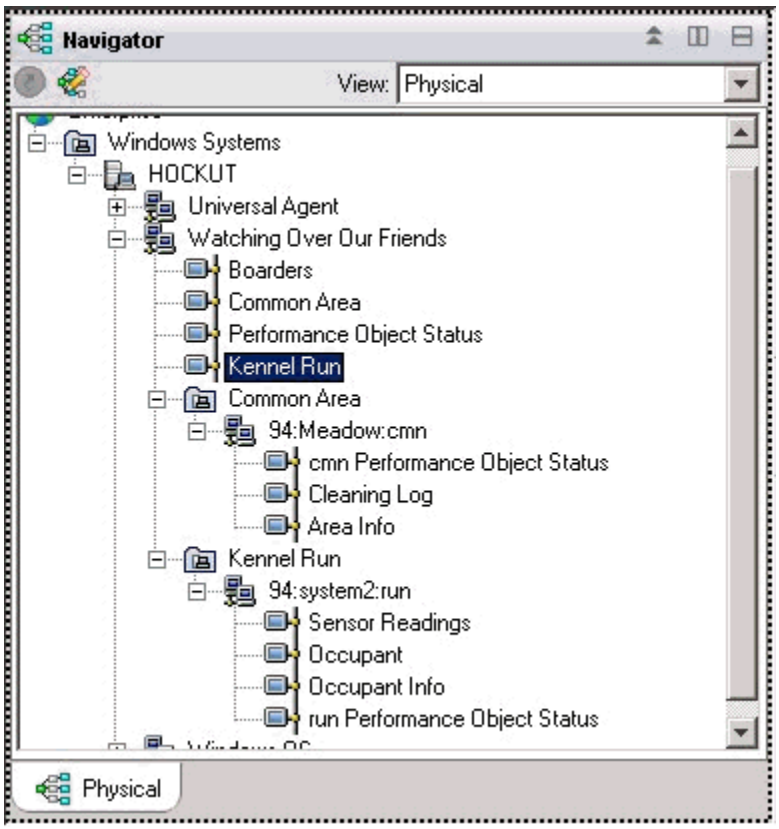


Figure 52. Types de sous-noeuds dans l'arborescence du navigateur

peuvent être utilisées dans le même agent où chaque type peut comporter plusieurs instances de sous-noeud.

La Figure 52, à la page 1390 présente deux types de sous-noeud surveillant deux types de ressource : Common Areas et Kennel Runs. En outre, plusieurs sous-noeuds sont définis pour chaque type. Il existe trois sous-noeuds de type Common Area ; ces sous-noeuds comportent l'ID suivant : Meadow, Hill et Tree. Il existe également quatre sous-noeuds de type Kennel (chacun collectant des données d'un système différent dédié à un Kennel Run) ; ces sous-noeuds comportent les ID suivants : system1, system2, system4 et system5.

Remarque : Les 24 premiers caractères des ID sous-noeud doivent être uniques pour toutes les instances du type de sous-noeud dans l'installation IBM Tivoli Monitoring.

Fournisseurs de données des sous-noeuds

Un sous-noeud peut contenir toute combinaison de données issue des types de fournisseur de données différents. Les fournisseurs de données Agent Builder les plus récents peuvent être utilisés dans un sous-noeud, y compris les fournisseurs de données suivants :

- WMI
- Perfmon
- Journal des événements Windows
- SNMP
- Evénements SNMP
- JMX
- Ping ICMP
- Script

- Journal
- CIM
- JDBC
- HTTP
- SOAP
- Socket
- API Java

Un sous-noeud peut également contenir un groupe d'attributs joint combinant des données de deux autres groupes d'attributs dépendant du même sous-noeud ou de groupes d'attributs de niveau agent.

Statut des sous-noeuds

Le statut d'un agent de sous-noeud peut être déterminé selon deux méthodes. La première méthode consiste à consulter les données affichées dans le groupe d'attributs Statut de l'objet de performances. Ce groupe d'attributs affiche le statut de chacun des autres groupes d'attributs au même niveau dans l'agent. Le groupe d'attributs Statut de l'objet de performances au niveau de l'agent affiche le statut de collecte des autres groupes d'attributs au niveau de l'agent. Le groupe d'attributs Statut de l'objet de performances de chaque sous-noeud affiche le statut de collecte des groupes d'attributs de ce sous-noeud.

Agent Builder crée également un groupe d'attributs par type de sous-noeud, ce qui affiche une seule ligne pour chaque sous-noeud configuré de ce type. Dans l'exemple de la (Figure 53, à la page 1391), quatre sous-noeuds sont en cours d'exécution pour collecter des données.

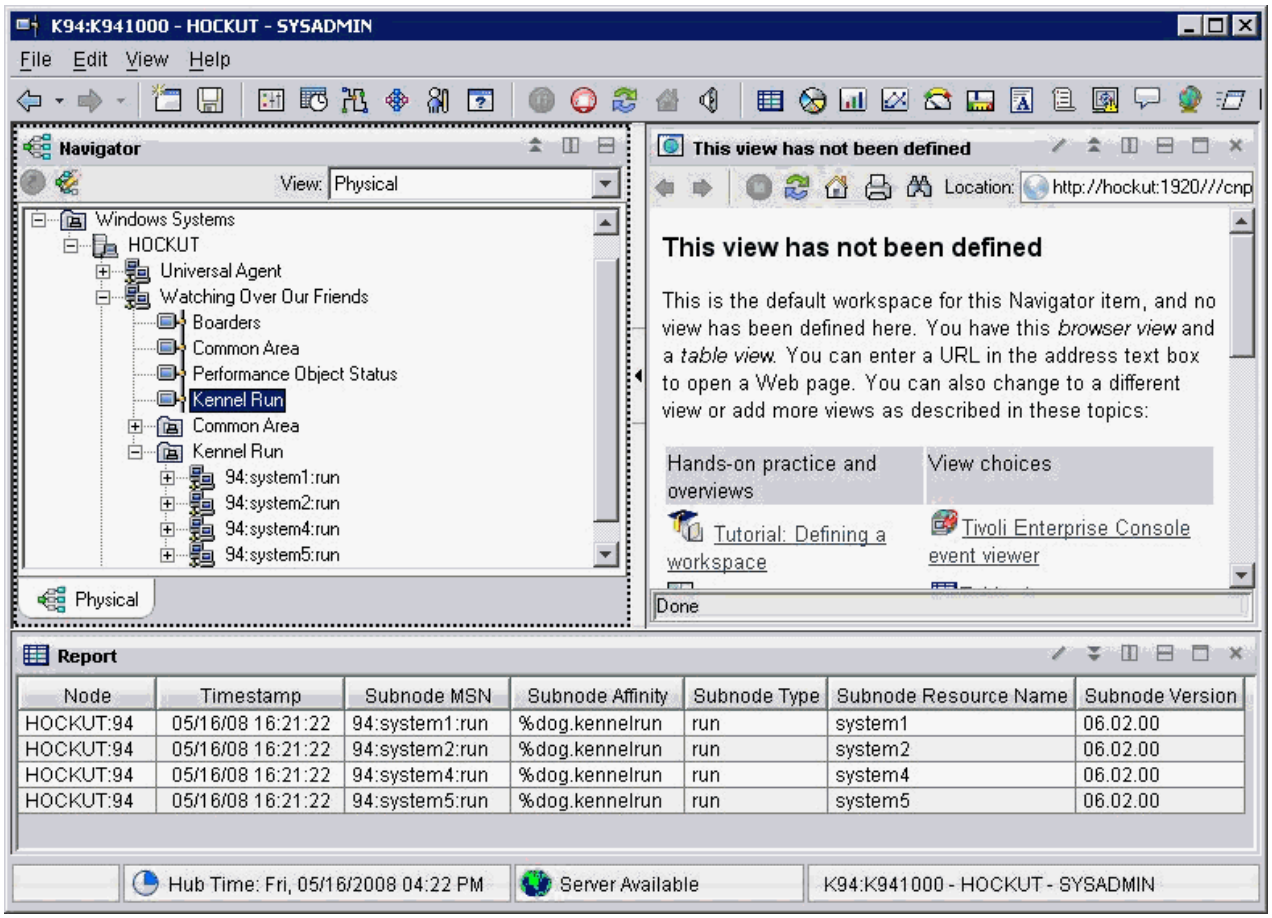


Figure 53. Surveillance de plusieurs instances de sous-noeud du même type de sous-noeud

Dans l'environnement IBM Tivoli Monitoring, le sous-noeud **Statut de l'objet de performances** contient des données visibles dans l'arborescence du navigateur et peut comporter des situations surveillant le statut des autres collectes de données.

Dans l'environnement IBM Cloud Application Performance Management, vous pouvez créer des seuils pour surveiller les données **Statut de l'objet de performances**.

L'exemple de la Figure 54, à la page 1392 présente un cas dans le cadre duquel la collecte de données a échoué (car la commande shell de script est introuvable). En général, toute valeur autre que NO_ERROR indique qu'un incident s'est produit. Pour chacun des collecteurs de données définis dans le sous-noeud, il existe une ligne dans la table.

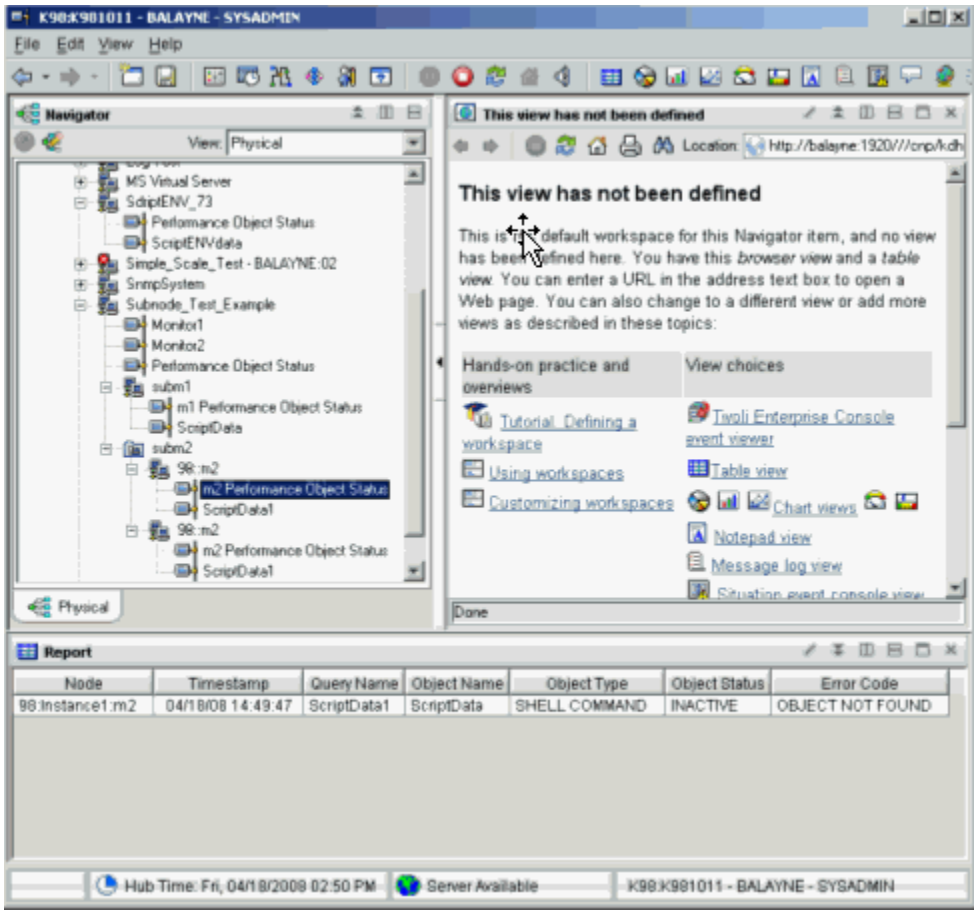


Figure 54. Exemple : collecte de données dans un sous-noeud

Sous-noeuds dans IBM Cloud Application Performance Management

Dans IBM Cloud Application Performance Management, vous pouvez définir une instance d'agent et/ou une instance de sous-noeud en tant que ressources surveillées, chaque ressource correspondant à un tableau de bord récapitulatif.

Les tableaux de bord de sous-noeud ne peuvent pas afficher les données de niveau agent. Pour afficher les données de niveau agent dans cet environnement, définissez un tableau de bord récapitulatif pour l'agent.

Selon les paramètres sélectionnés, les ressources d'agent et de sous-noeud peuvent apparaître au même niveau, sans distinction hiérarchique, ou les ressources de sous-noeud peuvent être répertoriées en tant qu'enfants des ressources d'agent.

Pour obtenir des instructions sur la configuration des ressources d'agent et de sous-noeud, voir «Préparation de l'agent pour Cloud APM», à la page 1417.

Création de sous-noeuds

Vous pouvez créer un sous-noeud en créant ou en éditant un agent.

Procédure

1. Effectuez l'une des opérations suivantes :
   - Lors de la création d'un agent à l'aide de l'assistant d'**agent**, sur la page **Source de données initiale de l'agent**, cliquez sur **Regroupements de sources de données** dans la zone **Catégories de données de surveillance**.
   - Avec un agent existant, procédez comme suit dans l'éditeur d'agent :
     a. Cliquez sur l'onglet **Sources de données** pour ouvrir la page **Définition de la source de données**.
     b. Sélectionnez l'agent et cliquez sur **Ajouter à la sélection**.
     c. Sur la page **Emplacement de la source de données**, dans la zone **Catégories de données de surveillance**, cliquez sur **Regroupements de sources de données**.
2. Dans la zone **Sources de données**, cliquez sur **Définition de sous-noeud**
3. Cliquez sur **Suivant**.
4. Complétez comme suit la page **Informations sur le sous-noeud** afin de définir le nouveau sous-noeud :
   a) Dans la zone **Nom**, entrez le nom du sous-noeud à créer.
   b) Dans la zone **Type**, entrez 1 à 3 caractères (à l'aide de nombres et/ou lettres) pour identifier le type du sous-noeud à créer.
   c) Dans la zone **Description**, entrez une description pour le sous-noeud à créer.
   d) Cliquez sur la case à cocher **Afficher le groupe d'attributs de noeuds pour ce type de sous-noeud** pour masquer ou afficher le groupe d'attributs de disponibilité. Pour plus de détails sur ce groupe d'attributs, voir «Noeud de disponibilité», à la page 1461.
   e) Cliquez sur **Suivant**.
5. Remplissez la page **Source de données de sous-noeud initiale** pour sélectionner une source de données comme premier élément dans le nouveau sous-noeud. Cliquez sur une catégorie dans la liste **Catégories de données de surveillance** et une source de données dans la liste **Sources de données**. Cliquez ensuite sur **Suivant**.

   Conseil : Vous pouvez créer la source de données comme d'habitude. Vous pouvez également déplacer une ou plusieurs sources de données déjà créées vers le groupe de navigation. Pour déplacer les sources de données, cliquez sur **Sources de données existantes** et, sur la page **Sources de données actuellement définies**, sélectionnez les sources de données.

   Important : Vous ne pouvez pas inclure de source de données de processus, de service Windows ou de code de retour de commande dans un sous-noeud. Comme solution de contournement, vous pouvez écrire un script qui détermine les informations de service ou de processus nécessaires et utiliser une source de données de sortie de script.
6. Si votre agent contient des propriétés de configuration personnalisées ou si la source de données sélectionnée nécessite une configuration, utilisez la page **Substitutions de configuration de sous-noeud** pour choisir les propriétés de configuration.

   Dans la fenêtre **Substitutions de configuration de sous-noeud**, choisissez les propriétés de configuration souhaitées pour le sous-noeud au niveau de l'agent. Ensuite, choisissez les propriétés à varier pour chaque sous-noeud.

   Utilisez **Déplacer**, **Copier** et **Supprimer** pour spécifier les propriétés de configuration, selon la procédure décrite dans la section «Configuration d'un sous-noeud», à la page 1394.
7. Cliquez sur **Suivant**.

   La page **Définition de la source de données** s'affiche.

Configuration de sous-noeud

Lorsqu'un sous-noeud est défini, une section de configuration unique est définie tout particulièrement pour ce sous-noeud.

Une section de configuration de sous-noeud est différente d'autres sections de configuration comme suit :

- L'ensemble des propriétés d'une section de sous-noeud peut être dupliqué, de sorte qu'il existe plusieurs ensembles de propriétés. Chaque ensemble de propriétés forme sa propre section. La présentation de toutes les sections est identique, mais des valeurs différentes peuvent être entrées dans chaque section.

  Par contraste, les propriétés des autres sections (qui sont désignées par sections de niveau agent) ne sont présentées qu'une seule fois pendant la configuration d'exécution. Elles ne forment pas des sous-sections et ne peuvent pas être dupliquées ou supprimées.

  Voir «Exemple de configuration de sous-noeud», à la page 1398 pour obtenir des exemples de configuration de sous-noeuds à l'aide de l'interface graphique et de la ligne de commande.
- Pour chaque exemplaire d'une section de noeud créé lors de la configuration d'exécution, l'agent crée une instance de sous-noeud distincte. Toutes ces instances de sous-noeud sont du même type.
- Les noms de propriétés dans les sections de sous-noeud peuvent être des doubles de noms de propriété dans les sections de niveau agent. Lors de la présence de doubles de noms, la valeur de propriété de sous-noeud remplace la valeur de propriété de niveau agent.
- Dans IBM Tivoli Monitoring version 6.2.1 et ultérieure, une section de sous-noeud peut comporter des valeurs de propriété par défaut qui s'appliquent à toutes les instances des sous-noeuds de ce type. Une valeur de propriété unique peut donc être consultée à trois niveaux :
  1. L'agent obtient la valeur de propriété à partir de la sous-section d'instance de sous-noeud.
  2. Si aucune valeur n'est configurée au niveau de l'instance de sous-noeud, la valeur de propriété est obtenue du niveau par défaut du sous-noeud.
  3. Si aucune valeur n'est configurée à l'un ou l'autre de ces deux niveaux, la valeur de propriété est obtenue d'une section de niveau agent.

Voir «Exemple de configuration de sous-noeud», à la page 1398 pour obtenir des exemples de configuration de sous-noeuds à l'aide de l'interface graphique et de la ligne de commande.

Configuration d'un sous-noeud

Utilisez la page **Substitutions de configuration de sous-noeud** pour configurer une source de données de sous-noeud.

Avant de commencer

Suivez les étapes décrites dans «Création de sous-noeuds», à la page 1393 pour créer un sous-noeud.

Pourquoi et quand exécuter cette tâche

Lorsque vous ajoutez une source de données à un sous-noeud, la page **Substitutions de configuration de sous-noeud** s'affiche si la source de données requiert une configuration. Elle présente les propriétés de configuration personnalisée et toutes les autres propriétés de configuration applicables au type de sous-noeud.

Procédure

- Dans la fenêtre **Substitutions de configuration de sous-noeud**, choisissez les propriétés de configuration souhaitées pour le sous-noeud au niveau de l'agent. Choisissez également les propriétés de configuration à varier pour chaque sous-noeud.
- Utilisez **Copier >>** pour copier les propriétés de configuration de sorte qu'elles soient situées au niveau de l'agent et du sous-noeud.

L'agent recherche d'abord une valeur au niveau du sous-noeud et, s'il ne trouve pas de valeur, il effectue une recherche au niveau de l'agent. Si une propriété située aux deux niveaux est une propriété obligatoire, celle-ci n'est requise qu'au niveau de l'agent et est toujours facultative au niveau du sous-noeud.

- Utilisez **Déplacer >>** pour déplacer des propriétés du niveau de l'agent au niveau du sous-noeud. La fonction **Déplacer>>** n'est pas admise pour les propriétés qui sont requises par une source de données de niveau agent ou par un sous-noeud d'un type différent.
- Utilisez **Supprimer** pour supprimer une des deux listes. Les propriétés ne peuvent être supprimées que si elles sont répertoriées au niveau de l'agent et au niveau du sous-noeud. Cette fonction ne permet pas de supprimer une propriété en intégralité.
- Utilisez **<< Copier** pour copier une propriété du sous-noeud vers le niveau de l'agent.
- Utilisez **<< Déplacer** pour déplacer une propriété du sous-noeud vers le niveau de l'agent.

Que faire ensuite

Vous pouvez modifier la configuration d'un sous-noeud existant à l'aide de l'éditeur d'agent.

Substitutions de configuration de sous-noeud

Utilisez les substitutions de configuration de sous-noeud pour remplacer les propriétés de configuration de l'agent par des propriétés spécifiques au sous-noeud.

La procédure (voir «Configuration d'un sous-noeud», à la page 1394) consiste à gérer la configuration de sous-noeud pour des propriétés automatiquement générées. La gestion des propriétés de configuration personnalisée est similaire. Toutes les propriétés de configuration personnalisée qui sont définies s'affichent dans la fenêtre **Substitutions de configuration de sous-noeud**.

Lors de la copie ou du déplacement d'une propriété personnalisée du niveau du sous-noeud vers le niveau de l'agent, vous êtes invité à indiquer la section dans laquelle placer la propriété. Vous pouvez sélectionner une section personnalisée existante ou entrer le nom d'une nouvelle section personnalisée.

Sélection des propriétés de configuration de sous-noeud

Sans les sous-noeuds, toutes les instances d'un type de source de données partagent les paramètres de configuration. Par exemple, tous les groupes d'attributs SNMP se connectent au même hôte à l'aide du même nom de communauté. Sans les sous-noeuds, chaque instance d'un sous-noeud est en mesure de se connecter à un hôte différent si la propriété SNMP_HOST est placée au niveau du sous-noeud.

La sélection des propriétés à substituer au niveau du sous-noeud est un critère important lors du développement d'un agent. Si un nombre excessif de propriétés est sélectionné, la section de configuration de sous-noeud devient encombrée et difficile à gérer. Si un trop petit nombre de propriétés est sélectionné, la fonctionnalité d'agent risque d'être limitée lorsqu'une personne souhaite varier d'un sous-noeud à l'autre une propriété.

Les propriétés suivantes ne peuvent pas être copiées au niveau du sous-noeud. (Tous les groupes d'attributs de tous les sous-noeuds et dans l'agent de base doivent utiliser la même version SNMP et le même type de connexion JMX) :

- Version SNMP
- Type de connexion de serveur MBean JMX
- Accueil Java
- Niveau de trace Java
- Arguments JVM
- Chemin d'accès aux classes pour les fichiers JAR externes
- Numéro du port de la source de données du socket
- Paramètres du chemin d'accès aux classes JMX ou JDBC

Configuration de sous-noeud avancée

Utilisez la configuration de sous-noeud avancée pour remplacer une propriété de configuration d'agent dans un sous-noeud.

Pourquoi et quand exécuter cette tâche

Les agents IBM Tivoli Monitoring version 6.2.1 et ultérieure sont dotés d'une option qui permet de remplacer les propriétés à partir de n'importe quelle section de configuration de niveau agent dans une instance de sous-noeud. La page **Substitutions de configuration de sous-noeud** contient une case à cocher intitulée **Autoriser le remplacement de toute propriété de configuration dans n'importe quel sous-noeud**. Pour plus d'informations, voir «Substitutions de configuration de sous-noeud», à la page 1395. Pour que cette option soit activée, vous devez sélectionner **6.2.1** comme **Version minimale d'ITM** lorsque vous renommez votre agent («Désignation et configuration de l'agent», à la page 1204). Si cette option est sélectionnée, chaque instance de sous-noeud peut remplacer toute propriété à partir d'une section de configuration de niveau agent. Mais ce remplacement peut être effectué uniquement à partir de l'interface graphique et non à partir de la ligne de commande **`itmcmd`**.

Procédure

L'option **Autoriser le remplacement de toute propriété de configuration dans n'importe quel sous-noeud** fait en sorte qu'une zone **Avancé** contenant une liste s'affiche dans chaque panneau de configuration de sous-noeud. La sélection initiale dans la zone **Avancé** fournit de brèves instructions : **Sélectionnez une section pour remplacer les valeurs**.

- Lorsque vous cliquez sur la liste, vous voyez une liste de toutes les sections autres que les sections de sous-noeud, qui contiennent des propriétés de configuration.
- Sélectionnez une section.

  Les propriétés de cette section sont ajoutées temporairement au panneau de sous-noeud. La valeur d'une propriété que vous modifiez s'ajoute à l'ensemble des propriétés définies pour le sous-noeud. Une source de données dans le sous-noeud recherche des valeurs de propriété dans le sous-noeud avant de consulter les sections au niveau de l'agent. .

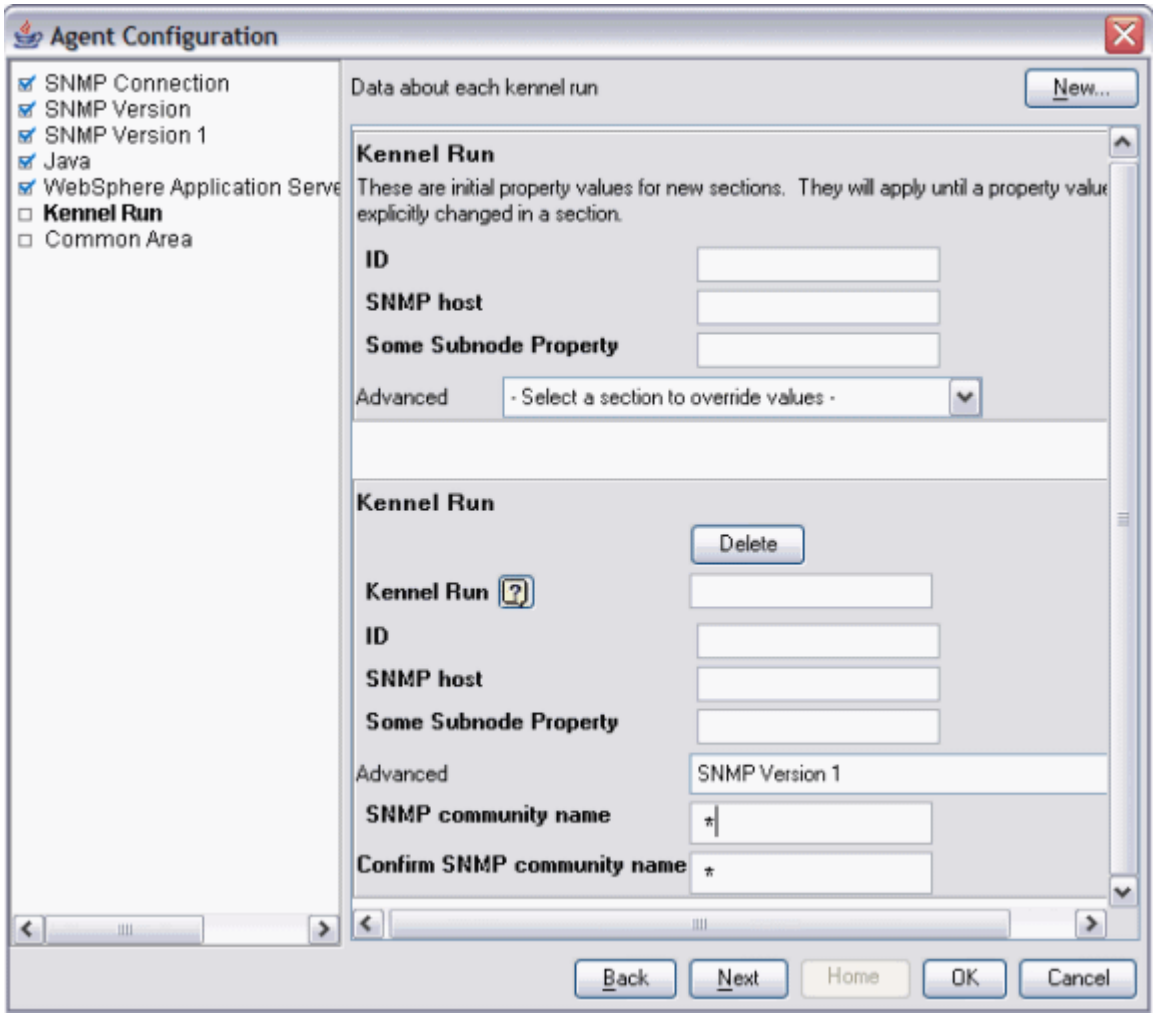


Figure 55. Propriétés SNMP version 1 développées

Les informations supplémentaires suivantes s'appliquent à la substitution de propriétés à partir des sections de niveau agent :

- Les propriétés copiées dans la section de sous-noeud ne s'affichent pas lorsque la section de niveau agent est sélectionnée dans la liste déroulante **Avancé**. Par exemple, dans la Figure 55, à la page 1397, l'**hôte SNMP** ne s'affiche pas sous la liste **Avancé** car il a été copié dans les propriétés de sous-noeud et est déjà affiché.
- Les sections qui ne contiennent aucune propriété à remplacer ne comportent pas de sélection dans la liste déroulante **Avancé**.
- Les valeurs remplacées que vous entrez pour une section sont conservées même si vous sélectionnez une autre section pour afficher des propriétés différentes.
- Sélectionnez **Autoriser le remplacement de toute propriété de configuration dans n'importe quel sous-noeud** pour activer cette fonction pour votre agent.

Configuration d'un sous-noeud à partir de la ligne de commande

Dans l'environnement IBM Tivoli Monitoring, vous pouvez également configurer un sous-noeud à partir de la ligne de commande.

Avant de commencer

Pour plus d'informations sur la configuration d'un sous-noeud, voir «Configuration de sous-noeud», à la page 1394.

Pourquoi et quand exécuter cette tâche

Procédure

- Pour configurer une instance de sous-noeud à partir de la ligne de commande, utilisez la commande suivante :

```
tacmd configureSystem -m HOSTNAME:00 -p
nom_section:id_instance_sous-noeud.nom_propriété=valeur
```

  Où :

  nom_section
  Identique au type de sous-noeud.

  id_instance_sous-noeud
  ID du sous-noeud défini pendant la configuration

  nom_propriété
  Nom de la propriété de configuration

  valeur
  Valeur de la propriété

Exemple de configuration de sous-noeud
Comment configurer un exemple d'agent avec un sous-noeud défini.

Exemple :

Cet exemple explique comment configurer un exemple d'agent qui a un seul sous-noeud intitulé Exemple de sous-noeud de type exs et les trois propriétés de configuration suivantes :

- `Agent Cfg` (le nom de propriété réel est `K00_AGENT_CFG`) est défini uniquement au niveau de l'agent.
- `Subnode Cfg` (le nom de propriété réel est `K00_SUBNODE_CFG`) est défini uniquement dans le sous-noeud de l'exemple.
- `Overridable Cfg` (le nom de propriété réel est `K00_OVERRIDABLE_CFG`) est défini au niveau de l'agent et a été copié dans l'exemple de sous-noeud.

La (Figure 56, à la page 1399) présente ces propriétés de configuration sur la page **Informations sur la configuration d'exécution** de l'éditeur d'agent.

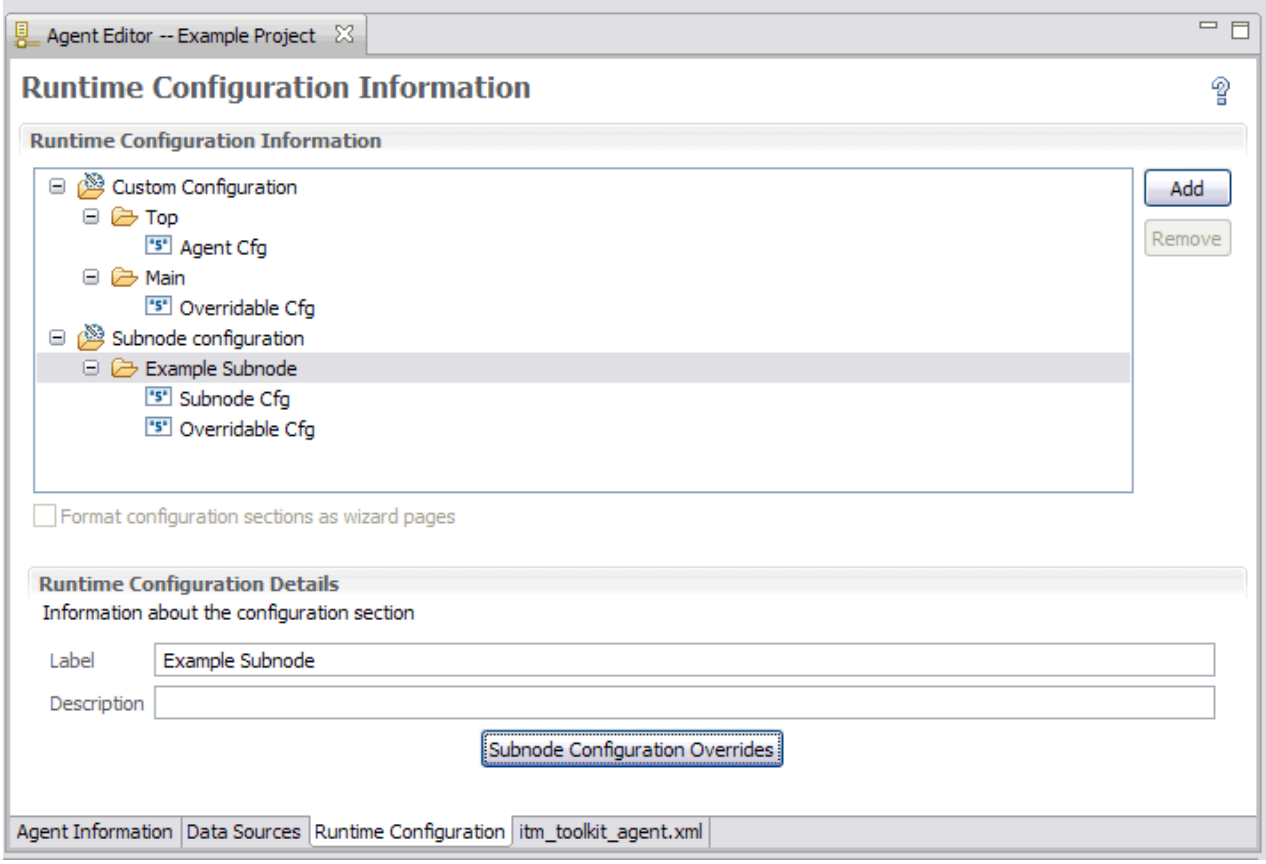


Figure 56. Définitions des propriétés de configuration d'Agent Builder

Lors de la configuration de cet exemple d'agent, la première page qui s'affiche est la section **Haut**, qui contient la propriété **Agent Cfg**, comme illustré dans la (Figure 57, à la page 1400). Dans la mesure où il s'agit d'une propriété de niveau agent, elle s'affiche une seule fois pendant la configuration d'agent. N'importe quelle instance de l'exemple de sous-noeud peut voir cette valeur de propriété, mais toutes les instances voient la même valeur.

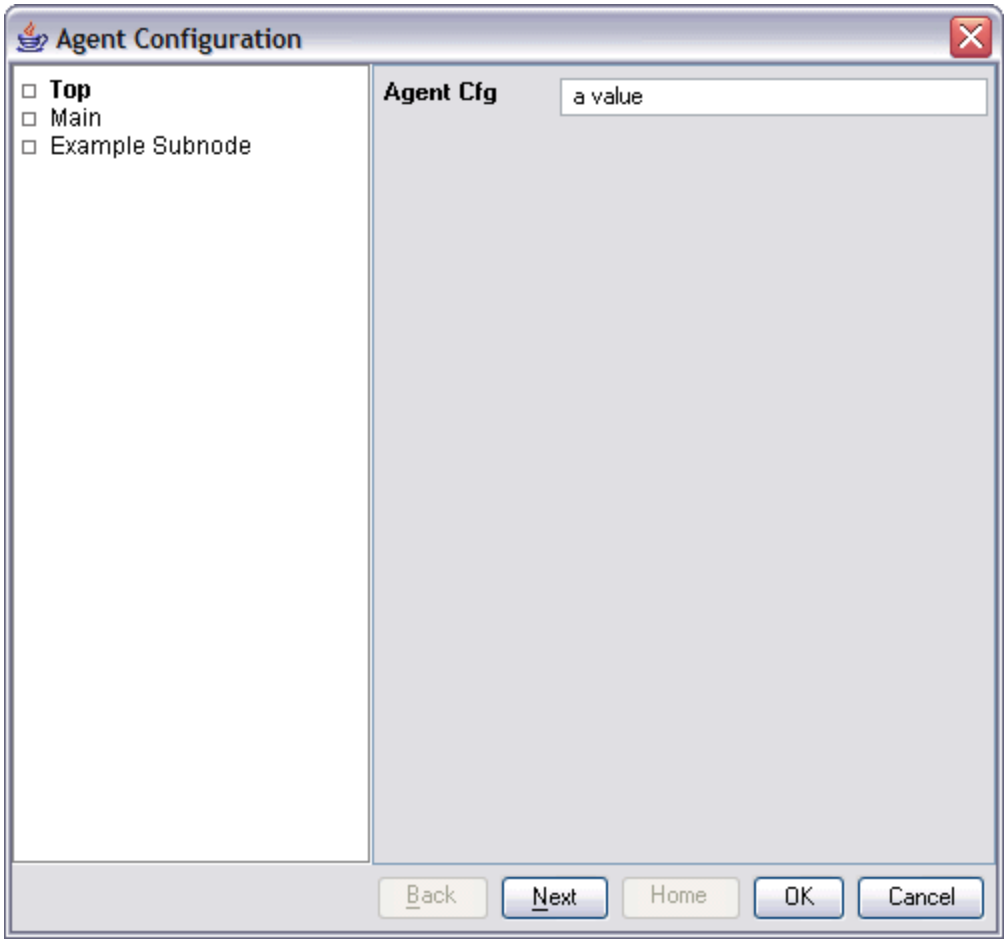


*Figure 57. Section **Haut** comportant la configuration de niveau agent pour la propriété **Agent Cfg***

Si vous effectuez la configuration à partir de la ligne de commande du serveur Tivoli Enterprise Monitoring Server, la propriété **Agent Cfg** peut être définie à l'aide de la commande suivante :

```
tacmd configureSystem -m HOSTNAME:00 -p "TOP.K00_AGENT_CFG=a value"
```

La section suivante qui s'affiche est la section **Principale**, comme illustré dans la Figure 58, à la page 1401. Il s'agit également d'une section de niveau agent qui contient la propriété **Overridable Cfg** de niveau agent. Cette propriété diffère de la propriété **Agent Cfg** car elle a été copiée dans l'exemple de sous-noeud dans Agent Builder. Cela signifie qu'une valeur par défaut pour la propriété peut être entrée dans la page **Principale**. Cependant, toutes les instances de l'exemple de sous-noeud peuvent remplacer la valeur entrée ici par une valeur différente.

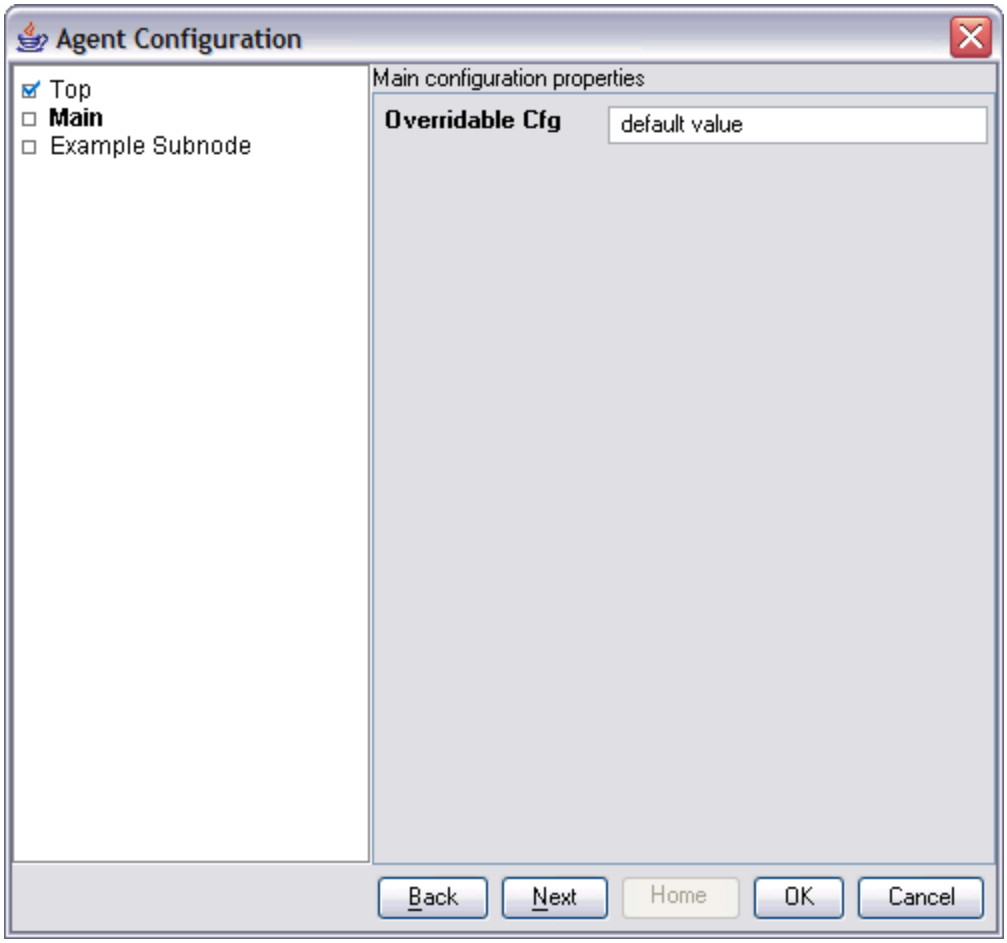


*Figure 58. Section **Principale** comportant la valeur par défaut de niveau agent pour la propriété **Overridable Cfg***

Si vous effectuez la configuration à partir de la ligne de commande du Tivoli Enterprise Monitoring Server, cette propriété peut être définie à l'aide de la commande suivante :

```
tacmd configureSystem -m HOSTNAME:00 -p "MAIN.K00_OVERRIDABLE_CFG=default value"
```

Vous pouvez placer ces deux propriétés dans la même section de niveau agent. Vous pouvez choisir le nombre de sections de niveau agent personnalisées à créer et le mode de distribution des propriétés personnalisées entre elles.

La section suivante qui s'affiche est la section **Exemple de sous-noeud**, comme illustré dans la Figure 59, à la page 1402. Dans la mesure où il s'agit de la première configuration de l'agent, aucune instance de sous-noeud n'est définie et aucune sous-section d'instance de sous-noeud n'est affichée. La sous-section des valeurs de propriétés initiales est affichée, même si elle est facultative et que certains types de sous-noeud risquent de ne pas l'afficher. Comme la sous-section des valeurs de propriété initiales est affichée, des valeurs par défaut peuvent être entrées pour n'importe laquelle des propriétés de configuration. La propriété **Overridable Cfg** comporte déjà une valeur par défaut obtenue de la propriété de niveau agent du même nom.

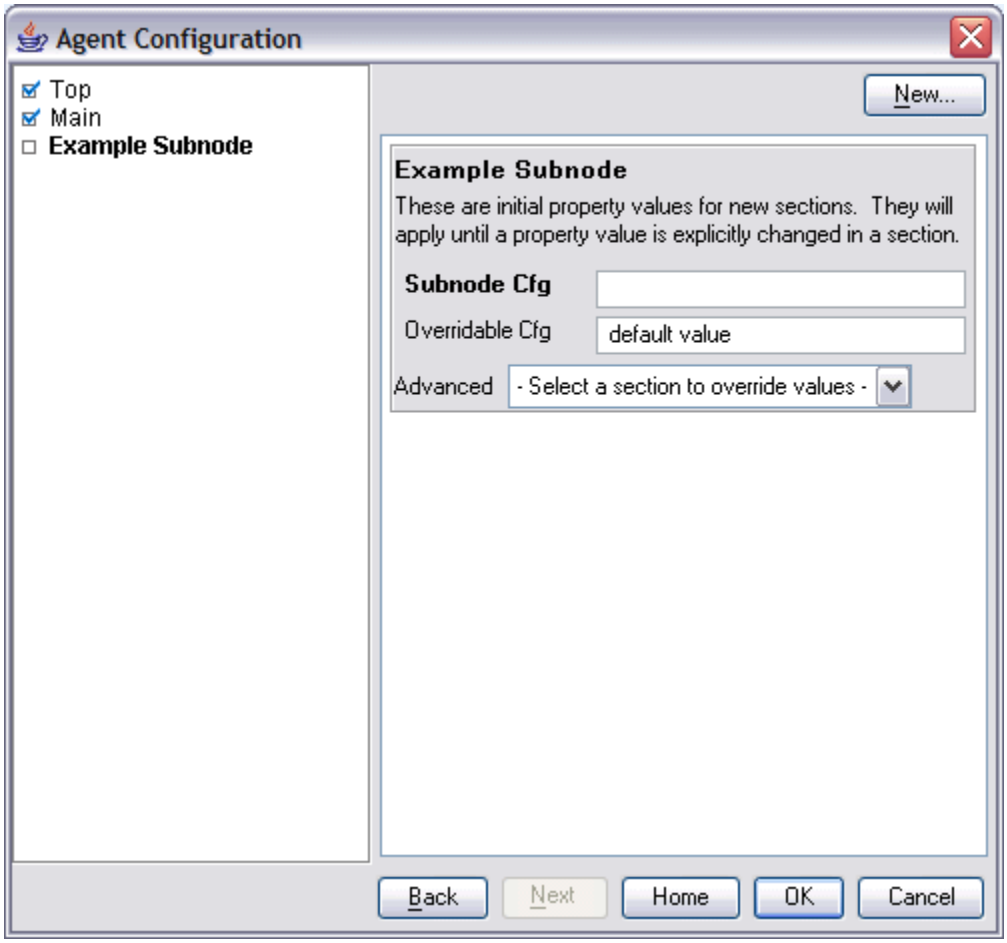


*Figure 59. Page de la section **Exemple de sous-noeud** ne comportant aucun sous-noeud*

Des instances de sous-noeud sont définies à l'aide des actions suivantes dans la page de la section **Exemple de sous-noeud** vide (Figure 60, à la page 1403) :

1. Dans la section **Exemple de sous-noeud** initiale, dans la zone **Subnode Cfg**, entrez la chaîne par défaut suivante pour la propriété : `sub-default value`.
2. Cliquez sur **Nouveau**. Une première sous-section **Exemple de sous-noeud** s'affiche sous la sous-section des propriétés initiales.
3. Dans la zone **Exemple de sous-noeud**, entrez l'ID instance de sous-noeud suivant : do.
4. Cliquez sur **Nouveau**. Une seconde sous-section **Exemple de sous-noeud** apparaît sous la première.
5. Dans la seconde zone **Exemple de sous-noeud**, entrez l'ID instance de sous-noeud suivant : `re`.
6. Dans la zone **Subnode Cfg**, entrez la valeur suivante pour la propriété **Subnode Cfg** : `sc override`.
7. Dans la zone **Overridable Cfg**, entrez la valeur suivante pour la propriété **Overridable Cfg** : `oc override`.

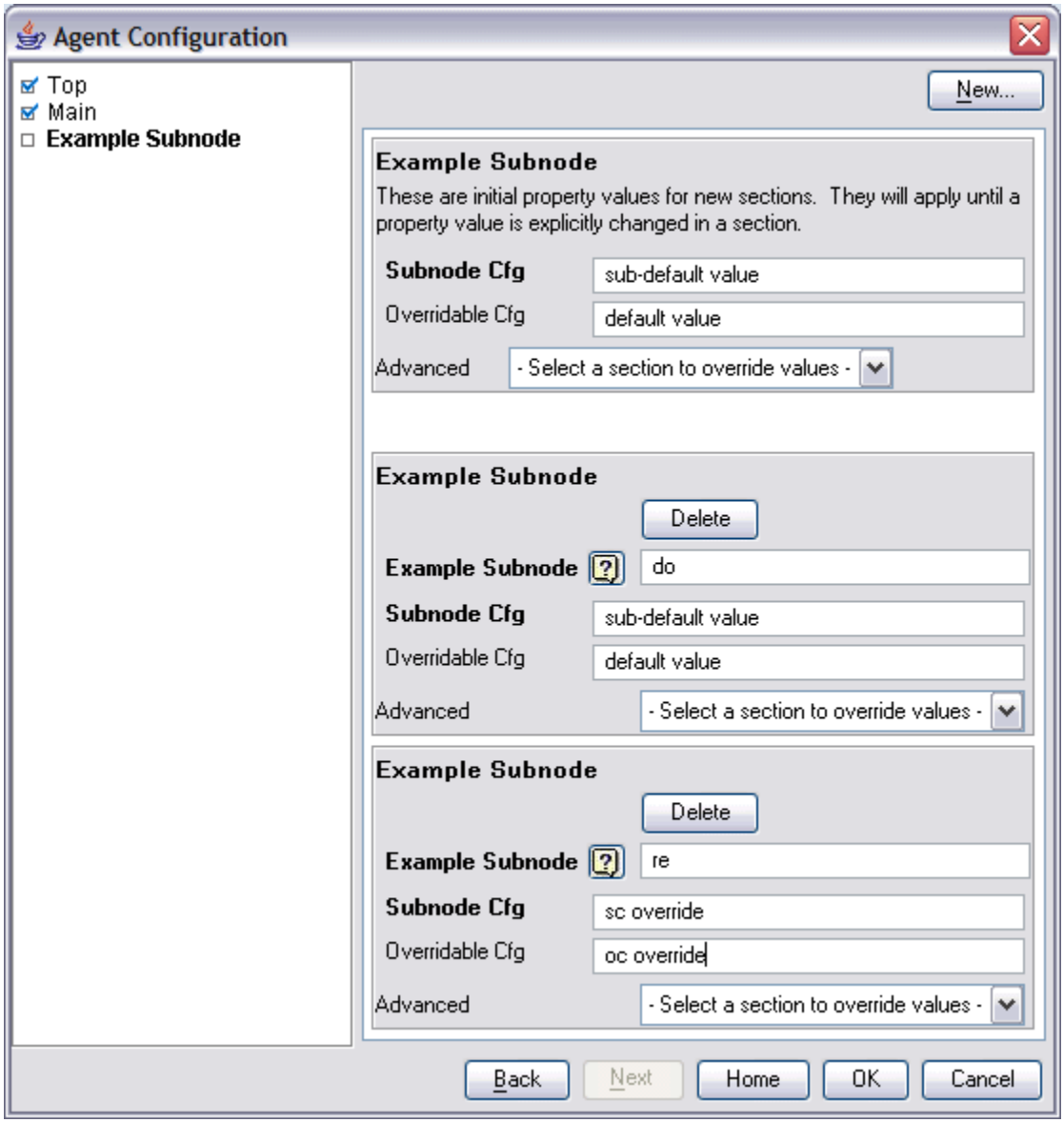


*Figure 60. Page de la section **Exemple de sous-noeud** dans laquelle deux instances de sous-noeud sont définies*

Les deux nouvelles sous-sections permettent à l'agent de créer deux instances de sous-noeud lors de son démarrage. Dans la mesure où les propriétés de la sous-section de sous-noeud **do** n'ont pas été modifiées, les valeurs de propriété par défaut sont utilisées par cette instance de sous-noeud. Etant donné que des valeurs différentes ont été entrées pour les propriétés dans la sous-section **re**, l'instance de sous-noeud **re** utilise les valeurs qui ont été entrées.

Vous pouvez définir une valeur par défaut à partir de la ligne de commande du Tivoli Enterprise Monitoring Server, à l'aide de la commande suivante :

```
tacmd configureSystem -m HOSTNAME:00 -p "exs.K00_SUBNODE_CFG=sub-default value"
```

Le format de définition des valeurs par défaut des sous-noeuds est exactement identique au format de définition des propriétés de niveau agent, à ceci près que le nom de section identifie une section de sous-noeud.

Vous pouvez créer les instances de sous-noeud à partir de la ligne de commande du Tivoli Enterprise Monitoring Server, à l'aide de la commande suivante :

```
tacmd configureSystem -m HOSTNAME:00 -p "exs:do.K00_OVERRIDABLE_CFG=default value" \
 "exs:re.K00_SUBNODE_CFG=sc override" "exs:re.K00_OVERRIDABLE_CFG=oc override"
```

L'ID instance de sous-noeud est inséré entre le nom de section et le nom de propriété. Lors de l'utilisation de la ligne de commande pour créer une instance de sous-noeud, indiquez au moins une propriété, même si toutes les propriétés utilisent des valeurs par défaut. En outre, il n'est pas nécessaire d'indiquer des valeurs par défaut sur la ligne de commande lors de la définition des instances de sous-noeud.

Toutes les propriétés de configuration d'agent peuvent être définies dans une commande unique. La commande suivante est équivalente à toutes les commandes individuelles précédentes :

```
tacmd configureSystem -m HOSTNAME:00 -p "TOP.K00_AGENT_CFG=a value" \
 "MAIN.K00_OVERRIDABLE_CFG=default value" \
 "exs.K00_SUBNODE_CFG=sub-default value" \
 "exs:do.K00_OVERRIDABLE_CFG=default value" \
 "exs:re.K00_SUBNODE_CFG=sc override" "exs:re.K00_OVERRIDABLE_CFG=oc override"
```

Sous-noeuds et sources de données Windows
Choisissez d'inclure les propriétés de connexion distante Windows dans l'agent ou non.

Pourquoi et quand exécuter cette tâche

Si un agent comporte des sources de données Windows uniquement au niveau de l'agent et non dans les sous-noeuds, l'inclusion des propriétés de configuration de connexion distante Windows dans l'agent est facultative. Les sources de données Windows sont le journal des événements Windows, Windows Management Instrumentation et l'Analyseur de performances Windows. Si elles ne sont pas incluses, ces sources de données surveillent par défaut le système Windows local et ne nécessitent pas de configuration. Par défaut, aucune source de données Windows n'est incluse dans aucun sous-noeud.

Pour choisir si les propriétés de connexion distante Windows doivent ou non être incluses dans l'agent, procédez comme suit :

Procédure

1. Sur la page **Informations sur Windows Management Instrumentation (WMI)**, cliquez sur **Options globales** lors de l'affichage des propriétés de source de données. Sélectionnez **Options globales** pendant la création de la source de données ou à partir de la page **Sources de données** de l'éditeur d'agent.
2. Dans la fenêtre **Options de source de données Windows globales**, sélectionnez **Inclure la configuration des connexions distantes Windows** si vous voulez inclure ces propriétés dans l'agent.

Sous-noeuds et sources de données de script
Les propriétés de configuration d'instance de sous-noeud sont accessibles dans les scripts de sous-noeud tout comme dans les scripts de niveau agent.

Les scripts ont accès à toutes les propriétés de configuration de niveau agent et à toutes les propriétés de configuration d'instance de sous-noeud. Si une propriété de niveau agent est remplacée au niveau du sous-noeud, le script n'a accès qu'à la valeur de propriété de niveau sous-noeud.

Personnalisation de la configuration de l'agent

Personnalisez la configuration des sources de données de processus, de fichier journal et de script.

Avant de commencer

Si vous ajoutez des sources de données SNMP, JMX, CIM, JDBC, HTTP et SOAP à votre agent, vous pouvez les configurer comme décrit dans les sections suivantes :

- «Surveillance de données à partir d'un serveur SNMP (Simple Network Management Protocol)», à la page 1266
- «Surveillance de beans gérés (MBeans) JMX (Java Management Extensions)», à la page 1277
- «Surveillance de données à partir d'un modèle CIM (Common Information Model)», à la page 1296
- «Surveillance de données à partir de JDBC (Java Database Connectivity)», à la page 1325
- «Surveillance de la disponibilité et du temps de réponse HTTP», à la page 1336
- «Surveillance des données à partir d'une source de données SOAP ou d'une autre source de données HTTP», à la page 1344

Pourquoi et quand exécuter cette tâche

Effectuez cette tâche pour personnaliser la configuration des sources de données de processus, de fichier journal et de script, de sorte qu'un agent puisse accéder à l'application qu'il surveille.

Tous les agents doivent être configurés pour pouvoir être démarrés. Tous les agents doivent posséder des informations de configuration de base, telles que la méthode de connexion au serveur Tivoli Enterprise Monitoring Server. En général, un agent doit posséder des informations de configuration supplémentaires afin d'accéder aux informations spécifiques au système sur lequel il est en cours d'exécution. Par exemple, si vous devez connaître l'emplacement d'installation d'un produit logiciel, ajoutez des propriétés de configuration pour demander ces informations. Vous pouvez également demander l'ID utilisateur et le mot de passe pour accéder à une interface.

La configuration personnalisée est définie par le développeur d'agent. Elle n'est pas requise pour tous les agents, mais elle peut être utilisée dans les domaines suivants de la collecte de données :

- Mise en correspondance d'un argument dans un contrôleur de processus
- Mise en correspondance de la ligne de commande dans un contrôleur de processus
- Composition d'un chemin ou non de fichier journal
- Définition d'une variable d'environnement dans un script

Remarque : Certains fournisseurs de données tels que JMX et SNMP ajoutent automatiquement cette configuration.

Remarque : Lorsque l'Agent Builder ajoute la configuration spécifique à un fournisseur de données, cette configuration est ajoutée uniquement en Anglais.

Lors de la définition de la source de données, si votre agent requiert des informations spécifiques au système pour une zone de la collecte de données, l'option **Insérer une propriété** ou **Insérer une propriété de configuration** apparaît.

Par exemple, lorsque vous créez un groupe d'attributs surveillant un fichier journal, l'option **Insérer une propriété de configuration** apparaît.

Procédure

1. Cliquez sur **Insérer une propriété de configuration** pour afficher la fenêtre **Propriétés de configuration**.
2. Dans la fenêtre **Propriétés de configuration**, cliquez sur une propriété, puis cliquez sur **Ajouter**.

   Remarque : A l'origine, aucune propriété de configuration n'est définie pour l'agent.
3. Dans la fenêtre **Propriété de configuration d'exécution**, complétez les zones suivantes :
   a) Dans la zone **Section**, complétez les zones suivantes :

      Libellé
      Texte décrivant les propriétés

      Description
      Description des propriétés (facultatif)
   b) Dans la zone **Propriété**, complétez les zones suivantes :

Libellé
Texte affiché dans le panneau de configuration d'agent, identifiant les informations à saisir.

Variable d'environnement
La variable d'environnement est affichée dans la zone **Variable d'environnement** et est mise à jour lorsque vous renseignez la zone de libellé. Agent Builder construit automatiquement le nom de la variable d'environnement à partir du code produit et du libellé. Si vous souhaitez modifier la variable d'environnement indépendamment du libellé, vous pouvez décocher la case **Faire correspondre le libellé**.

Description
(facultatif) Description de la propriété à définir.

Type
Type d'informations collectées, à savoir l'une des options suivantes :

Chaîne
Pour toutes les informations alphabétiques à collecter (par exemple, emplacements d'installation, noms d'utilisateur et noms d'hôtes).

Mot de passe
Pour toutes les informations devant être chiffrées lorsqu'elles sont stockées. Outre la fourniture d'un chiffrement des données, les données saisies dans la zone de texte sont masquées par des astérisques. De plus, vous êtes invité à entrer ces informations deux fois pour valider les données.

Numérique
Pour toutes les informations numériques (par exemple, numéros de port).

Choix
Pour une liste de valeurs spécifiques. Cette option permet d'activer la table Choix. Vous pouvez définir des valeurs spécifiques en cliquant sur **Ajouter**. Les valeurs entrées s'affichent dans le panneau de configuration d'agent en tant que groupe de sélections, à partir duquel vous ne pouvez effectuer qu'une seule sélection.

Texte en lecture seule
Affiche du texte lors de la configuration de l'agent, mais aucune information n'est collectée.

Séparateur
Affiche un séparateur horizontal, mais aucune information n'est collectée.

Afficheur de fichiers
Collecte une chaîne correspondant à un nom de fichier. Cliquez sur **Parcourir** pour parcourir le système de fichiers pour rechercher le fichier souhaité.

Valeur par défaut
(Facultatif) Spécifiez la valeur affichée dans le panneau de configuration au moment de l'exécution lorsque l'agent est configuré pour la première fois. Si vous souhaitez que la valeur par défaut pour UNIX/Linux soit différente de la valeur par défaut pour Windows, cliquez sur **Plusieurs valeurs**.

Dans la fenêtre **Valeurs par défaut de la propriété de configuration**, indiquez les valeurs par défaut souhaitées pour les systèmes Windows et pour les systèmes UNIX et Linux.

Remarque : La prise en charge de plusieurs valeurs par défaut est une fonction qui n'est supportée que dans IBM Tivoli Monitoring version 6.2.1 et ultérieure. Si votre agent est compatible avec IBM Tivoli Monitoring V6.2, une invite vous informe de cette exigence et vous pouvez annuler ou continuer avec la compatibilité V6.2.1 activée.

Obligatoire
Cochez cette zone si l'utilisateur doit entrer une valeur lorsque l'agent est configuré. Désélectionnez cette zone si elle est facultative pour permettre à l'utilisateur d'entrer une valeur.

c) Pour ajouter un choix, cliquez sur **Ajouter**

4. Dans la fenêtre **Valeur de la propriété de configuration**, renseignez les zones **Libellé** et **Valeur**.

Le libellé s'affiche sous la forme d'un des choix. S'il est sélectionné, la valeur devient celle de la propriété.

5. Cliquez sur **OK**.

   La nouvelle propriété de configuration et la nouvelle section de configuration s'affichent dans la fenêtre **Propriétés de configuration** sous **Configuration personnalisée**.
6. Facultatif : Pour ajouter une autre propriété dans une section existante, sélectionnez la section ou une propriété existante dans la section, puis cliquez sur **Ajouter**. Vous effectuez la sélection de l'arborescence de configuration d'exécution de la fenêtre **Propriétés de configuration**.
7. Complétez les zones de la nouvelle propriété (zones identiques à celles de l'étape «3», à la page 1405).
8. Cliquez sur **OK**. La dernière propriété ajoutée est sélectionnée.
9. Conservez la sélection ou sélectionnez la propriété que vous voulez insérer dans le nom de fichier journal.
10. Cliquez sur **OK**. La propriété est insérée dans le nom de fichier journal.

    Vous pouvez ensuite continuer l'assistant pour terminer la définition de votre groupe d'attributs de fichier journal.

    Remarque : Même si une propriété de configuration est définie dans le contexte d'un nom de fichier journal, elle peut être utilisée dans d'autres emplacements. Par exemple, une source de données de script est un emplacement qui accepte une propriété de configuration. Cette souplesse signifie que vous pouvez accéder à la valeur de l'élément de configuration **Informations sur le fichier** à l'aide de la variable de script *$K00_APPLICATION_LOG_FILE* si le code produit est K00. Vous pouvez également utiliser la variable de fichier de traitement par lots Windows *%K00_APPLICATION_LOG_FILE%*.

Modification des propriétés de configuration à l'aide de l'éditeur d'agent

Utilisez l'éditeur d'agent pour modifier les propriétés de configuration de votre agent.

Pourquoi et quand exécuter cette tâche

Cette tâche fournit des informations sur l'affichage, l'ajout et la modification des propriétés de configuration à l'aide de l'éditeur d'agent.

Procédure

1. Cliquez sur l'onglet **Configuration d'exécution**.
2. Sélectionnez une section de configuration, puis cliquez sur **Ajouter**.

   Le bouton **Ajouter** fonctionne de la manière indiquée à la rubrique «Personnalisation de la configuration de l'agent», à la page 1404. Il n'existe aucune option **Modifier**, car une section ou une propriété de configuration est modifiée sur cette page lorsqu'elle est sélectionnée.
3. Sélectionnez une propriété de configuration pour afficher la zone **Détails de la configuration d'exécution**.
4. Dans la zone **Détails de la configuration d'exécution**, modifiez les zones pour configurer la propriété.

Configuration d'une connexion distante Windows

Informations sur la configuration d'une connexion distante Windows

Pourquoi et quand exécuter cette tâche

Windows Management Instrumentation (WMI), l'Analyseur de performances Windows (Perfmon) et les sources de données du journal des événements Windows peuvent surveiller des données sur le système sur lequel l'agent est installé. Ces sources de données peuvent également surveiller des données sur les systèmes Windows distants. Ces trois types de source de données sont appelés sources de données Windows. Si ces sources de données Windows surveillent les données à distance, elles partagent toutes

les propriétés de configuration des connexions distantes Windows pour le niveau d'agent sur lequel elles sont définies.

Si vous définissez une source de données Windows dans le niveau de base de votre agent, les propriétés de configuration des connexions distantes Windows ne sont pas automatiquement ajoutées à l'agent. Elles ne sont pas ajoutées afin de conserver la compatibilité avec les versions d'agents antérieures qui pourraient utiliser le fournisseur de données Windows avant l'activation de la surveillance à distance. La source de données Windows de votre agent surveille des données sur le système Windows local sur lequel l'agent est installé.

Si vous définissez une source de données Windows dans un sous-noeud de votre agent, les propriétés de configuration des connexions distantes Windows s'ajoutent automatiquement à l'agent. La source de données Windows doit prendre en charge la connexion distante Windows si elle se trouve dans un sous-noeud. Vous ne pouvez pas désélectionner l'option tant que toutes les sources de données Windows ne sont pas supprimées de l'ensemble des sous-noeuds de l'agent. Il se peut que chaque instance d'un sous-noeud soit configuré pour surveiller un système Windows distant différent. Toutes les sources de données Windows du sous-noeud partagent les mêmes propriétés de configuration des connexions distantes Windows.

Pour configurer un agent de base de sorte qu'il surveille à distance un système Windows distant unique, procédez comme suit.

Procédure

1. Dans la fenêtre **Définition de la source de données** de l'éditeur d'agent, cliquez sur **Options globales**.
   La fenêtre **Options de source de données Windows globales** s'ouvre.
2. Sélectionnez **Inclure la configuration des connexions distantes Windows**.
3. Cliquez sur **OK**.

Résultats

Vous pouvez accéder aux propriétés de configuration suivantes, spécifiques aux connexions, dans la page **Informations sur la configuration d'exécution** de l'éditeur d'agent en sélectionnant **Configuration de l'accès distant Windows** > **Connexion distante Windows**.

Hôte Windows distant
Nom d'hôte de l'ordinateur Windows distant

Mot de passe Windows distant
Mot de passe pour Windows distant

`Nom d'utilisateur\DOMAIN` Windows distant
Nom d'utilisateur de l'hôte Windows distant

Que faire ensuite

Vous pouvez visualiser, ajouter et modifier les propriétés de configuration à l'aide de l'éditeur d'agent. Pour plus d'informations, voir «Modification des propriétés de configuration à l'aide de l'éditeur d'agent», à la page 1407. Si une source de données Windows est définie dans un sous-noeud, vous pouvez également indiquer des substitutions de configuration de sous-noeud. Pour obtenir des instructions, voir «Configuration de sous-noeud», à la page 1394.

Création d'un utilisateur avec les droits Windows Management Instrumentation (WMI)

Vous pouvez ajouter et configurer un utilisateur sur un système Windows avec les droits nécessaires pour parcourir les données WMI.

Pourquoi et quand exécuter cette tâche

Si votre agent collecte des données à partir d'un système distant à l'aide de Windows Management Instrumentation (WMI), il a besoin des droits d'accès aux données WMI sur le système distant. L'agent peut accéder aux données WMI sur un système distant si vous fournissez les données d'identification

d'un compte doté des droits d'accès aux données WMI sur le système. La procédure s'applique à Windows 7, Windows 2008 Server et Windows Vista.

Remarque : Votre agent peut également accéder aux données sur un système Windows distant à l'aide des sources de données de Windows Performance Monitor (Perfmon) et Windows Event Log. Cependant, dans le cas des sources de données Windows Performance Monitor (Perfmon) et Windows Event Log, vous devez fournir des données d'identification en tant qu'administrateur pour le système distant.

Procédure

1. Créez un compte utilisateur :
   a. Accédez à Windows **Démarrer** > **Outils d'administration** > **Gestion de l'ordinateur**. La fenêtre **Gestion de l'ordinateur** s'ouvre.
   b. Développez **Utilisateurs et groupes locaux**.
   c. Cliquez avec le bouton droit de la souris sur le dossier **Utilisateurs** et sélectionnez **Nouvel utilisateur**.
   d. Complétez les détails de l'utilisateur et cliquez sur **Créer** puis **Fermer**.
2. Configurez l'appartenance à un groupe pour le nouveau compte utilisateur :
   a. Dans la fenêtre **Gestion de l'ordinateur**, sélectionnez le dossier **Utilisateurs**.
   b. Cliquez avec le bouton droit de la souris sur le nouveau compte utilisateur, puis sélectionnez **Propriétés**.
   c. Cliquez sur l'onglet **Appartient à**.
   d. Cliquez sur **Ajouter**.
   e. Cliquez sur **Avancé**.
   f. Cliquez sur **Rechercher maintenant**.
   g. Sélectionnez les groupes suivants :
      - Utilisateurs de COM distribué
      - Utilisateurs du journal de performances
      - Utilisateurs distants

      Conseil : Appuyez sur la touche Ctrl tout en cliquant pour sélectionner plusieurs groupes.
   h. Cliquez sur **OK** jusqu'à ce que vous retourniez à la fenêtre **Gestion de l'ordinateur**.
   i. Sélectionnez **Fichier** > **Quitter** pour quitter la fenêtre **Gestion de l'ordinateur**.
3. Affectez les droits DCOM (Distributed Component Object Model) :
   a. Accédez à Windows **Démarrer** > **Outils d'administration** > **Services de composants**. La fenêtre **Services de composants** s'ouvre.
   b. Développez **Services de composants** > **Ordinateurs** > **Poste de travail**.
   c. Cliquez avec le bouton droit sur **Poste de travail** et sélectionnez **Propriétés**. La fenêtre **Propriétés de : Poste de travail** s'ouvre.
   d. Cliquez sur l'onglet **sécurité COM**.
   e. Dans la zone **Droits d'accès**, cliquez sur **Modifier les limites**.
   f. Dans **Utilisateurs COM distribués**, vérifiez que **Accès local** et **Accès distant** sont sélectionnés.
   g. Cliquez sur **OK** pour sauvegarder les paramètres.
   h. Dans la fenêtre **Propriétés de : Poste de travail**, section **Autorisations d'exécution et d'activation**, cliquez sur **Modifier les limites**.
   i. Dans **Utilisateurs COM distribués**, vérifiez que **Exécution locale**, **Exécution à distance**, **Activation locale** et **Activation à distance** sont sélectionnés.
   j. Cliquez sur **OK** pour sauvegarder les réglages et cliquez à nouveau sur **OK** pour fermer la fenêtre **Propriétés de : Poste de travail**.

k. Sélectionnez **Fichier** > **Quitter** pour quitter la fenêtre **Services de composants**.

4. Configurez les affectations de sécurité des espaces de nom WMI

a. Accédez à Windows **Démarrer** > **Exécuter**.

b. Entrez `wmimgmt.msc` et cliquez sur **OK**.

c. Cliquez avec le bouton droit de la souris sur **Contrôle WMI (local)** et sélectionnez **Propriétés**.

d. Cliquez sur l'onglet **Sécurité**.

e. Cliquez sur **Sécurité**.

f. Cliquez sur **Ajouter**.

g. Cliquez sur **Avancé**.

h. Cliquez sur **Rechercher maintenant**.

i. Sélectionnez le nouveau compte utilisateur, puis cliquez sur **OK** jusqu'à ce que vous retourniez à la fenêtre **sécurité pour Root**.

j. Cliquez sur **Avancé** et sélectionnez le compte utilisateur nouvellement créé.

k. Cliquez sur **Editer**.

l. A partir du menu de sélection **Appliquer à :**, sélectionnez **Cet espace de noms et les sous-espaces de noms**.

m. Dans **Méthodes d'exécution**, vérifiez que les cases **Activer le compte**, **Appel à distance autorisé** et **Sécurité de lecture** sont cochées.

n. Cliquez sur **OK** jusqu'à ce que vous retourniez à la fenêtre **wmimgmt**.

o. Sélectionnez **Fichier** > **Quitter** pour quitter la fenêtre **wmimgmt**.

Que faire ensuite

Pour plus d'informations sur la collecte de données WMI à partir d'un système distant, voir «Surveillance de données à partir de Windows Management Instrumentation (WMI)», à la page 1261.

Configuration d'une connexion distante SSH (Secure Shell)

Informations sur la configuration d'une connexion distante SSH

Pourquoi et quand exécuter cette tâche

Les sources de données de script peuvent surveiller des données sur le système sur lequel l'agent est installé, mais aussi sur les systèmes distants. Si ces sources de données de script surveillent les données à distance, elles partagent toutes les mêmes propriétés de configuration des connexions distantes SSH pour le niveau d'agent sur lequel elles sont définies. Les versions antérieures d'un agent peuvent utiliser le fournisseur de données de script avant l'activation de la surveillance à distance. Afin de conserver la compatibilité avec de précédentes versions d'agents, les propriétés de configuration des connexions distantes SSH ne sont pas automatiquement ajoutées à l'agent. La source de données de script de votre agent surveille des données sur le système local sur lequel l'agent est installé.

Si vous définissez une source de données de script dans un sous-noeud et que vous sélectionnez **Activer la collecte de données via SSH**, vous pouvez configurer chaque instance de sous-noeud pour surveiller un système distant différent. Toutes les sources de données de script du sous-noeud partagent les mêmes propriétés de configuration des connexions distantes SSH.

Si vous souhaitez que l'agent surveille à distance un système distant, procédez comme suit.

Procédure

Dans la fenêtre **Définition de la source de données** d'éditeur d'agent associée à la source de données de script, sélectionnez **Activer la collecte de données via SSH**.

Résultats

Vous pouvez accéder aux propriétés de configuration suivantes, spécifiques aux connexions, dans la page **Informations sur la configuration d'exécution** de l'**Editeur d'agent** en sélectionnant **Configuration de Secure Shell (SSH)** > **Connexion distante SSH**.

Adresse réseau
Adresse IP ou nom d'hôte de l'ordinateur distant.

Numéro de port SSH
Numéro du port IP sur lequel le serveur SSH s'exécute. La valeur par défaut est 22.

Type d'authentification
Type d'authentification à utiliser pour vous connecter au serveur SSH distant. Vous pouvez choisir Mot de passe ou Clé publique.

Déconnexion du système distant après chaque intervalle de collecte
Option permettant de déterminer si le fournisseur de données de script supprime la session de connexion au système distant après la collecte de données. Par défaut, la valeur est Non.

Suppression du script du système distant après chaque intervalle de collecte
Option permettant de supprimer le script du système distant après chaque intervalle de collecte de données. Par défaut, la valeur est Non.

Si le type d'authentification sélectionné est Password, vous pouvez accéder aux propriétés de configuration suivantes dans la page **Informations sur la configuration d'exécution** de l'**Editeur d'agent** en sélectionnant **Configuration de Secure Shell (SSH)** > **Password** :

Nom d'utilisateur
Nom d'utilisateur pour le système distant

Mot de passe
Mot de passe pour le système distant

Si le type d'authentification sélectionné est Clé publique, vous pouvez accéder aux propriétés de configuration suivantes dans la page **Informations sur la configuration d'exécution** de l'**Editeur d'agent** en sélectionnant **Configuration de Secure Shell (SSH)** > **Clé publique** :

Nom d'utilisateur
Nom d'utilisateur associé au fichier de clés publiques

Fichier de clés publiques
Fichier de clés publiques associé à l'utilisateur

Fichier de clés privées
Fichier de clés privées associé à l'utilisateur

Mot de passe
Mot de passe utilisé pour déverrouiller le fichier de clés privées

Que faire ensuite

Vous pouvez visualiser, ajouter et modifier les propriétés de configuration à l'aide de l'éditeur d'agent. Pour obtenir des instructions, voir «Modification des propriétés de configuration à l'aide de l'éditeur d'agent», à la page 1407. Si les propriétés de configuration des connexions distantes SSH sont incluses dans un sous-noeud, vous pouvez également indiquer des substitutions de configuration de sous-noeud. Pour obtenir des instructions, voir «Configuration de sous-noeud», à la page 1394.

Création d'espaces de travail, de commandes Action et de situations

Après avoir installé un agent dans un environnement IBM Tivoli Monitoring, vous pouvez créer des espaces de travail, des requêtes, des commandes Action et des situations pour votre solution de surveillance.

Les situations, les espaces de travail, les commandes Action et les requêtes que vous créez peuvent être inclus dans le module d'installation. Pour avoir une image d'installation pour les situations, les espaces de

travail, ainsi que pour l'agent lui-même, les fichiers de situation et d'espace de travail doivent se trouver dans le même projet que l'agent. Agent Builder fournit un assistant pour créer les fichiers appropriés dans le projet d'agent. Pour plus d'informations sur l'importation des fichiers de prise en charge de l'application, voir «Importation des fichiers de prise en charge de l'application», à la page 1447.

Création de situations, de commandes Action et de requêtes

Recherchez des informations pour vous aider à créer des situations, des commandes Action et des requêtes.

Pour créer des situations, des commandes Action et des requêtes, utilisez le client Tivoli Enterprise Portal et l'éditeur de situations intégré. Pour obtenir des informations détaillées sur la procédure de création de situations, voir le manuel Tivoli Enterprise Portal User's Guide. Vous pouvez également utiliser la documentation d'aide qui est installée avec Tivoli Enterprise Portal Server. Un agent de surveillance Agent Builder peut reconnaître et exécuter un traitement spécial pour un ensemble de commandes Action spécifiques. Pour plus d'informations sur les commandes spéciales Action, voir «Guide de référence des commandes Action», à la page 1551.

Les situations des agents de surveillance système ne sont pas créées de la même façon que les situations d'entreprise, créées à l'aide de l'éditeur de situations Tivoli Enterprise Portal ou de la commande **tacmd createSit**. Pour les agents Tivoli System Monitor, des situations privées sont créées en local dans un fichier XML de configuration de situation privée pour l'agent. Pour plus d'informations sur la création de situations pour des agents Tivoli System Monitor, voir "Situations privées" dans le chapitre "Autonomie d'agent" du document *IBM Tivoli - Guide d'administration*.

Création d'espaces de travail

Placez Tivoli Enterprise Portal en mode Administrateur pour créer des espaces de travail à exporter et à inclure dans votre solution.

Pourquoi et quand exécuter cette tâche

Créez les espaces de travail dans l'environnement dans lequel ils sont utilisés. Lorsque vous générez des espaces de travail, vous devez modifier les paramètres d'affichage de votre ordinateur pour créer les espaces de travail avec la résolution minimale normalement utilisée dans votre environnement. La mise en place d'espaces de travail avec une résolution supérieure risque de créer des vues trop désordonnées pour pouvoir raisonnablement être utilisées avec des résolutions inférieures.

Pour créer des espaces de travail que vous pourrez exporter et inclure dans votre solution, vous devez mettre Tivoli Enterprise Portal en mode "Administrateur". Pour placer Tivoli Enterprise Portal en mode "Administrateur", procédez comme suit :

Procédure

1. Allez dans le répertoire *INSTALLATION_ITM*/CNP et ouvrez le fichier `cnp.bat`.

   Si vous avez utilisé l'installation par défaut, le répertoire est `C:\IBM\ITM\CNP`. Dans le fichier `cnp.bat`, mettez à jour la ligne `set _CMD= %_JAVA_CMD%` pour inclure l'option `-Dcnp.candle.mode="$_KCJ_$"`.

   Si vous voulez créer des extensions sur les systèmes Linux ou AIX, utilisez le chemin suivant :

   ```
   /opt/IBM/ITM/li263/cj/bin/cnp.sh
   ```

   où *li263* représente le système d'exploitation sur lequel Tivoli Enterprise Portal est en cours d'exécution.

   La ligne mise à jour `set _CMD= %_JAVA_CMD%` doit être similaire à la suivante :

   ```
   set _CMD= %_JAVA_CMD% -Dcnp.candle.mode="$_KCJ_$" -Xms64m -Xmx256m -showversion -noverify
    -classpath %CPATH% -Dkjr.trace.mode=LOCAL -Dkjr.trace.file=C:\IBM\ITM\CNP\LOGS\kcjras1.log
   -Dkjr.trace.params=ERROR -DORBtcpNoDelay=true -Dibm.stream.nio=true
   -Dice.net.maxPersistentConnections=16 -Dice.net.persistentConnectionTimeout=1
   -Dcnp.http.url.host=SKINANE -Dvbroker.agent.enableLocator=false  -Dnv_inst_flag=%NV_INST_FLAG
   ```

```
%
-Dnvwc.cwd=%NVWC_WORKING_DIR% -Dnvwc.java=%NVWC_JAVA% candle.fw.pres.CMWApplet
```

Remarque : La commande est présentée ici sur plusieurs lignes pour des raisons de formatage uniquement.

2. Ouvrez un nouveau client Tivoli Enterprise Portal et connectez-vous à l'aide de l'ID utilisateur `sysadmin`.
3. Définissez l'ID utilisateur "sysadmin" en mode "Administrateur". Dans Tivoli Enterprise Portal, sélectionnez **Editer** > **Administrer les utilisateurs**. Sélectionnez **sysadmin**, puis, sous l'onglet **Permissions**, sélectionnez **Administration de l'espace de travail**. Cochez la case **Mode d'administration d'espace de travail**.

   Si vous effectuez la sélection correctement, ***ADMIN MODE*** s'affiche dans la barre de titre du bureau.

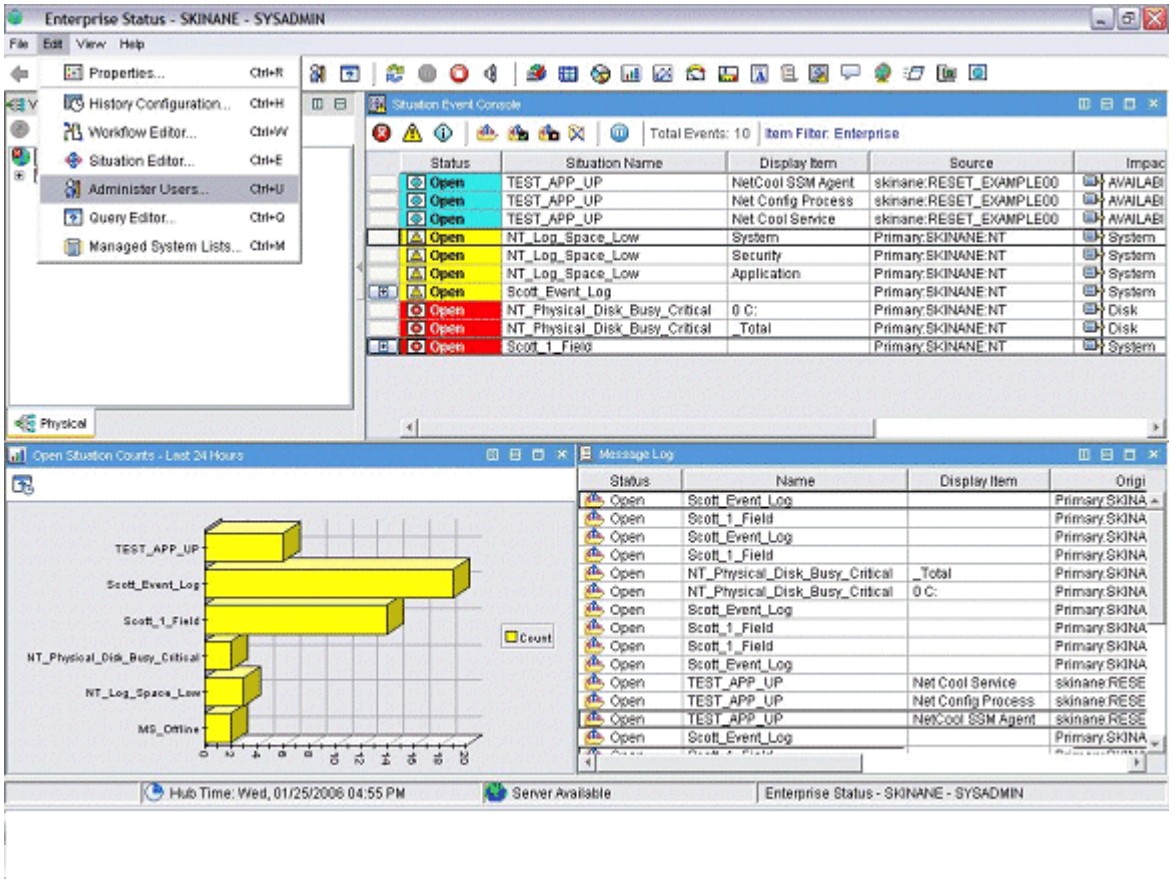


Figure 61. Définition de l'ID utilisateur `sysadmin`

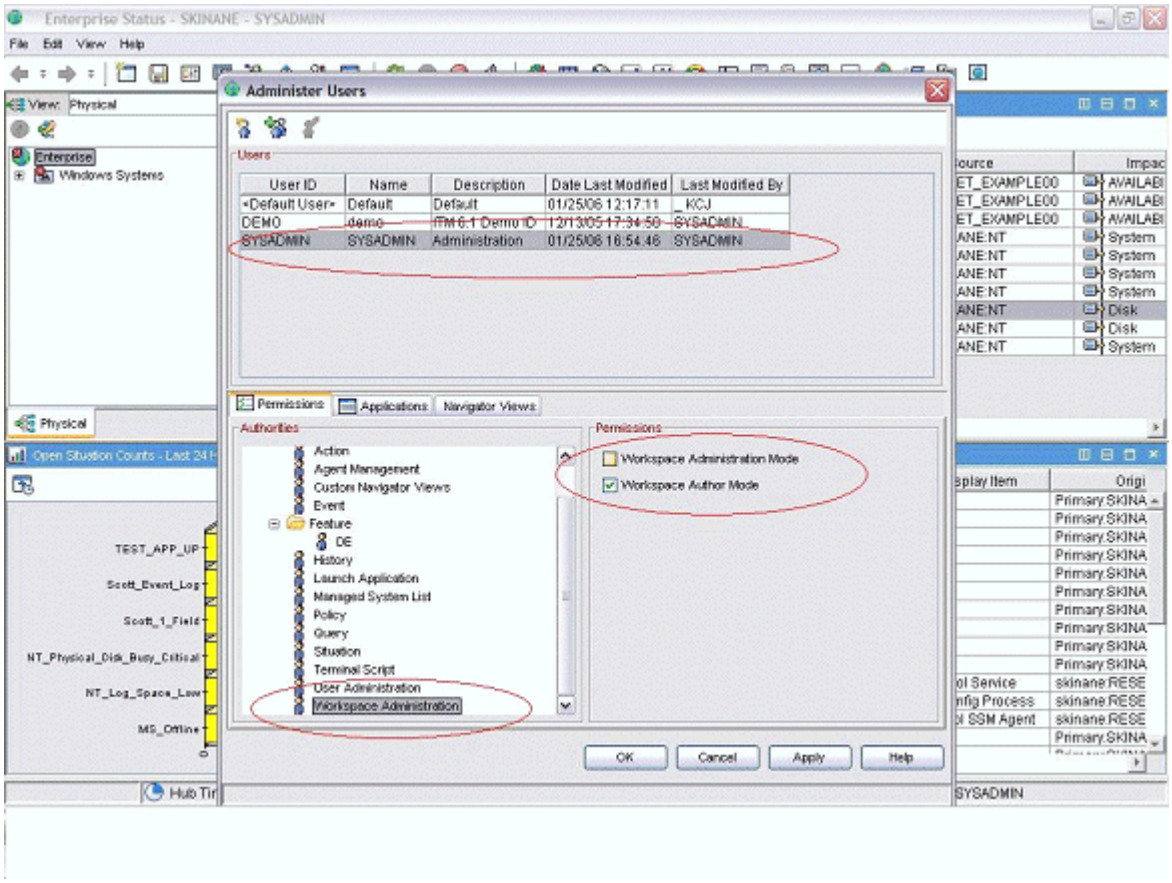


Figure 62. Définition de l'ID utilisateur `sysadmin` (suite)

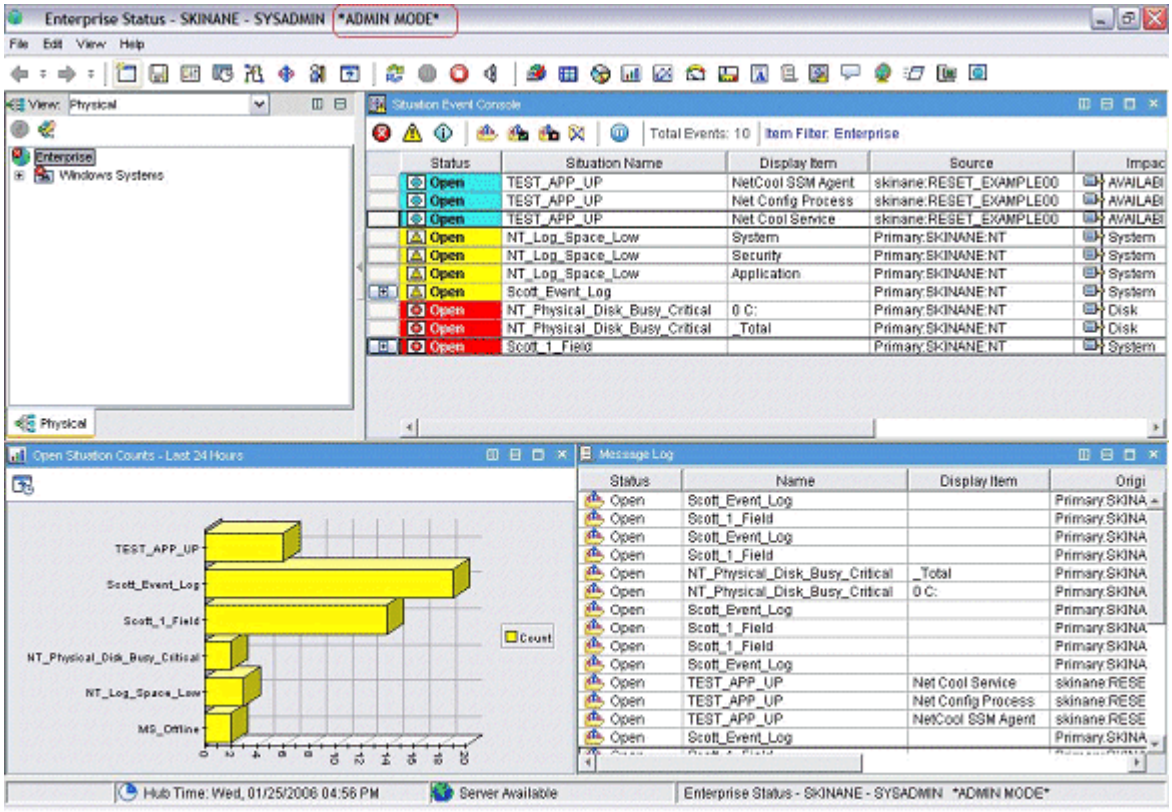


Figure 63. Définition de l'ID utilisateur `sysadmin` (suite)

Que faire ensuite

Une fois que vous êtes en mode "Administrateur", comme illustré à la (Figure 63, à la page 1415), vous êtes prêt à créer des espaces de travail pour votre application. Pour plus d'informations sur la procédure de personnalisation et de création d'espaces de travail, voir le manuel Tivoli Enterprise Portal User's Guide. Vous pouvez également utiliser la documentation d'aide qui est installée avec votre composant Tivoli Enterprise Portal.

Si vous voulez que vos espaces de travail soient en "lecture seule" et ne puissent pas être supprimés par un client, définissez les propriétés "non éditables" et "non effaçables" pour chaque espace de travail. Dans les propriétés de l'espace de travail, vous devez sélectionner les propriétés suivantes :

- **Ne pas autoriser les modifications**
- **Produit fourni par IBM (marquer comme non effaçable)**

Vous pouvez accéder aux propriétés en visualisant un espace de travail ou en cliquant sur l'icône comportant les commandes. Vous pouvez également consulter l'une des pages d'affichage des propriétés, et naviguer jusqu'au niveau de l'espace de travail dans l'arborescence des propriétés. Si vous avez plusieurs espaces de travail pour chaque élément du navigateur, vous devez définir les propriétés de chacun d'entre eux, comme indiqué dans l'exemple de capture d'écran suivant :

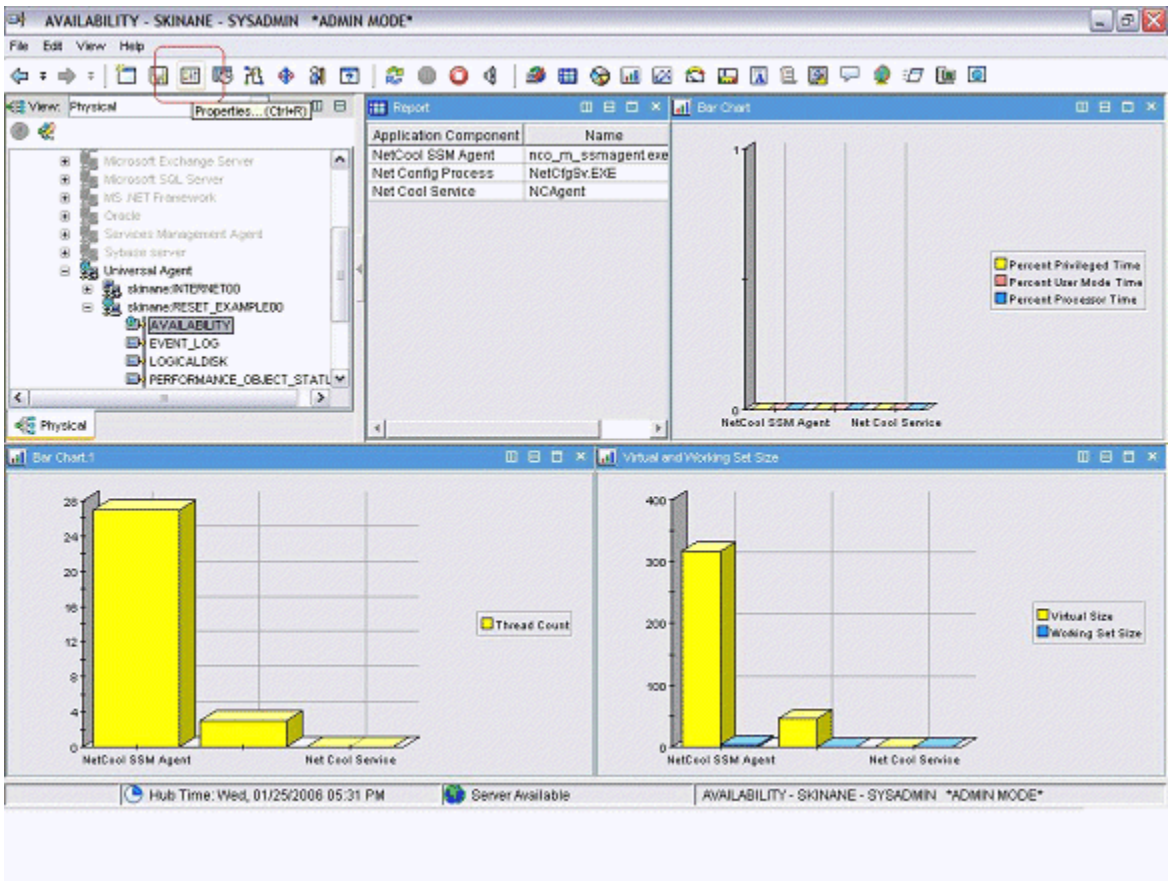


Figure 64. Définition des propriétés de l'espace de travail

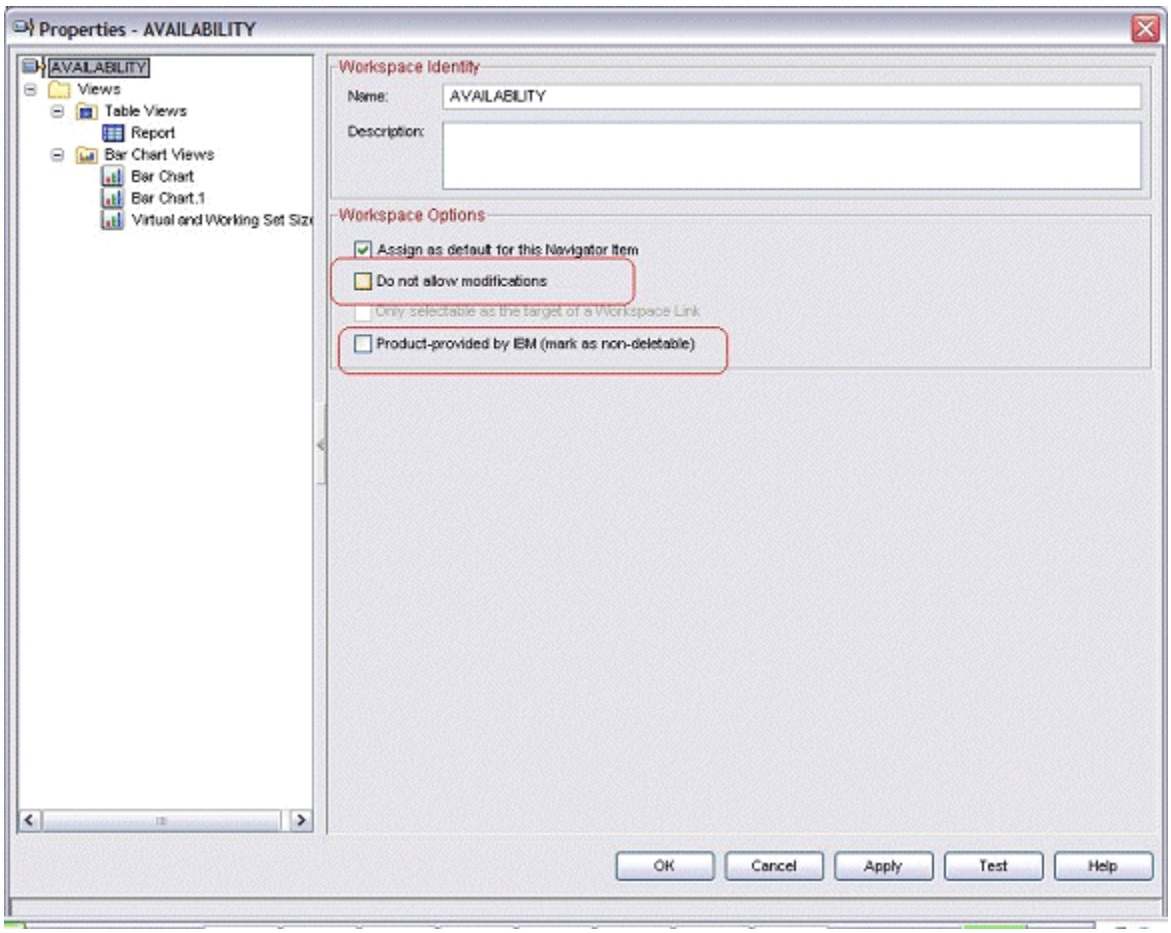


Figure 65. Définition des propriétés de l'espace de travail (suite)

Préparation de l'agent pour Cloud APM

Pour utiliser votre agent avec IBM Cloud Application Performance Management, vous devez le préparer à l'aide de l'assistant de **Configuration du tableau de bord**. Cet assistant configure les informations que vous pouvez visualiser dans les tableaux de bord récapitulatif et détaillé de Cloud APM. Il définit également les informations de ressource dont Cloud APM a besoin pour l'agent.

Avant de commencer

Pour préparer l'agent pour Cloud APM, vous devez vérifier que l'agent fournit les données suivantes :

- Un ou plusieurs ensembles de données (groupes d'attributs) qui produisent une ligne de données. Vous pouvez utiliser les attributs issus de ces ensembles de données pour remplir le tableau de bord récapitulatif.

  Important : Pour que des informations soient intégrées au tableau de bord récapitulatif, vous devez les fournir dans un ensemble de données qui produit une ligne de données unique. Certaines sources de données créent des ensembles de données produisant plusieurs lignes de données ; par exemple, les sources de données de code retour de commande, de service Windows et de processus placent les données dans l'ensemble de données Disponibilité unique, lequel produit plusieurs lignes. En pareil cas, vous devez créer un ensemble de données filtré qui produit une ligne afin d'inclure les données dans un tableau de bord récapitulatif. Pour plus d'informations, voir «Création d'un groupe d'attributs filtré», à la page 1383.
- Un attribut numérique dans l'un de ces ensembles de données qui indique le statut du service surveillé (normal, avertissement, critique ou toute autre valeur de statut similaire). Vous devez définir les valeurs de gravité du statut pour cet attribut. Pour obtenir des instructions sur la définition des valeurs de

gravité du statut, voir «Spécification de la gravité pour un attribut utilisé comme indicateur de statut», à la page 1236.

- Si le numéro de port sur lequel l'application surveillée fournit le service est fixe, vous devez connaître le port. Si le port risque de changer entre les différents déploiements, l'un des ensembles de données qui produisent une ligne de données doit contenir une zone numérique qui indique le port.
- Un attribut de chaîne dans l'un de ces ensembles de données qui indique l'adresse IP du serveur, si l'agent peut être installé sur un hôte pour surveiller un serveur qui s'exécute sur un hôte différent. Si l'agent surveille toujours l'hôte sur lequel il s'exécute, cet attribut n'est pas obligatoire.

  Conseil : Si un attribut qui fournit le nom d'hôte est disponible, vous pouvez créer un attribut dérivé pour l'adresse IP à l'aide de la fonction `nameToIpAddress`. Pour plus d'informations sur la création d'un attribut dérivé, voir «Création d'attributs dérivés», à la page 1229. Pour plus d'informations sur la fonction, voir «ipAddressToName», à la page 1243.

Si l'agent comporte des sous-noeuds, ces conditions s'appliquent à chaque sous-noeud pour lequel vous voulez créer un tableau de bord.

Pourquoi et quand exécuter cette tâche

Cloud APM surveille les *ressources*. Une ressource correspond à une instance de l'agent, parfois à un nous-noeud. Pour définir une ressource, vous devez indiquer le nom du type de la ressource, le nom du serveur, l'adresse IP et le numéro de port qui s'appliquent au service surveillé.

Cloud APM affiche un tableau de bord récapitulatif pour chaque ressource surveillée. Le tableau de bord récapitulatif contient un indicateur de statut ; grâce à cet indicateur (généralement vert, jaune ou rouge pour les statuts normal, avertissement ou critique), l'utilisateur peut afficher le statut de la ressource d'un seul coup d'oeil. Le même tableau de bord peut contenir d'autres indicateurs de santé généraux.

Sur le tableau de bord récapitulatif, les données s'affichent sous la forme d'éléments uniques. Par conséquent, l'ensemble de données contenant ces données ne doit générer qu'une seule ligne.

Un tableau de bord détaillé peut éventuellement être disponible pour l'agent. L'utilisateur peut cliquer sur le tableau de bord récapitulatif pour afficher le tableau de bord détaillé. Le tableau de bord détaillé peut afficher des tables, si bien que les données de tous les ensembles de données peuvent être utilisées sur ce tableau de bord.

Vous devez sélectionner les attributs qui s'affichent sur le tableau de bord récapitulatif (y compris l'indicateur de statut) et sur le tableau de bord détaillé.

Important : Les données contenues dans les attributs que vous sélectionnez sont automatiquement transmises de l'agent au serveur Cloud APM toutes les minutes. La spécification d'un volume de données trop important peut entraîner une surcharge du réseau, du serveur ou de l'hôte surveillé. Sélectionnez uniquement les attributs obligatoires. Par exemple, si un ensemble de données joint ou un attribut dérivé doit être affiché, ne spécifiez pas les attributs source en plus.

Important : Aucune donnée autre que ces attributs n'est transmise à Cloud APM. Vous ne pouvez ni afficher ni utiliser d'autres données dans Cloud APM, à l'exception des seuils qui sont surveillés au niveau de l'agent. Si vous utilisez d'autres données dans les seuils, vous risquez de ne plus pouvoir afficher le statut des seuils dans la console Cloud APM.

Procédure

1. Dans la vue **Informations sur l'agent**, cliquez sur le lien **Tableaux de bord**.
2. Sous **Composants du tableau de bord**, sélectionnez **Afficher les composants d'agent dans le tableau de bord**.

   Conseil : Si vous créez un agent pour une utilisation exclusive avec IBM Tivoli Monitoring, vous pouvez également sélectionner **Aucun tableau de bord présent pour cet agent**. Dans ce cas, n'exécutez pas les étapes suivantes de cette procédure. Vous ne pouvez pas installer un agent de ce type dans un environnement Cloud APM.
3. Cliquez sur le lien **Assistant de configuration de tableau de bord**.

4. Si l'agent comporte des sous-noeuds, définissez les dispositions des ressources de sous-noeud et d'agent dans Cloud APM :
   - Sélectionnez **Instances d'agent de base** pour afficher l'agent de base (les données extérieures aux sous-noeuds) en tant que ressource.
   - Pour chaque sous-noeud, sélectionnez **Instances "*noms*" de sous-noeud** pour afficher ce sous-noeud en tant que ressource.
   - Le cas échéant, pour chacun des sous-noeuds sélectionnés, sélectionnez **Afficher en tant qu'enfant d'agent**. Dans ce cas, la ressource de sous-noeud est affichée en tant qu'enfant sous la ressource d'agent dans des listes dans la console Cloud APM.

   Cloud APM affiche un tableau de bord récapitulatif et un tableau de bord détaillé pour chacun des composants que vous avez sélectionnés.

   Important : Si vous réexécutez l'assistant et désélectionnez un agent ou un sous-noeud, les ressources de l'agent ou du sous-noeud ne sont pas automatiquement supprimées. Pour supprimer les ressources, développez **Ressources** dans la vue Structure, sélectionnez les ressources à supprimer et appuyez sur la touche Suppr du clavier.
5. Sur la page **Sélection d'attribut - Statut**, sélectionnez l'attribut qui indique le statut du service surveillé. Les attributs numériques issus de groupes qui renvoient une ligne de données unique sont disponibles.

   Conseil : Si vous ne souhaitez pas afficher le statut du tableau de bord, désélectionnez **Fournir un statut à cet agent**.
6. Sur la même page, vous pouvez indiquer si vous souhaitez afficher les informations supplémentaires dans les tableaux de bord récapitulatif et détaillé :
   - Pour afficher d'autres indicateurs de santé généraux dans le tableau de bord récapitulatif, vérifiez que la case **Sélectionnez des attributs supplémentaires à afficher dans les informations récapitulatives de cet agent** est cochée. Sinon, cochez-la.
   - Pour afficher d'autres données dans le tableau de bord détaillé, vérifiez que la case **Sélectionnez des attributs supplémentaires à afficher dans les informations détaillées de cet agent** est cochée. Sinon, cochez-la. (Cette case doit être cochée dans la plupart des cas car un tableau de bord détaillé est nécessaire pour afficher un volume de données suffisamment important pour rendre un agent de surveillance significatif).

   Cliquez sur **Suivant**.
7. Si vous avez sélectionné **Sélectionnez des attributs supplémentaires à afficher dans les informations récapitulatives de cet agent** sur la page **Sélection d'attribut - Récapitulatif**, sélectionnez jusqu'à quatre attributs supplémentaires à inclure dans le tableau de bord récapitulatif. Les attributs issus de groupes qui renvoient une ligne de données unique sont disponibles. Cliquez sur **Suivant**.
8. Si vous avez sélectionné **Sélectionnez des attributs supplémentaires à afficher dans les informations détaillées de cet agent** sur la page **Sélection d'attribut - Détails**, sélectionnez les attributs à inclure dans le tableau de bord détaillé. Tous les attributs de l'agent sont disponibles. Pour éviter les problèmes de performances, indiquez le moins d'attributs possible. Cliquez sur **Suivant**.
9. Sur la page **Type de ressource**, entrez le type de serveur que vous surveillez, par exemple `Email server` ou `SampleCo Database Server`. Cliquez sur **Suivant**.
10. Sur la page **Sélection d'attribut - Nom de serveur logiciel**, entrez un nom de serveur logiciel fixe dans la zone **Nom corrigé** ou sélectionnez un attribut issu de votre agent qui fournit le nom du serveur logiciel. Ce nom apparaît à l'utilisateur pour cette instance surveillée spécifique, par exemple le nom de l'instance du serveur d'applications JBoss. Cliquez sur **Suivant**.

    Important : N'exécutez pas deux agents de surveillance, instances d'agent, sous-noeuds ou plus portant le même agent de surveillance logiciel sur le même hôte surveillé. Si votre agent possède des instances ou des sous-noeuds, vérifiez qu'un nom de serveur logiciel unique est généré pour chaque instance ou sous-noeud. Si deux agents différents génèrent le même nom de serveur logiciel, ne les installez pas sur le même hôte surveillé.

11. Sur la page **Sélection d'attribut - Adresse IP**, sélectionnez un attribut issu de votre agent qui spécifie l'adresse IP (et non le nom d'hôte) de la connexion d'interface principale utilisée par le serveur surveillé ou l'application. Par exemple, la connexion HTTP d'un serveur HTTP ou la connexion d'un serveur de base de données. Sinon, sélectionnez **Utilisez l'adresse IP de l'agent** pour utiliser l'adresse de l'hôte sur lequel l'agent s'exécute. Cliquez sur **Suivant**.
12. Sur la page **Sélection d'attribut - Port**, entrez le port sur lequel l'application surveillée fournit un service ou sélectionnez un attribut numérique issu de votre agent qui spécifie ce port. Cliquez sur **Terminer**.
13. Si vous avez sélectionné un agent et un sous-noeud, ou plusieurs sous-noeuds en tant que ressources, cliquez sur **Suivant** pour saisir les informations de ressource et de tableau du bord relatives au composant suivant (agent ou sous-noeud). Si le bouton **Suivant** est désactivé, vous avez saisi les informations pour tous les composants requis ; cliquez sur **Terminer** pour fermer l'assistant.

Résultats
Lorsque vous installez l'agent sur un hôte surveillé, vous pouvez afficher le tableau de bord récapitulatif et le tableau de bord détaillé dans l'onglet **Présentation des statuts**.

Important : Un délai pouvant aller jusqu'à 30 minutes peut se produire entre l'installation de l'agent et la disponibilité des tableaux de bord, particulièrement si c'est la première fois que ce type et cette version d'agent sont installés dans votre environnement.

Cliquez sur le tableau de bord récapitulatif de l'agent pour afficher le tableau de bord détaillé. Par défaut, toutes les informations contenues dans le tableau de bord détaillé s'affichent sous la forme de tableaux.

Vous pouvez utiliser l'onglet **Détails d'attribut** pour configurer l'affichage personnalisé de ces informations sous la forme de tableaux et de graphiques.

Test de votre agent dans Agent Builder

Après avoir utilisé Agent Builder pour créer un agent, vous pouvez tester l'agent dans Agent Builder.

Testez l'agent afin de vérifier que les données de surveillance que vous attendez sont bien les données affichées. Vous pourrez ainsi apprendre à modifier ou à peaufiner les paramètres de l'agent pour vous assurer que les données affichées sont utiles et fiables.

Vous pouvez tester votre agent dans Agent Builder à l'aide des méthodes suivantes :

1. Commencez par utiliser la fonction de test de groupe d'attributs Agent Builder pour tester des groupes d'attributs individuels un par un. Pour plus d'informations, voir «Test des groupes d'attributs», à la page 1420.
2. Après avoir effectué les tests des groupes d'attributs, vous pouvez utiliser la fonction de test d'agent de Agent Builder pour tester tous les groupes d'attributs de votre agent en même temps. Pour plus d'informations, voir «Test complet de l'agent», à la page 1424.

Important : Lors du test de votre agent dans Agent Builder, les valeurs spéciales suivantes apparaissent pour les attributs numériques :

- -1 : erreur générale
- -2 : données manquantes
- -3 : aucune valeur (par exemple, NULL a été renvoyé par une base de données)

Test des groupes d'attributs

Vous pouvez utiliser le test des groupes d'attributs pour tester les groupes d'attributs de l'agent créé avec Agent Builder, un groupe d'attributs à la fois. Vous pouvez tester de nombreux groupes d'attributs avant de compléter la définition du groupe d'attributs. Par exemple, vous pouvez lancer le test à partir de l'**Assistant d'IBM Tivoli Monitoring Agent** lorsque vous définissez les groupes d'attributs d'un nouvel agent. Vous pouvez également lancer le test à partir d'**IBM Tivoli Monitoring Agent Component Wizard** lorsque vous définissez les groupes d'attributs d'un nouvel agent.

Avant de commencer

Avant de commencer à tester un groupe d'attributs, vous pouvez :

- Définir des préférences pour tester les groupes d'attributs. Pour plus d'informations, voir «Test des groupes d'attributs - préférences», à la page 1422.
- Définir des variables d'environnement, des propriétés de configuration et, le cas échéant, des informations relatives à Java. Pour plus d'informations, voir «Test des groupes d'attributs - configuration», à la page 1423.

Pourquoi et quand exécuter cette tâche

Agent Builder prend en charge une fonction de test de groupe d'attributs pour la plupart des sources de données.

Procédure

- Démarrez la procédure de test de l'une des manières suivantes :
  1. Lors de la création de l'agent ou du groupe d'attributs, cliquez sur **Tester** dans la page Informations de la source de données appropriée.
  2. Après la création de l'agent, sélectionnez un groupe d'attributs à la page **Définition de la source de données** de l'éditeur d'agent et cliquez sur **Tester**. Pour plus d'informations sur l'éditeur d'agent, voir «Utilisation de l'éditeur d'agent pour modifier l'agent», à la page 1207.

  Lorsque vous cliquez sur **Tester** dans l'une des deux étapes précédentes, la fenêtre de test des groupes d'attributs s'affiche. Cette fenêtre varie en fonction des sources de données.

  Agent Builder prend en charge une fonction de test du groupe d'attributs pour la plupart des sources de données.

  Pour plus d'informations sur les procédures de test associées à des groupes d'attributs particuliers, consultez les sections Test suivantes :

  – Windows Management Instrumentation (WMI) - Pour plus d'informations sur la procédure de test WMI, voir «Test des groupes d'attributs WMI», à la page 1263
  – Windows Performance Monitor (Perfmon) - Pour plus d'informations sur la procédure de test Perfmon, voir «Test des groupes d'attributs Perfmon», à la page 1266.
  – Protocole SNMP (Simple Network Management Protocol) - Pour plus d'informations sur la procédure de test SNMP, voir «Test des groupes d'attributs SNMP», à la page 1270.
  – Expéditeur d'événements SNMP (Simple Network Management Protocol) - Pour plus d'informations sur la procédure de test de l'expéditeur d'événements SNMP, voir «Test des groupes d'attributs d'événement SNMP», à la page 1275.
  – Java Management Extensions (JMX), - Pour plus d'informations sur la procédure de test JMX, voir «Test des groupes d'attributs JMX», à la page 1296
  – Modèle CIM (Common Information Model) - Pour plus d'informations sur la procédure de test du modèle CIM, voir «Test des groupes d'attributs CIM», à la page 1298.
  – Fichier journal - Pour plus d'informations sur la procédure de test du fichier journal, voir «Test des groupes d'attributs de fichier journal», à la page 1310.
  – Script - Pour plus d'informations sur la procédure de test du script, voir «Procédure de surveillance de la sortie à partir d'un script», à la page 1322.
  – Java Database Connectivity (JDBC), - Pour plus d'informations sur la procédure de test JDBC, voir «Test des groupes d'attributs JDBC», à la page 1332
  – Ping ICMP (Internet Control Message Protocol) - Pour plus d'informations sur la procédure de test ICMP, voir «Test des groupes d'attributs Ping», à la page 1335.
  – Disponibilité du protocole HTTP (Hypertext Transfer Protocol) - Pour plus d'informations sur la procédure de test HTTP, voir «Test des groupes d'attributs HTTP», à la page 1343.

– SOAP - Pour plus d'informations sur la procédure de test SOAP, voir «Test des groupes d'attributs SOAP», à la page 1351.
– Socket TCP (Transmission Control Protocol) - Pour plus d'informations sur la procédure de test du socket, voir «Test des groupes d'attributs de socket», à la page 1362.
– Interface de programme d'application (API) Java - Pour plus d'informations sur la procédure de test de l'API Java, voir «Test des groupes d'attributs d'application Java», à la page 1377

Certaines sources de données ne disposent pas d'une fonction de test du groupe d'attributs. Par exemple :

– Lorsque le navigateur d'Agent Builder vous permet d'afficher des données réelles sur un système. Vous pouvez par exemple afficher les processus en cours d'exécution sur le système (processus), les services installés sur le système (services Windows) et les journaux des événements Windows présents sur le système.
– Vous ne pouvez pratiquement pas personnaliser l'agent (journal binaire AIX, code retour de commande).
– Les groupes d'attributs Joint et Filtré ne peuvent pas être testés à l'aide de la fonction de test de groupe d'attributs, car ces groupes reposent sur plusieurs groupes d'attributs.

Remarque :

1. Utilisez le test complet de l'agent pour tester des sources de données qui ne peuvent pas l'être à l'aide de la fonction de test de groupe d'attributs. Pour plus d'informations sur le test complet de l'agent, voir «Test complet de l'agent», à la page 1424.
2. Lors des tests des sources de données, après avoir cliqué sur **Collecter des données**, il se peut que des données ne s'affichent pas du tout ou ne soient pas actualisées après le premier clic. Dans ce cas, cliquez sur **Collecter des données** une seconde fois pour afficher les données actualisées.

- Débogage :

  Chaque source de données testée comporte un répertoire de test créé pour elle par Agent Builder. Ce répertoire est utilisé pour l'environnement d'exécution test de la source de données. Les fichiers journaux relatifs à la série de tests effectuée sur la source de données sont stockés dans ce répertoire. Les fichiers journaux peuvent s'avérer utiles pour déboguer les problèmes détectés lors de la procédure de test.

  Remarque :

  1. L'emplacement du fichier journal test apparaît sous la forme d'un message d'état dans la fenêtre **Test** lorsque vous cliquez sur **Démarrer l'agent** ou sur **Arrêter l'agent**.
  2. Tous les répertoires de test de source de données sont supprimés lorsqu'Agent Builder est arrêté.

Test des groupes d'attributs - préférences
Définissez vos préférences avant de tester un groupe d'attributs.

Pourquoi et quand exécuter cette tâche
Avant de commencer à tester un groupe d'attributs, vous pouvez définir certaines préférences pour déterminer la manière dont les attributs sont testés.

Procédure

1. Sélectionnez **Fenêtre** > **Préférences** dans la barre de menus d'Agent Builder.
   La fenêtre **Préférences** s'ouvre.
2. Sélectionnez **Agent Builder**.

   Les préférences relatives au test des groupes d'attributs sont les suivantes :

   Afficher la boîte de dialogue de changement de type de données lors du test
   Lorsque cette option est sélectionnée, Agent Builder suggère des modifications du type de données d'un attribut. C'est entre autres le cas lorsque le type de données d'un attribut ne

correspond pas aux données renvoyées lors du test de cet attribut. Par exemple, lorsque la longueur de chaîne définie pour un attribut est insuffisante pour maintenir une valeur renvoyée par un test. Dans ce cas, Agent Builder suggère de redéfinir l'attribut afin de lui accorder une longueur de chaîne supérieure. Lorsque cette option n'est pas sélectionnée, Agent Builder ne vérifie pas les types de données et ne suggère aucune modification pendant la phase de test. Cette option est sélectionnée par défaut.

Nombre maximum d'attributs de journal ou de script créés
La valeur indiquée dans cette zone détermine le nombre maximum d'attributs qu'Agent Builder analyse lors du test initial d'un groupe d'attributs de script ou de fichier journal. La valeur par défaut est 25.

3. Pour sauvegarder vos préférences, cliquez sur **OK** puis fermez la fenêtre **Préférences**.

   Pour restaurer les paramètres par défaut, cliquez sur **Restaurer les valeurs par défaut** puis sur **OK**.

Test des groupes d'attributs - configuration
Définissez des variables d'environnement, des propriétés de configuration et des informations Java avant de tester un groupe d'attributs.

Pourquoi et quand exécuter cette tâche
Avant de lancer le test d'un groupe d'attributs, vous pouvez éventuellement définir des variables d'environnement, des propriétés de configuration et, le cas échéant, des informations Java depuis la fenêtre Test de la source de données. Les informations Java constituent un sous-ensemble des données de configuration. Certaines variables d'environnement possèdent des valeurs spécifiques définies par défaut pour le test de groupe d'attributs. Pour plus d'informations sur les variables d'environnement possédant des valeurs spéciales pour le test des groupes d'attributs, voir «Variables d'environnement de test», à la page 1428.

Procédure

1. Facultatif : Cliquez sur **Définir l'environnement** dans la fenêtre **Test** de la source de données. La fenêtre **Variables d'environnement** s'ouvre. Une fois remplie, la fenêtre **Variables d'environnement** répertorie toutes les variables d'environnement utilisées pendant l'exécution du test. La vue initiale de la fenêtre Variable d'environnement reprend l'ensemble des variables d'environnement définies dans votre agent. Elle inclut également toutes les variables d'environnement que vous avez ajoutées à partir des tests précédents de cet agent.
   a) Cliquez sur **Ajouter** ou **Modifier** pour ajouter ou modifier des variables individuelles.
   b) Cliquez sur **Supprimer** pour supprimer des variables individuelles ou sur **Restaurer la valeur par défaut** pour restaurer les variables par défaut et supprimer toutes les autres.
   c) Cliquez sur **OK** pour sauvegarder vos modifications et revenir à la fenêtre **Test**.
2. Facultatif : Cliquez sur **Configuration** dans la fenêtre **Test** de la source de données. La fenêtre **Configuration d'exécution** s'ouvre.
   a) Cliquez sur **Editer la configuration de l'agent** pour ajouter une propriété de configuration ou pour modifier des propriétés de configuration existantes à l'aide de la fenêtre **Propriétés de configuration**.
   b) Sélectionnez une propriété de configuration et cliquez sur **Modifier** pour modifier une propriété de configuration existante associée au groupe d'attributs soumis au test.
   c) Sélectionnez une propriété de configuration et cliquez sur **Restaurer la valeur par défaut** pour restaurer une propriété de configuration sur sa valeur par défaut.

   Important : Si une source de données JMX se connecte à un serveur WebSphere Application Server distant, assurez-vous qu'un serveur WebSphere Application Server local est installé et que l'emplacement Java est associé à l'environnement d'exécution Java utilisé par ce serveur. Pour plus de détails sur la configuration de la connexion, voir «Surveillance de beans gérés (MBeans) JMX (Java Management Extensions)», à la page 1277.
3. Cliquez sur **OK** pour sauvegarder vos modifications et revenir à la fenêtre **Test**.
4. **Remarque :** Vous pouvez définir des informations Java pour les types de groupes d'attributs suivants :

- Java Management Extensions (JMX)
- JDBC (Java Database Connectivity)
- Disponibilité HTTP (Hypertext Transfer Protocol)
- SOAP
- Interface de programme d'application Java (API)

Les informations Java constituent un sous-ensemble des données de configuration décrites à l'étape «2», à la page 1423

Facultatif : Cliquez sur **Informations Java** dans la fenêtre **Test** de la source de données.

La fenêtre **Informations relatives à Java** s'ouvre.

a) Entrez les informations relatives à Java.
Par exemple, entrez ou accédez à l'emplacement de l'environnement d'exécution Java (JRE), sélectionnez un **Niveau de trace Java** ou entrez des **Arguments JVM**

b) Cliquez sur **OK** pour sauvegarder vos modifications et revenir à la fenêtre **Test**.

Test complet de l'agent

Utiliser le test complet de l'agent pour tester tous les groupes d'attributs de l'agent ensemble. Vous pouvez également utiliser le test complet de l'agent pour tester des sources de données qui ne peuvent pas l'être à l'aide de la fonction de test de groupe d'attributs.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le test complet de l'agent pour exécuter l'agent de la même façon que dans IBM Tivoli Monitoring, sans avoir besoin d'installer IBM Tivoli Monitoring.

Important : Sur les systèmes Windows, pour exécuter un test complet de l'agent dans Agent Builder (voir «Test complet de l'agent», à la page 1424), vérifiez que la version 32 bits du système d'exploitation sur lequel vous exécutez Agent Builder, à savoir Windows 32 bits, est sélectionnée dans la fenêtre Informations sur l'agent. Sur les systèmes Linux, la version 64 bits doit être sélectionnée.

Procédure

1. Ouvrez la perspective **Test de l'agent** :
   a) Dans l'éditeur d'agent, ouvrez l'onglet **Informations sur l'agent**.
   b) Cliquez sur **Tester l'agent**.

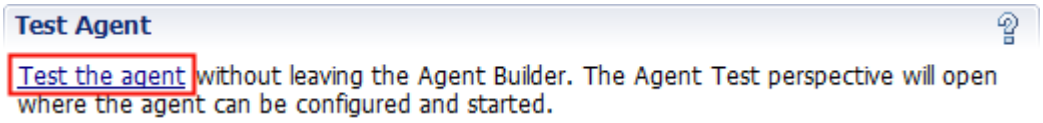


*Figure 66. Section **Test de l'agent** de l'**éditeur d'agent**, page **Informations sur l'agent**.*

   Vous pouvez également, à partir du menu d'Agent Builder, sélectionner **Fenêtre** > **Ouvrir la perspective** > **Autre**, sélectionner **Test de l'agent** et cliquer sur **OK**.

La perspective **Test de l'agent** s'ouvre (Figure 68, à la page 1427). La vue **Test de l'agent** répertorie les agents ouverts dans l'éditeur d'agent ; vous pouvez tester tous ces agents. La vue **Test du groupe d'attribut** s'affiche également ; à l'origine, cette vue est vide. La vue **Test du groupe d'attribut** affiche des données qui sont collectées à partir d'un groupe d'attributs sélectionné lorsque l'agent est en cours d'exécution.

Conseil : Si aucun agent n'est en cours d'édition, la perspective **Test de l'agent** est vide. Pour remplir la vue, allez à la perspective **IBM Tivoli Monitoring** et ouvrez un agent dans l'**Editeur d'agent**. Lorsqu'un agent est ouvert dans l'**Editeur d'agent**, retournez à la perspective **Test de l'agent** pour tester l'agent.

2. Facultatif : Définissez les variables d'environnement et les propriétés de configuration avant de démarrer le test.

Vous pouvez accéder aux fenêtres **Variables d'environnement** et **Configuration d'exécution** de deux manières à partir de la vue **Test de l'agent** :

- Cliquez avec le bouton droit de la souris sur l'agent dans la vue **Test de l'agent** pour ouvrir un menu de sélection. Vous pouvez sélectionner **Définir l'environnement** dans le menu pour ouvrir la fenêtre **Variables d'environnement**. Vous pouvez sélectionner **Configuration** dans le menu pour ouvrir la fenêtre **Configuration d'exécution**.
- Cliquez sur l'icône du menu de la vue sur la barre d'outils de la vue **Test de l'agent** pour accéder aux éléments de menu **Définir l'environnement** et **Configuration**, comme dans la sélection précédente.

Pour plus d'informations sur l'utilisation des fenêtres **Variables d'environnement** et **Configuration d'exécution**, voir «Test des groupes d'attributs», à la page 1420.

Important :

a. L'agent est rempli automatiquement avec le dernier ensemble de configuration correspondant à chaque groupe d'attributs testé.

b. Certaines variables d'environnement peuvent présenter des valeurs par défaut différentes pour le test de groupe d'attributs et le test complet de l'agent. Pour plus d'informations sur les variables d'environnement possédant des valeurs spéciales pour le test de groupe d'attributs («Variables d'environnement de test», à la page 1428).

c. Si une source de données JMX se connecte à un serveur WebSphere Application Server distant, assurez-vous qu'un serveur WebSphere Application Server local est installé et que l'emplacement Java est associé à l'environnement d'exécution Java utilisé par ce serveur. Pour plus de détails sur la configuration de la connexion, voir «Surveillance de beans gérés (MBeans) JMX (Java Management Extensions)», à la page 1277.

d. Dans une source de données SOAP, HTTP, JMX, JDBC ou API Java, vous pouvez utiliser le paramètre **Java** > **Arguments JVM** pour contrôler la consignation des traces d'agent. Définissez la valeur suivante :

```
-DJAVA_TRACE_MAX_FILES=fichiers -DJAVA_TRACE_MAX_FILE_SIZE=taille
```

où *fichiers* correspond au nombre maximal de fichiers journaux de trace conservés (valeur par défaut = 4) et *taille* correspond à la taille maximale des fichiers journaux en ko (valeur par défaut = 5 000). Par exemple, vous pouvez définir la valeur suivante :

```
-DJAVA_TRACE_MAX_FILES=7 -DJAVA_TRACE_MAX_FILE_SIZE=100
```

L'agent écrit alors 100 kilooctets dans le premier fichier journal, puis passe au second fichier journal, et ainsi de suite. Après avoir écrit sept fichiers journaux de 100 kilooctets chacun, l'agent écrase le premier fichier journal.

e. Si, dans une version installée, votre agent comporte des sous-noeuds, vous pouvez définir des valeurs de configuration différentes pour chaque sous-noeud ainsi que des valeurs distinctes pour les groupes d'attributs de l'agent de base. Toutefois, dans une configuration de test d'agent complète, vous ne pouvez définir chaque valeur de configuration qu'une seule fois ; le paramètre s'applique à l'agent de base et à ses sous-noeuds. Vous ne pouvez tester qu'une instance de chaque sous-noeud.

3. Dans la vue **Test de l'agent**, sélectionnez l'agent que vous souhaitez tester, puis cliquez sur l'icône  **Démarrer l'agent**.

Une fenêtre indique que l'agent est en cours de démarrage. Lorsque l'agent démarre, ses groupes d'attributs sont affichés comme enfants de l'agent dans la vue **Test de l'agent**. Les groupes d'attributs sont signalés par l'icône de groupe d'attributs  .

Les groupes d'attributs de statut qui donnent des informations sur l'agent (**Statut de l'objet de performances**, **Statut du pool d'unités d'exécution** et **Statut de l'action**) sont affichés comme

enfants de l'agent dans la vue **Test de l'agent**. Les groupes d'attributs de statut sont signalés par l'icône d'information .

Vous pouvez démarrer et exécuter plusieurs agents en même temps.

L'icône **Arrêter l'agent** devient disponible lors du démarrage de l'agent.

Si votre agent comporte des sous-noeuds ou des groupes de navigation, ils sont affichés comme noeuds dans la vue **Test de l'agent**. Les définitions de sous-noeud s'affichent dans l'agent. Une instance de sous-noeud s'affiche dans le noeud de définition de sous-noeud. Des groupes d'attributs et des groupes de navigation apparaissent dans le noeud d'instance de sous-noeud. Par exemple :

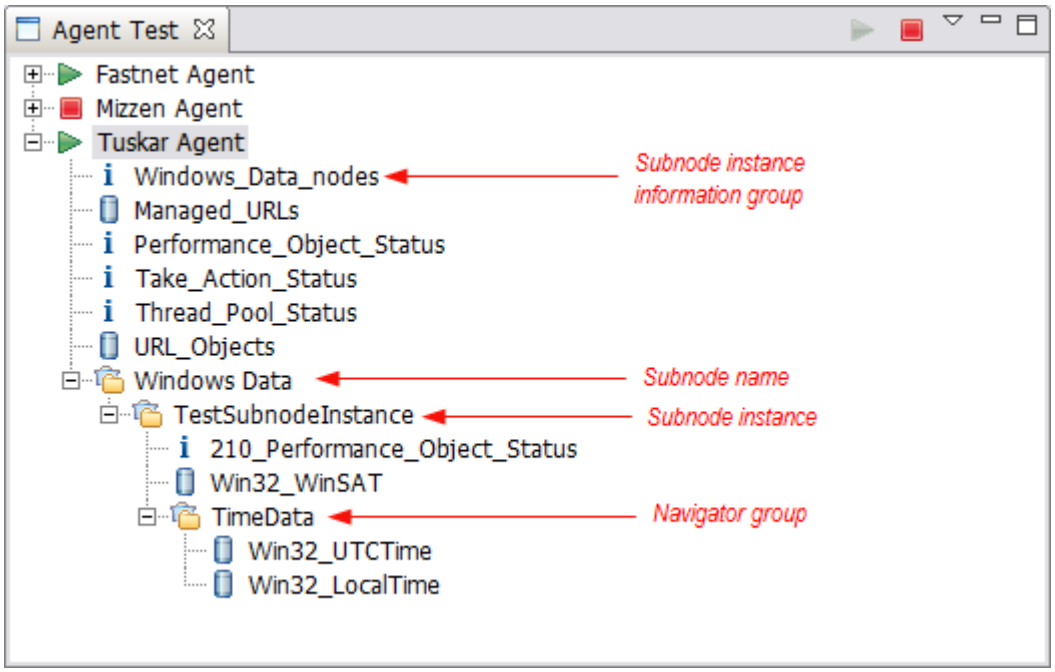


*Figure 67. Vue **Test de l'agent** avec exemple de sous-noeud et groupe de navigation mis en évidence.*

Vous pouvez cliquer avec le bouton droit de la souris sur l'un des noeuds de la vue **Test de l'agent** pour accéder aux sélections de menu telles que **Editer** et **Arrêter l'agent**. L'option **Editer** permet d'ouvrir la vue **Définition de la source de données** pour le noeud sélectionné dans l'**éditeur d'agent**.

Remarque : Les modifications que vous apportez à l'**éditeur d'agent** ne sont pas visibles dans l'agent en cours d'exécution tant que vous ne l'avez pas arrêté puis redémarré.

4. Dans la vue **Test de l'agent**, sélectionnez le premier groupe d'attributs que vous souhaitez tester.

   Lors de la sélection d'un groupe d'attributs, la collecte de données commence pour le groupe d'attributs sélectionné. Si la collecte requiert un certain temps, une fenêtre indique que la collecte de données est en cours. Lorsque la collecte de données est terminée, les données collectées sont affichées dans la vue **Test de groupe d'attributs**, par exemple :

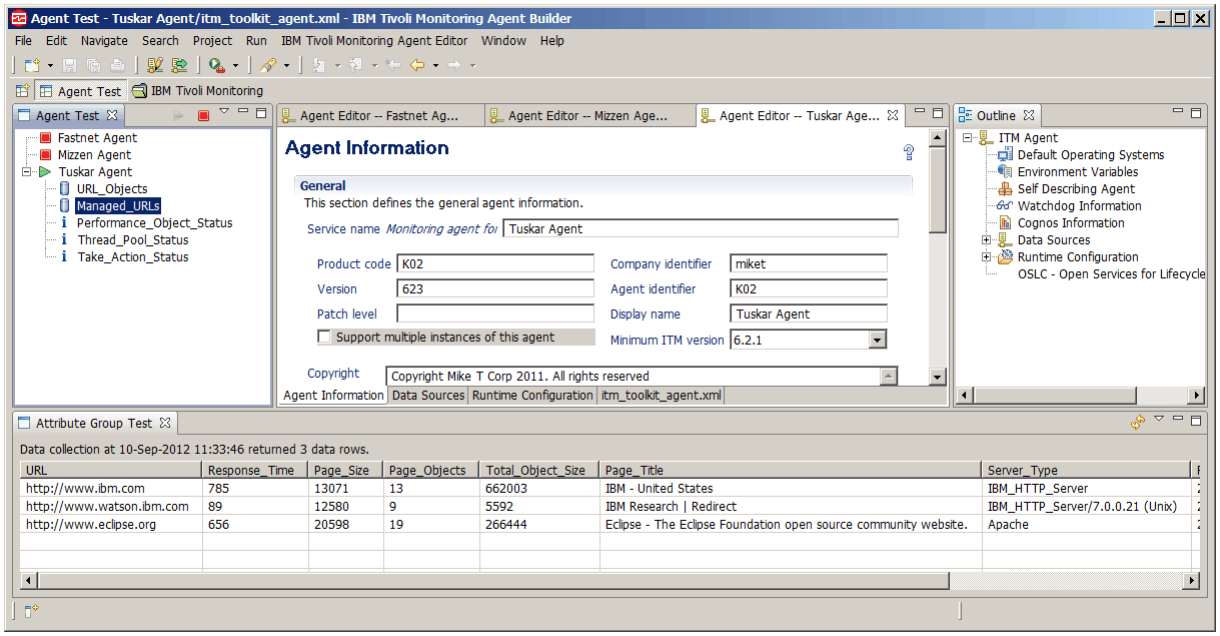


*Figure 68. Perspective **Test de l'agent***

Si aucune donnée ne s'affiche, un message indiquant`0 ligne(s) de données renvoyée(s)` apparaît dans la vue **Test du groupe d'attributs**. Le non renvoi d'informations par l'agent peut s'expliquer de diverses façons. Ces raisons sont notamment les suivantes :

- Absence de données
- Définition incorrecte
- Configuration incorrecte

Vous pouvez vérifier la raison pour laquelle aucune donnée n'est renvoyée en consultant la valeur du **Code_Erreur** dans le groupe d'attributs **Statut de l'objet de performances**. Pour plus d'informations sur l'affichage du groupe d'attributs **Statut de l'objet de performances**, voir l'étape «9», à la page 1428.

Pour collecter des données pour un autre groupe d'attributs dans l'agent en cours d'exécution, sélectionnez le groupe d'attributs voulu.

Lorsque vous sélectionnez un groupe d'attributs dans la vue **Test de l'agent**, le groupe d'attributs correspondant est affiché dans la vue **Editeur d'agent**.

5. Facultatif : Pour certains types de groupe d'attributs, après la collecte initiale de données, vous devez lancer une seconde collecte de données pour obtenir des valeurs de données utiles.

   Pour exécuter une collecte de données, cliquez sur l'icône de collecte de données  dans la vue **Test du groupe d'attributs**.

   Si la collecte requiert un certain temps, une fenêtre indique qu'une collecte de données est en cours. Lorsque la collecte de données est terminée, les données collectées sont affichées dans la vue **Test du groupe d'attributs**.
6. Facultatif : Cliquez sur un en-tête de colonne d'attribut dans la vue **Test du groupe d'attributs** pour ouvrir les **Informations d'attribut** dans l'onglet **Définition de la source de données** de l'**éditeur d'agent**. Vous pouvez également accéder à ces mêmes **Informations d'attribut** en cliquant avec le bouton droit de la souris sur une cellule de données dans la table et en choisissant **Editer** dans le menu.

   Vous pouvez modifier les propriétés de l'attribut normalement. Les modifications que vous apportez ne sont pas visibles dans l'agent en cours d'exécution tant que vous ne l'avez pas arrêté puis redémarré.
7. Facultatif : Vous pouvez ouvrir plusieurs vues **Test du groupe d'attributs** en même temps.

Pour ouvrir une autre vue **Test du groupe d'attributs**, cliquez sur l'icône de menu de la vue sur la barre d'outils de la vue **Test du groupe d'attributs**, puis sélectionnez **Ouvrir la vue pour le groupe d'attributs**.

Remarque : Lorsqu'une vue **Test du groupe d'attributs** supplémentaire est ouverte, elle affiche les mêmes informations d'attribut que la vue **Test du groupe d'attributs** initiale. Vous pouvez ensuite sélectionner un autre groupe d'attributs dans la vue **Test de l'agent** pour afficher les informations d'un groupe d'attributs différent dans la vue **Test de groupe d'attributs** originale. Lorsqu'une vue **Test du groupe d'attributs** supplémentaire est ouverte pour la première fois, elle s'ouvre au même emplacement que la vue initiale, mais dans un onglet différent. Pour afficher les deux vues simultanément, vous pouvez faire glisser l'onglet vers un autre emplacement dans l'espace de travail.

8. Facultatif : Si votre agent possède des sous-noeuds, vous pouvez sélectionner le groupe d'attributs d'informations pour l'instance de sous-noeud pour voir comment les sous-noeuds sont répertoriés dans votre agent (Figure 67, à la page 1426). La sélection du groupe d'attributs d'informations pour l'instance de sous-noeud affiche les informations de l'instance de sous-noeud dans la vue **Test de groupe d'attributs** (pour tous les sous-noeuds en ligne du type sélectionné).
9. Facultatif : Pour consulter plus d'informations sur le fonctionnement de l'agent, vous pouvez sélectionner les groupes d'attributs **Statut de l'objet de performances** et **Statut du pool d'unités d'exécution** dans la vue **Test de l'agent**. Ces groupes d'attributs de statut sont signalés par l'icône d'informations  . Sélectionnez ces groupes pour afficher les informations d'état sur les collectes de données précédentes des groupes d'attributs.

   Par exemple :

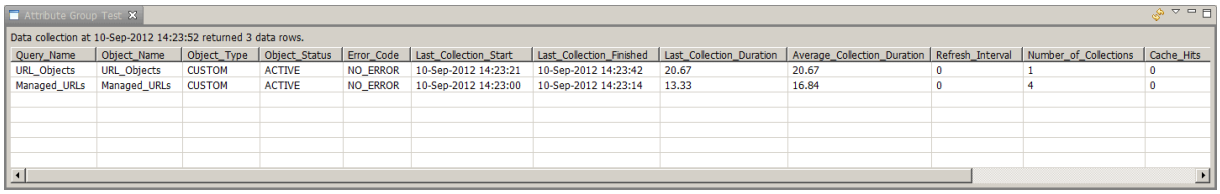


   *Figure 69. Vue **Test du groupe d'attributs** affichant des informations supplémentaires (Statut de l'objet de performances) sur les collectes de données pour les groupes d'attributs **Managed_URLs** et **Managed_Nodes***

10. Une fois que vous avez fini de tester votre agent, cliquez sur l'icône d'arrêt de l'agent  .

Variables d'environnement de test

Les variables d'environnement ci-après permettent de contrôler le comportement de l'agent au moment du test.

Les variables d'environnement sont des valeurs nommées dynamiques qui déterminent le mode d'exécution de l'agent. Dans le cas du test des groupes d'attributs, certaines variables d'environnement de l'agent sont associées à des valeurs spéciales. Ces valeurs sont utilisées pour que l'agent réponde de manière à satisfaire au test d'un groupe d'attributs unique. Dans le cas du test complet de l'agent, les valeurs par défaut sont utilisées et non les valeurs spéciales. Les valeurs par défaut signifient que l'agent fonctionne de manière standard, ce qui est plus adapté au test complet de l'agent.

Les variables d'environnement comportant des valeurs spéciales pour le test des groupes d'attributs sont décrites dans le tableau suivant. Pour plus d'informations sur toutes les variables d'environnement de l'agent, voir («Liste des variables d'environnement», à la page 1210). Pour plus d'informations sur la définition des variables d'environnement, voir («Variables d'environnement», à la page 1209).

Tableau 299. Variables d'environnement

Variable d'environnement	Valeur par défaut (test complet de l'agent)	Valeur de test du groupe d'attributs	Raison de la modification de la valeur de test du groupe d'attributs
CDP_DP_INITIAL_COLLECTION_DELAY	varie	1	Cette valeur s'applique à un agent avec un pool d'unités d'exécution. Elle correspond au temps d'attente, en secondes, du pool d'unités d'exécution avant que la demande de collecte de données d'origine ne soit envoyée à un fournisseur de données. **Remarque :** Si CDP_DP_INITIAL_COLLECTION_DELAY n'est pas défini, le pool d'unités d'exécution attend le laps de temps indiqué dans CDP_DP_REFRESH_INTERVAL ou CDP_ATTRIBUTE_GROUP_REFRESH_INTERVAL. Cette durée est identique à le délai d'attente du pool d'unités d'exécution entre les collectes de données. En outre, elle est susceptible d'être trop longue pour la première collecte de données.
CDP_DP_CACHE_TTL	55	1	Lorsque la valeur est définie sur 1, le fournisseur de données regroupe les données immédiatement après la réception de la demande de collecte. Sinon, il renvoie les données qui sont en mémoire cache depuis 60 secondes.

Installation de votre agent dans une infrastructure de surveillance à des fins de test et d'utilisation

Après avoir testé votre agent dans Agent Builder, vous pouvez installer l'agent dans un environnement IBM Tivoli Monitoring ou IBM Cloud Application Performance Management existant à des fins de test et d'utilisation.

L'installation et le test de votre agent dans une infrastructure de surveillance présentent les avantages suivants :

- Vous pouvez configurer et tester plusieurs instances d'un agent qui s'exécutent simultanément.
- Vous pouvez configurer et tester plusieurs instances de sous-noeuds qui s'exécutent simultanément.
- Dans un environnement Tivoli Monitoring, vous pouvez générer des espaces de travail, des situations, des actions et des requêtes dans Tivoli Enterprise Portal.

Important : Déployez les versions initiales de votre agent dans une version de test version de l'infrastructure de surveillance. Sous Tivoli Monitoring, utilisez un serveur de surveillance et un serveur de portail distincts. Sous Cloud APM, utilisez un compte cloud de test ou un déploiement de test distinct du serveur de surveillance sur site. Déployez la version finale de votre agent sur une infrastructure de production.

Si vous déployez une version de l'agent sur l'infrastructure de surveillance de production, puis que vous modifiez n'importe quel jeu de données de l'agent, la nouvelle version peut être en conflit avec la version

antérieure sur le serveur. Dans ce cas, il peut être impossible d'utiliser n'importe quelle version de l'agent.

Installation d'un agent

Il existe deux méthodes permettant d'installer les agents que vous créez avec Agent Builder.

1. Pour tester votre agent avec une infrastructure de surveillance exécutée sur le même système qu'Agent Builder, vous pouvez installer l'agent dans l'installation locale de Tivoli Monitoring ou Cloud APM.
2. Pour tester ou utiliser l'agent avec un système Tivoli Monitoring ou Cloud APM qui n'est pas exécuté sur le même système qu'Agent Builder, vous pouvez générer un fichier compressé (*package d'agent*) que vous pouvez transférer vers les autres systèmes et déployer.

Remarque :

1. Avec Tivoli Monitoring, après avoir installé un agent, vous pouvez voir les attributs de performances dans les tables de Tivoli Enterprise Portal. Pour la prise en charge des situations ou espaces de travail, voir «Importation des fichiers de prise en charge de l'application», à la page 1447.
2. Avec Tivoli Monitoring, après avoir installé l'agent, vous pouvez utiliser Tivoli Enterprise Portal pour vérifier les données issues de l'agent. Pour plus d'informations, voir «Modifications dans Tivoli Enterprise Portal», à la page 1441. Pour modifier l'agent après avoir consulté les données dans Tivoli Enterprise Portal, voir «Utilisation de l'éditeur d'agent pour modifier l'agent», à la page 1207.
3. Pour un agent prenant en charge Linux ou UNIX, générez l'image d'installation sur un système Linux ou UNIX car ce type de système crée les fichiers avec les droits appropriés.

Installation en local d'un agent

Installez l'agent dans un environnement de surveillance sur le système local où Agent Builder s'exécute.

Pourquoi et quand exécuter cette tâche

Pour installer votre agent dans un environnement de surveillance sur le système local, procédez comme suit :

1. Cliquez sur le fichier `itm_toolkit_agent.xml` dans l'arborescence de navigation de l'Explorateur de projets d'Agent Builder en utilisant l'une des méthodes suivantes :
   a. Cliquez avec le bouton droit de la souris sur le fichier `itm_toolkit_agent.xml` et sélectionnez **IBM** > **Générer un agent**.
   b. Sélectionnez le fichier `itm_toolkit_agent.xml` et sélectionnez l'icône  **Générer un agent** dans la barre d'outils.
   c. Cliquez deux fois sur le fichier `itm_toolkit_agent.xml` et sélectionnez **Agent Editor** > **Générer un agent**.
2. Dans la fenêtre **Assistant Générer un agent**, dans la section **Installer l'agent localement**, entrez le répertoire d'installation de l'infrastructure de surveillance. Agent Builder indique la valeur qui se trouve dans la variable d'environnement `CANDLE_HOME`. Si cette variable n'est pas définie, la valeur par défaut de Windows, `C:\IBM\ITM`, est affichée.

   Les cases sont cochées comme suit :

   Installer l'agent
   Cochée si Agent Builder détecte une instance appropriée de Tivoli Enterprise Monitoring Agent ou un agent IBM Cloud APM à l'emplacement spécifié. Un agent approprié est un agent qui prend en charge le système d'exploitation local et dont la version minimale est correcte.

   Installer le support de TEMS support
   Cochée dans un environnement Tivoli Monitoring si Agent Builder détecte une instance de Tivoli Enterprise Monitoring Server à l'emplacement spécifié.

Installer le support de TEPS support
Cochée dans un environnement Tivoli Monitoring si Agent Builder détecte une instance de Tivoli Enterprise Portal Server à l'emplacement spécifié.

3. Sélectionnez les composants à installer (agent, support Tivoli Enterprise Monitoring Server, support Tivoli Enterprise Portal Server).
4. Dans un environnement Tivoli Monitoring, si Tivoli Enterprise Monitoring Server ou Tivoli Enterprise Portal Server est installé sur l'ordinateur local et que vous installez les fichiers de support de ces serveurs, vous pouvez choisir de redémarrer les serveurs.

   Dans ce cas, les cases **Redémarrer TEMS sans données d'identification** et **Redémarrer TEPS** sont cochées dans la section **Installer l'agent localement** dans l'assistant Générer l'agent. Vous pouvez décocher les cases pour installer le support sans recycler les serveurs.

   Lorsque vous décochez la case **Redémarrer TEMS sans données d'identification**, vous êtes invité à entrer l'ID utilisateur et le mot de passe de Tivoli Enterprise Monitoring Server. Entrez ces informations et cliquez sur **Se connecter**. Si vous exécutez Tivoli Monitoring lorsque la sécurité est désactivée, entrez "sysadmin" pour l'ID utilisateur, laissez la zone de mot de passe à blanc, puis cliquez sur **Connexion**.

   Si vous souhaitez continuer sans entrer d'informations d'identification, cliquez sur **Se connecter** sans spécifier d'ID utilisateur et de mot de passe ou cliquez sur **Annuler**. Si vous suivez ces étapes, Tivoli Enterprise Monitoring Server est recyclé.

   Important : Pour installer des fichiers de support sans recycler Tivoli Enterprise Monitoring Server, assurez-vous que Tivoli Enterprise Monitoring Server est en cours d'exécution.
5. Sélectionnez les composants d'agent à générer. Vous pouvez sélectionner **Agent de base** et/ou **Génération de rapports Cognos**.
6. Dans un environnement IBM Cloud APM, vous pouvez activer la fonction de signature de sécurité pour les agents autodescriptifs. Cliquez sur **Modifier toutes les préférences de signature des fichiers JAR**. Vous pouvez ajouter un horodatage aux fichiers JAR signés et spécifier l'autorité d'horodatage. Spécifiez les détails de votre fichier de clés Java.

   Remarque : Vous devez créer le fichier de clés Java grâce aux outils Java. Par exemple, pour générer une clé privée et un certificat avec une clé publique correspondante dans un fichier de clés Java, vous pouvez exécuter cette commande :

   - *chemin_install_ab*/jre/bin/keytool -genkeypair -keystore *chemin_fichier_clés* -storepass *motdepasse_magasin_clés* -alias *alias_magasin_clés* -dname "CN=*nom_commun*, OU=*unité_organisationnelle*, L=*ville_ou_région*, ST=*état_ou_province*, C=*pays*" -keypass *motdepasse_clé*

   Où :

   - *chemin_install_ab* correspond à l'emplacement d'installation d'Agent Builder
   - *chemin_fichier_clés* correspond au chemin d'accès vers un fichier de clés JKS existant ou vers l'emplacement où un fichier de clés JKS est créé
   - *motdepasse_fichier_clés* correspond au mot de passe requis pour accéder à tout élément de ce fichier de clés
   - *alias_fichier_clés* correspond à un nom qui identifie cette clé au sein du fichier de clés (valeur par défaut : "mykey")
   - *motdepasse_clé* correspond au mot de passe requis pour accéder à cette clé (valeur par défaut : key_store_password)

   Le certificat doit être inclus dans le fichier de clés du serveur.
7. Une fois les détails de **signature JAR** renseignés, cliquez sur **OK**.
8. Cliquez sur **Terminer**.

9. Configurez et démarrez l'agent. Pour plus d'informations, voir «Configuration et démarrage de l'agent dans un environnement IBM Tivoli Monitoring», à la page 1434 ou «Configuration de l'agent», à la page 1436 et «Démarrage et arrêt de l'agent», à la page 1437 dans un environnement IBM Cloud APM.

   Si vous utilisez Tivoli Monitoring v6.2 groupe de correctifs 1 ou une version ultérieure, vous pouvez installer le support Tivoli Enterprise Monitoring Server et Tivoli Enterprise Portal Server sans redémarrer les serveurs. Dans ce cas, les cases **Redémarrer TEMS sans données d'identification** et **Redémarrer TEPS** sont cochées dans la section **Installer l'agent localement** dans l'assistant Générer l'agent. Vous pouvez décocher les cases pour installer le support sans recycler les serveurs. Lorsque vous décochez la case **Redémarrer TEMS sans données d'identification**, vous êtes invité à entrer l'ID utilisateur et le mot de passe de Tivoli Enterprise Monitoring Server. Entrez l'ID utilisateur et le mot de passe de Tivoli Enterprise Monitoring Server, puis cliquez sur **Connexion**. Si vous exécutez Tivoli Monitoring lorsque la sécurité est désactivée, entrez "sysadmin" pour l'ID utilisateur, laissez la zone de mot de passe à blanc, puis cliquez sur **Connexion**. Vous pouvez également continuer sans entrer de données d'identification (cliquez sur **Connexion** sans indiquer d'ID utilisateur et de mot de passe, ou cliquez sur **Annuler**. Cette action permet de recycler Tivoli Enterprise Monitoring Server.

   Remarque : Tivoli Enterprise Monitoring Server doit être en cours d'exécution pour que les fichiers de prise en charge puissent être installés sans que Tivoli Enterprise Monitoring Server soit recyclé.

Création du package d'agent
Vous pouvez utiliser Agent Builder pour créer un package d'installation d'agent compressé.

Pourquoi et quand exécuter cette tâche

Un package d'agent contient tous les paramétrages nécessaires à l'exécution de l'agent, ainsi que les scripts d'installation et de configuration. Il englobe également les fichiers d'assistance de l'environnement de surveillance.

Vous pouvez l'utiliser pour installer l'agent dans les environnements IBM Tivoli Monitoring et IBM Cloud Application Performance Management.

Procédure

1. Cliquez sur le fichier `itm_toolkit_agent.xml` dans l'arborescence de navigation de l'**Explorateur de projets** d'Agent Builder en utilisant l'une des méthodes suivantes :
   - Cliquez avec le bouton droit de la souris sur le fichier `itm_toolkit_agent.xml` et sélectionnez **IBM** > **Générer un agent**.
   - Sélectionnez le fichier `itm_toolkit_agent.xml` et cliquez sur l'icône  **Générer un agent** dans la barre d'outils.
   - Cliquez deux fois sur le fichier `itm_toolkit_agent.xml` et sélectionnez **Agent Editor** > **Générer un agent**.
2. Entrez le nom du répertoire où conserver la sortie (un package compressé ou des fichiers étendus) dans la section **Générer l'image de l'agent**.
3. Cochez la case **Conserver les fichiers intermédiaires** pour que les fichiers développés générés soient séparés du fichier zip ou tar.
4. Cochez la case **Créer un fichier ZIP** pour créer un fichier compressé dans le répertoire indiqué. Le fichier zip compressé porte le nom `smai-`*`nom_agent-version`*`.zip` pour les systèmes Windows par défaut.
5. Cochez la case **Créer un fichier TAR** pour créer un fichier compressé dans le répertoire indiqué. Le fichier tar compressé porte le nom `smai-`*`nom_agent-version`*`.tgz` pour les systèmes UNIX et Linux par défaut.
6. Sélectionnez les composants d'agent à générer. Vous pouvez sélectionner **Agent de base** et/ou **Génération de rapports Cognos**.

Important : Pour l'environnement IBM Cloud Application Performance Management, ne sélectionnez pas la génération de rapports **Cognos Reporting**, car les rapports ne sont actuellement pas pris en charge et l'inclusion des rapports augmente la taille du package.

7. Vous pouvez éventuellement activer la signature de sécurité pour les fichiers d'application de l'agent. Pour activer la signature de sécurité, sélectionnez **Signer le fichier JAR de prise en charge de l'autodescription**. Cliquez sur **Modifier toutes les préférences de signature des fichiers JAR**. Vous pouvez ajouter un horodatage aux fichiers JAR signés et spécifier l'autorité d'horodatage. Spécifiez les détails de votre fichier de clés Java.

   Important : Vous pouvez créer le fichier de clés Java grâce aux outils Java. Par exemple, pour générer une clé privée et un certificat avec une clé publique correspondante dans un fichier de clés Java, vous pouvez exécuter cette commande :

   - `chemin_install_ab/jre/bin/keytool -genkeypair -keystore chemin_fichier_clés -storepass motdepasse_magasin_clés -alias alias_magasin_clés -dname "CN=nom_commun, OU=unité_organisationnelle, L=ville_ou_région, ST=état_ou_province, C=pays" -keypass motdepasse_clé`

   Où :

   - *chemin_install_ab* correspond à l'emplacement d'installation d'Agent Builder
   - *chemin_fichier_clés* correspond au chemin d'accès vers un magasin de clés JKS existant ou vers l'emplacement où un magasin de clés JKS sera créé
   - *motdepasse_magasin_clés* correspond au mot de passe nécessaire pour accéder aux éléments de ce magasin de clés
   - *alias_magasin_clés* correspond à un nom qui identifie cette clé au sein du magasin de clés (valeur par défaut : `"mykey"`)
   - *motdepasse_clé* correspond au mot de passe nécessaire pour accéder à cette clé (valeur par défaut : `motdepasse_magasin_clés`)

   Insérez ce certificat dans le magasin de clés du serveur.

8. Cliquez sur **Terminer**.

Installation du package dans un environnement IBM Tivoli Monitoring
Pour tester ou utiliser l'agent dans l'environnement IBM Tivoli Monitoring, utilisez le package généré pour installer l'agent sur les systèmes contrôlés, les systèmes Monitoring Server concentrateurs et le système Portal Server.

Avant de commencer
Avant d'installer l'agent sur un système contrôlé, veillez à ce que l'agent de système d'exploitation Tivoli Monitoring soit présent et qu'il fonctionne. Pour plus d'informations sur l'installation d'agents Tivoli Monitoring, voir Installation d'agents de surveillance dans le Tivoli Monitoring Knowledge Center.

Important : Pour afficher les informations d'agent dans Tivoli Enterprise Portal, vous devez installer les composants suivants :

- L'agent sur tous les systèmes contrôlés
- Les fichiers de support Tivoli Enterprise Monitoring Server sur les serveurs Tivoli Enterprise Monitoring Servers concentrateurs
- Les fichiers de support Tivoli Enterprise Portal Server sur Tivoli Enterprise Portal Server
- Les fichiers de support Tivoli Enterprise Portal Server sur Tivoli Enterprise Portal Server et, le cas échéant, les clients bureautiques Tivoli Enterprise Portal

Procédure

1. Copiez le fichier compressé, appelé par défaut *code_produit*`.zip` pour les systèmes Windows et *code_produit*`.tgz` pour les systèmes UNIX et Linux, dans le système où vous souhaitez installer l'agent.

2. Extrayez le fichier dans un emplacement temporaire.

   Remarque : Linux AIX Pour les systèmes UNIX et Linux, cet emplacement temporaire ne doit pas être `/tmp/code_produit`, où le code produit est en minuscules.

   Vous pouvez installer l'agent à distance à l'aide du fichier compressé.

   - Linux Sur un système Linux, utilisez la commande suivante pour extraire le fichier `.tgz` :

     ```
     tar -xvzf nomfichier
     ```

   - UNIX Sur un système AIX, utilisez la commande suivante pour extraire le fichier `.tgz` :

     ```
     gunzip nomfichier
     tar -xvf nomfichier
     ```

3. Exécutez le script d'installation approprié.

   - Pour installer en même temps l'agent, Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server et le support de Tivoli Enterprise Portal :

     ```
     InstallIra.bat/.sh emplacement_installation_itm [[-h nomhôte_TEMS_concentrateur] -u
     nomutilisateur_TEMS_concentrateur -p motdepasse_TEMS_concentrateur]
     ```

   - Pour installer l'agent sans installer les fichiers d'assistance :

     ```
     installIraAgent.bat/.sh emplacement_installation_itm
     ```

   - Pour installer le support de Tivoli Enterprise Monitoring Server, procédez comme suit :

     ```
     installIraAgentTEMS.bat/.sh emplacement_installation_itm [[-h nomhôte_TEMS_concentrateur]
     -u
     nomutilisateur_TEMS_concentrateur -p motdepasse_TEMS_concentrateur]
     ```

   - Pour installer Tivoli Enterprise Portal Server et le support de Tivoli Enterprise Portal :

     ```
     installIraAgentTEPS.bat/.sh emplacement_installation_itm
     ```

   L'emplacement d'installation, *emplacement_installation_itm*, doit correspondre au premier argument et est obligatoire pour tous les scripts : `installIra.bat/.sh`, `installIraAgent.bat/.sh`, `installIraAgentTEMS.bat/.sh` et `installIraAgentTEPS.bat/.sh`. Il s'agit de l'emplacement où les composants Tivoli Monitoring sont installés sur ce système.

   Les autres arguments sont facultatifs.

   Si vous installez des fichiers de support Monitoring Server et qu'aucun ID utilisateur n'est indiqué, Tivoli Enterprise Monitoring Server est recyclé.

4. Configurez et démarrez l'agent en suivant les instructions indiquées dans «Configuration et démarrage de l'agent dans un environnement IBM Tivoli Monitoring», à la page 1434.

Que faire ensuite

si vous avez apporté à la présentation de votre agent des modifications qui entraînent le déplacement ou la suppression des éléments du navigateur, redémarrez Tivoli Enterprise Portal Server et Tivoli Enterprise Portal. Le redémarrage garantit que vos modifications soient correctement reconnues.

Configuration et démarrage de l'agent dans un environnement IBM Tivoli Monitoring

Après avoir installé un agent sur un système contrôlé dans un environnement IBM Tivoli Monitoring, configurez l'agent et démarrez-le.

Procédure

1. Ouvrez la fenêtre **Gérer les services Tivoli Monitoring**.

   La nouvelle entrée **Monitoring Agent for *nom_agent*** est affichée.

2. Cliquez avec le bouton droit de la souris sur l'entrée, puis sélectionnez **Configurer avec les valeurs par défaut**. Cliquez sur le bouton **OK** pour accepter les valeurs par défaut si vous y êtes invité.

   Important :

   a. Sur les systèmes UNIX, sélectionnez l'option **Configurer**.

   b. Dans le cas des agents à plusieurs instances, lors de la configuration, vous êtes invité à indiquer un nom d'instance.

   Conseil : Si votre agent utilise une source de données JMX pour se connecter à un serveur WebSphere Application Server distant, assurez-vous que WebSphere Application Server est également installé sur l'hôte exécutant l'agent, puis associez le paramètre `Java Home` à l'environnement d'exécution Java utilisé par le serveur WebSphere Application Server local.

   Conseil : Pour une source de données SOAP, HTTP, JMX, JDBC ou API Java, vous pouvez utiliser le paramètre **Java** > **Arguments JVM** pour contrôler la consignation des traces d'agent. Définissez la valeur suivante dans ce paramètre :

   ```
   -DJAVA_TRACE_MAX_FILES=fichiers -DJAVA_TRACE_MAX_FILE_SIZE=taille
   ```

   où *fichiers* correspond au nombre maximal de fichiers journaux de trace conservés (valeur par défaut = 4) et *taille* correspond à la taille maximale des fichiers journaux en ko (valeur par défaut = 5 000). Par exemple, vous pouvez définir la valeur suivante :

   ```
   -DJAVA_TRACE_MAX_FILES=7 -DJAVA_TRACE_MAX_FILE_SIZE=100
   ```

   L'agent écrit alors 100 kilooctets dans le premier fichier journal, puis passe au second fichier journal, et ainsi de suite. Après avoir écrit sept fichiers journaux de 100 kilooctets chacun, l'agent écrase le premier fichier journal.

   Si vous avez ajouté des éléments de configuration d'exécution à votre agent ou si vous avez sélectionné une source de données, vous voyez apparaître des panneaux de configuration. Ils permettent de collecter les informations nécessaires pour votre agent.

3. Cliquez avec le bouton droit de la souris sur l'entrée d'agent, puis sélectionnez **Démarrer**.
4. Ouvrez Tivoli Enterprise Portal et naviguez jusqu'au nouvel agent.

Installation et utilisation d'un agent dans un environnement IBM Cloud Application Performance Management

Pour tester ou utiliser l'agent dans l'environnement IBM Cloud Application Performance Management, utilisez le package généré pour installer l'agent sur tous les systèmes contrôlés. Dans certains cas, vous devez configurer l'agent pour pouvoir le démarrer. Vous pouvez démarrer et arrêter l'agent en fonction des besoins.

Installation de l'agent

Utilisez le module d'installation préparé par Agent Builder pour installer l'agent sur tous les systèmes surveillés.

Avant de commencer

Veillez à ce qu'un agent pour IBM Cloud Application Performance Management, en règle générale l'agent de système d'exploitation, se trouve déjà sur le système contrôlé et qu'il fonctionne.

Windows Sur les systèmes Windows, utilisez un interpréteur de commandes de ligne de commande d'administration pour installer et configurer des agents. Pour démarrer un interpréteur de commandes d'administration, sélectionnez **Invite de commandes** dans le menu des programmes Windows, cliquez avec le bouton droit de la souris, puis cliquez sur **Exécuter en tant qu'administrateur**.

Procédure

1. Extrayez le package dans le répertoire temporaire et utilisez ce répertoire.
2. Installez l'agent à l'aide de la commande suivante, en fonction de votre système d'exploitation :

- Windows Sur les systèmes Windows, `installIraAgent.bat` *`emplacement_install_agent`*
- Linux AIX Sur les systèmes Linux et UNIX, `./installIraAgent.sh` *`emplacement_install_agent`*

Où *emplacement_install_agent* correspond à l'emplacement d'installation de l'agent existant. L'emplacement par défaut est le suivant :

- Windows Sur les systèmes Windows, `C:\IBM\APM`
- Linux Sur les systèmes Linux, `/opt/ibm/apm/agent`
- AIX Sur les systèmes AIX, `/opt/ibm/apm/agent`

Important : Si vous avez ajouté des propriétés de configuration personnalisées dans la fenêtre **Runtime Configuration** d'Agent Editor, si l'agent prend en charge plusieurs instances ou si l'agent utilise une source de données prédéfinie devant être configurée (par exemple, un ID utilisateur et un mot de passe), vous devez configurer l'agent avant de pouvoir le démarrer. Si un agent n'a pas besoin d'être configuré, il démarre automatiquement une fois installé.

Configuration de l'agent

Si vous avez ajouté des propriétés de configuration personnalisée dans la fenêtre Runtime Configuration de l'éditeur d'agent, si l'agent prend en charge plusieurs instances, ou si l'agent utilise une source de données prédéfinie qui a besoin d'être configurée (par exemple, un ID utilisateur et un mot de passe), vous devez configurer l'agent avant de pouvoir le démarrer.

Avant de commencer

Windows Sur les systèmes Windows, utilisez un interpréteur de commandes de ligne de commande d'administration pour installer et configurer des agents. Pour démarrer un interpréteur de commandes d'administration, sélectionnez **Invite de commandes** dans le menu des programmes Windows, cliquez avec le bouton droit de la souris, puis cliquez sur **Exécuter en tant qu'administrateur**.

Pourquoi et quand exécuter cette tâche

Au cours du processus de configuration, vous pouvez :

- Définir le nom de l'instance pour créer ou modifier une instance, si l'agent prend en charge plusieurs instances.
- Définir des propriétés de configuration disponibles pour l'agent.
- Créer et configurer des sous-noeuds, si l'agent peut les prendre en charge.

Windows Sur les systèmes Windows, pour définir des propriétés de configuration ou créer des sous-noeuds, vous devez utiliser la procédure de configuration en mode silencieux. Vous trouverez un exemple de fichier de réponses de configuration en mode silencieux (*nomagent*`_silent_config.txt`) dans le répertoire *rép_install*`\samples`. Créez une copie de ce fichier et définissez les variables de configuration selon les besoins.

Linux AIX Sur les systèmes Linux et UNIX, vous pouvez éventuellement utiliser la procédure de configuration en mode silencieux. Vous pouvez également utiliser la procédure interactive. Si vous démarrez la commande de configuration sans indiquer le nom du fichier de réponses, l'utilitaire de configuration vous invitera à indiquer les valeurs de configuration.

Procédure

1. Accédez au répertoire *rép_install*`/bin`.
2. Exécutez la commande suivante pour configurer l'agent :
   - Si l'agent ne prend pas en charge plusieurs instances :
     - Windows Sur les systèmes Windows, *nom*`-agent.bat config [`*fichiers_réponses*`]`

– Linux AIX Sur les systèmes Linux et UNIX, `./nom-agent.sh config [fichier_réponses]`

- Si l'agent prend en charge plusieurs instances :
  – Windows Sur les systèmes Windows, `nom-agent.bat config nom_instance [fichier_réponses]`
  – Linux AIX Sur les systèmes Linux et UNIX, `./nom-agent.sh config nom_instance [fichier_réponses]`

Où :

- *nom_instance* correspond au nom de l'instance. Si aucune instance ne porte ce nom, l'instance est alors créée. Si elle existe déjà, l'instance est reconfigurée. Vous devez créer au moins une instance pour pouvoir utiliser l'agent.
- *fichier_réponses* correspond au fichier de réponses de configuration en mode silencieux.

Conseil : Si votre agent utilise une source de données JMX pour se connecter à un serveur WebSphere Application Server distant, assurez-vous que WebSphere Application Server est également installé sur l'hôte exécutant l'agent, puis associez le paramètre `Java Home` à l'environnement d'exécution Java utilisé par le serveur WebSphere Application Server local.

Conseil : Pour une source de données SOAP, HTTP, JMX, JDBC ou API Java, vous pouvez utiliser le paramètre **Java** > **Arguments JVM** pour contrôler la consignation des traces d'agent. Définissez la valeur suivante dans ce paramètre :

```
-DJAVA_TRACE_MAX_FILES=fichiers -DJAVA_TRACE_MAX_FILE_SIZE=taille
```

où *fichiers* correspond au nombre maximal de fichiers journaux de trace conservés (valeur par défaut = 4) et *taille* correspond à la taille maximale des fichiers journaux en ko (valeur par défaut = 5 000). Par exemple, vous pouvez définir la valeur suivante :

```
-DJAVA_TRACE_MAX_FILES=7 -DJAVA_TRACE_MAX_FILE_SIZE=100
```

L'agent écrit alors 100 kilooctets dans le premier fichier journal, puis passe au second fichier journal, et ainsi de suite. Après avoir écrit sept fichiers journaux de 100 kilooctets chacun, l'agent écrase le premier fichier journal.

Démarrage et arrêt de l'agent

Pour surveiller un système, assurez-vous que l'agent est démarré sur le système. Vous pouvez démarrer et arrêter l'agent à tout moment. Si l'agent prend en charge plusieurs instances, vous pouvez démarrer et arrêter chaque instance indépendamment.

Procédure

1. Accédez au répertoire `rép_install/bin`.
2. Exécutez la commande suivante pour démarrer l'agent :
   - Si l'agent ne prend pas en charge plusieurs instances :
     – Windows Sur les systèmes Windows, `nom-agent.bat start`
     – Linux AIX Sur les systèmes Linux et UNIX, `./nom-agent.sh start`
   - Si l'agent prend en charge plusieurs instances :
     – Windows Sur les systèmes Windows, `nom-agent.bat start nom_instance`
     – Linux AIX Sur les systèmes Linux et UNIX, `./nom-agent.sh start nom_instance`
3. Exécutez la commande suivante pour arrêter l'agent :
   - Si l'agent ne prend pas en charge plusieurs instances :

  - Windows Sur les systèmes Windows, *nom*`-agent.bat stop`
  - Linux AIX Sur les systèmes Linux et UNIX, `./`*nom*`-agent.sh stop`
- Si l'agent prend en charge plusieurs instances :
  - Windows Sur les systèmes Windows, *nom*`-agent.bat stop` *nom_instance*
  - Linux AIX Sur les systèmes Linux et UNIX, `./`*nom*`-agent.sh stop` *nom_instance*

Agent de post-génération et résultats de l'installation

L'installation d'un agent Agent Builder crée et modifie certains fichiers de votre système. Dans un environnement IBM Tivoli Monitoring, vous pouvez également visualiser les modifications dans Tivoli Enterprise Portal.

Nouveaux fichiers sur votre système

Après avoir généré et installé l'agent que vous avez créé avec Agent Builder, vous pouvez voir les nouveaux fichiers suivants sur votre système d'agents :

Remarque : *xx* désigne le code produit à deux caractères.

Windows

Systèmes Windows :

TMAITM6\k*xx*agent.exe
Fichier binaire de l'agent

TMAITM6\K*xx*ENV
Paramètres des variables d'environnement

TMAITM6\K*xx*.ref
Configuration du fournisseur d'agent

TMAITM6\SQLLIB\k*xx*.his
Description SQL des informations d'attribut de l'agent

TMAITM6\SQLLIB\k*xx*.atr
Informations d'attribut de l'agent

TMAITM6*xx*_dd_*version*.xmll
Description du produit

TMAITM6*xx*_dd.properties
Nom du produit

TMAITM6\kxxcma.ini
Fichier de définition de service d'agent

TMAITM6*your files*
Fichiers supplémentaires inclus à partir de l'API Java ou des sources de données du socket avec un type de fichier *Exécutable* ou *Bibliothèque*. Scripts inclus à partir des sources de données de code retour de commande ou de script.

Linux AIX

Systèmes UNIX/Linux :

registre/*xx*architecture.ver
Versions internes et fichier prérequis

***architecture*/*xx*/bin/*xx*_dd_*version*.xml**
Description du produit

***architecture*/*xx*/bin/k*xx*agent**
Fichier binaire de l'agent

***architecture*/*xx*/bin/*xx*_dd.properties**
Nom du produit

***architecture*/*xx*/work/k*xx*.ref**
Configuration du fournisseur d'agent

***architecture*/*xx*/tables/ATTRLIB/k*xx*.atr**
Informations d'attribut de l'agent

***architecture*/*xx*/hist/k*xx*.his**
Description SQL des informations d'attribut de l'agent

architecture*/*xx*/bin/*your files
Fichiers supplémentaires inclus à partir de l'API Java ou des sources de données du socket avec un type de fichier *exécutable*. Scripts inclus à partir des sources de données de code retour de commande ou de script.

architecture*/*xx*/lib/*vos fichiers
Fichiers supplémentaires inclus à partir de l'API Java ou des sources de données du socket avec un type de fichier bibliothèque.

config/.*xx*.rc
Fichier d'installation interne

config/*xx*.environment
Variables d'environnement

config/*xx*_dd_*version*.xml
Description du produit

config/*xx*_dd.properties
Nom du produit

config/.ConfigData/k*xx*env
Paramètres des variables d'environnement

Remarque : Exécutez la commande suivante pour déterminer l'architecture du système :

```
cinfo -p xx
```

où *xx* désigne le code produit à deux caractères.

Par exemple, pour un système Solaris 8 64 bits qui exécute un agent dont le code produit est 19, voici la sortie obtenue :

```
# /opt/ibm/apm/agent/bin/cinfo -p 19

*********** Fri Aug 17 11:23:58 EDT 2007 ******************
User : root Group: other
Host name : guadalajara  Installer Lvl:06.20.00.00
CandleHome: /opt/IBM/ITM
***********************************************************
Platform codes:
sol286 : Current machine
sol286 : Product (19)
tmaitm6/sol286 : CT Framework (ax)
```

Examinez la ligne en gras. La chaîne située avant le signe deux-points, `sol286`, désigne l'architecture utilisée pour cet agent. Cette chaîne diffère selon les associations de systèmes d'exploitation et de type de matériel. Pour activer cette fonction, l'agent doit déjà être installé.

Les fichiers suivants sont destinés aux sources de données Java. Ils ne sont créés que si l'agent contient des sources de données JMX, JDBC, HTTP ou SOAP :

- `cpci.jar`
- `jlog.jar`
- `common/jatlib-1.0.jar`

Les fichiers suivants sont destinés au support d'exécution JMX. Ils ne sont créés que si l'agent contient des sources de données JMX :

- `common/jmx-1.0.jar`
- `common/connectors/jboss/connJboss-1.0.jar`
- `common/connectors/jsr160/connJSR160-1.0.jar`
- `common/connectors/was/connWas-1.0.jar`
- `common/connectors/weblogic/connWeblogic-1.0.jar`

Le fichier suivant est destiné au support d'exécution JDBC. Ces fichiers ne sont créés que si l'agent contient des sources de données JDBC :

- `common/jdbc-1.0.jar`

Le fichier suivants est destiné au support d'exécution HTTP ou SOAP. Ces fichiers ne sont créés que si l'agent contient des sources de données HTTP ou SOAP :

- `http-1.0.jar`

Les fichiers suivants sont destinés au support d'exécution de l'interface de programme d'application Java. Ils ne sont créés que si l'agent contient des sources de données d'interface de programme d'application Java :

- `cpci.jar`
- `custom/`*`votre fichier JAR`* Le nom de ce fichier JAR est indiqué dans les **Paramètres globaux** d'une source de données d'interface de programme d'application Java.
- `custom/`*`votre fichier JAR`* Fichiers supplémentaires avec un type de fichier de ressources Java.

Les fichiers sont identiques sur les systèmes Windows, UNIX et Linux pour les sources de données Java, mais ils se trouvent dans des répertoires différents :

- Windows Chemin Windows : `TMAITM6\kxx\jars`
- Linux AIX Chemin UNIX/Linux : *`architecture`*`/`*`xx`*`/jars`

Les fichiers suivants sont destinés au support d'exécution de la surveillance des fichiers journaux. Ils ne sont créés que si l'agent contient des sources de données de fichiers journaux :

- Windows Sur les systèmes Windows : TMAITM6\kxxudp.dll
- Linux Sur les systèmes Solaris/Linux : *architecture*/*xx*/lib/libkxxudp.so
- Sur les systèmes HP-UX : *architecture*/*xx*/lib/libkxxudp.sl
- UNIX Sur les systèmes AIX : *architecture*/*xx*/lib/libkxxudp.a

Les fichiers suivants sont destinés au support d'exécution de la surveillance des scripts SSH. Ils ne sont créés que si l'agent contient une source de données de script activée pour la collecte de données SSH :

- Windows Sur les systèmes Windows : `TMAITM6\kxxssh.dll`
- Linux Sur les systèmes Solaris/Linux : *`architecture`*`/`*`xx`*`/lib/libkxxssh.so`
- Sur les systèmes HP-UX : *`architecture`*`/`*`xx`*`/lib/libkxxssh.sl`
- UNIX Sur les systèmes AIX : *`architecture`*`/`*`xx`*`/lib/libkxxssh.a`

Modifications dans la fenêtre Gérer les services Tivoli Enterprise Monitoring

Après l'installation d'un agent dans un environnement IBM Tivoli Monitoring, une entrée pour l'agent apparaît dans la fenêtre **Gérer les services Tivoli Monitoring**. Cette entrée est intitulée **Monitoring Agent for *nom_agent***.

Important : Gérer les services Tivoli Enterprise Monitoring n'est pas pris en charge dans l'environnement IBM Cloud Application Performance Management.

Windows Sur les systèmes Windows, cette entrée contient une colonne **Tâche/Sous-système** qui détermine si votre agent prend en charge plusieurs instances :

- Un agent à instance unique affiche une nouvelle application dans la fenêtre **Gérer les services Tivoli Enterprise Monitoring**. Cette application est intitulée **Monitoring Agent for *nom_agent***. Un service est créé pour l'agent (Figure 70, à la page 1441). La colonne **Tâche/Sous-système** contient la valeur **Principale**.
- Un agent multi-instance affiche un nouveau modèle d'application dans la fenêtre **Gérer les services Tivoli Enterprise Monitoring**. Ce modèle est intitulé **Monitoring Agent for *nom_agent***. Aucun service n'est créé pour l'agent tant que vous n'avez pas créé d'instance de l'agent à partir de ce modèle. La colonne **Tâche/Sous-système** contient la valeur **Modèle** pour indiquer que cette entrée est un modèle servant à créer des instances de l'agent.

Linux AIX Sur les systèmes Linux et UNIX, l'entrée associée à l'agent est identique, que votre agent prenne en charge plusieurs instances, ou non.

Remarque : Les captures d'écran suivantes s'appliquent à un système Windows. Les systèmes UNIX et Linux sont dotés d'écrans similaires.

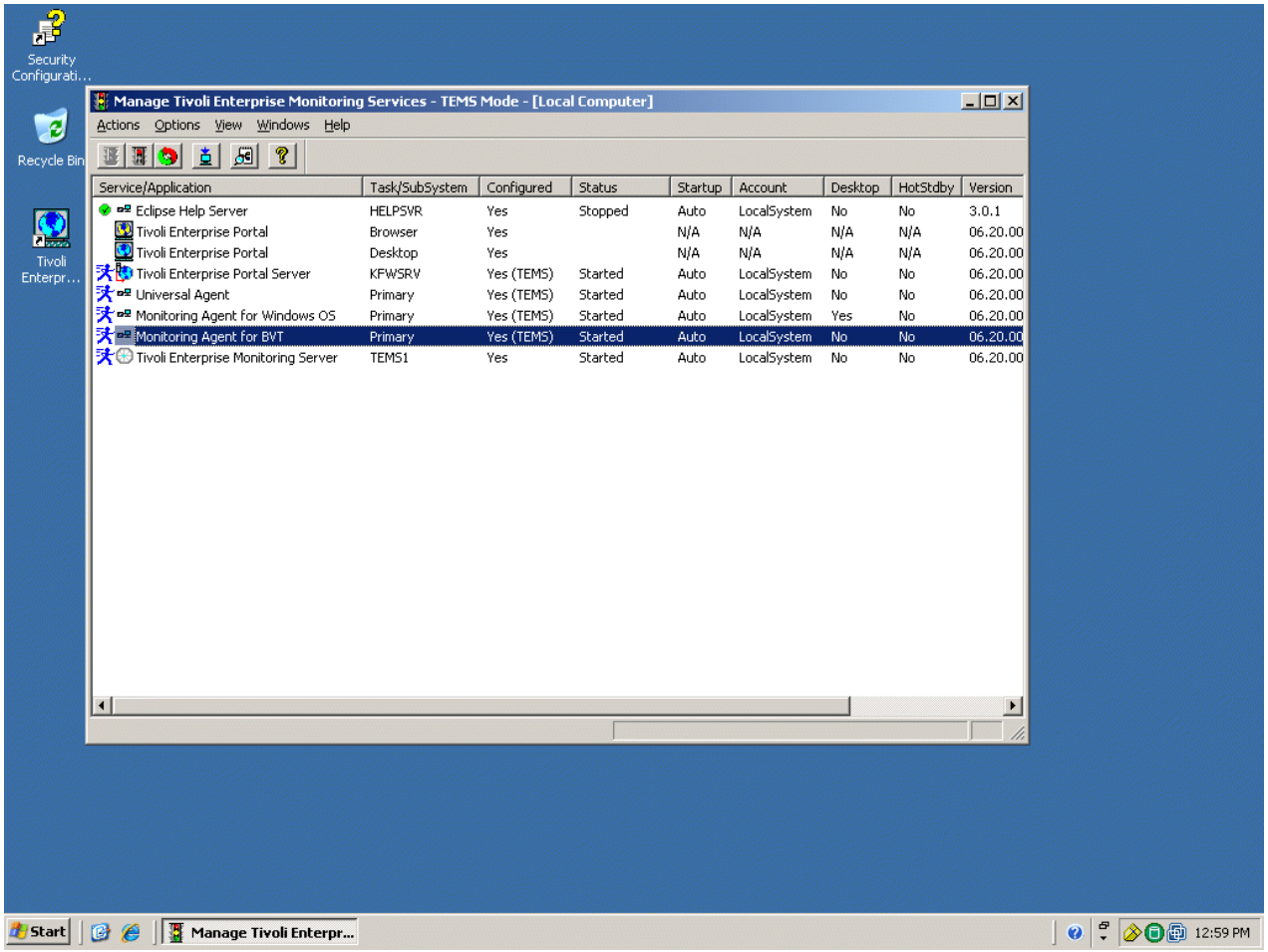


Figure 70. Fenêtre Gérer les services Tivoli Enterprise Monitoring

Modifications dans Tivoli Enterprise Portal

Dans un environnement IBM Tivoli Monitoring, après avoir installé et démarré l'agent, cliquez sur l'icône **Régénérer** de couleur verte dans Tivoli Enterprise Portal. Vous pouvez alors afficher le nouvel agent. Les modifications suivantes s'affichent sur le portail :

- Un nouveau sous-noeud pour l'agent dans la vue physique de Tivoli Enterprise Portal.
- Des noeuds pour chacun des groupes de navigation et une source de données que vous avez définie à l'aide d'Agent Builder (Figure 71, à la page 1442).

  Remarque : pour chaque élément du navigateur, vous devez définir une requête par défaut.

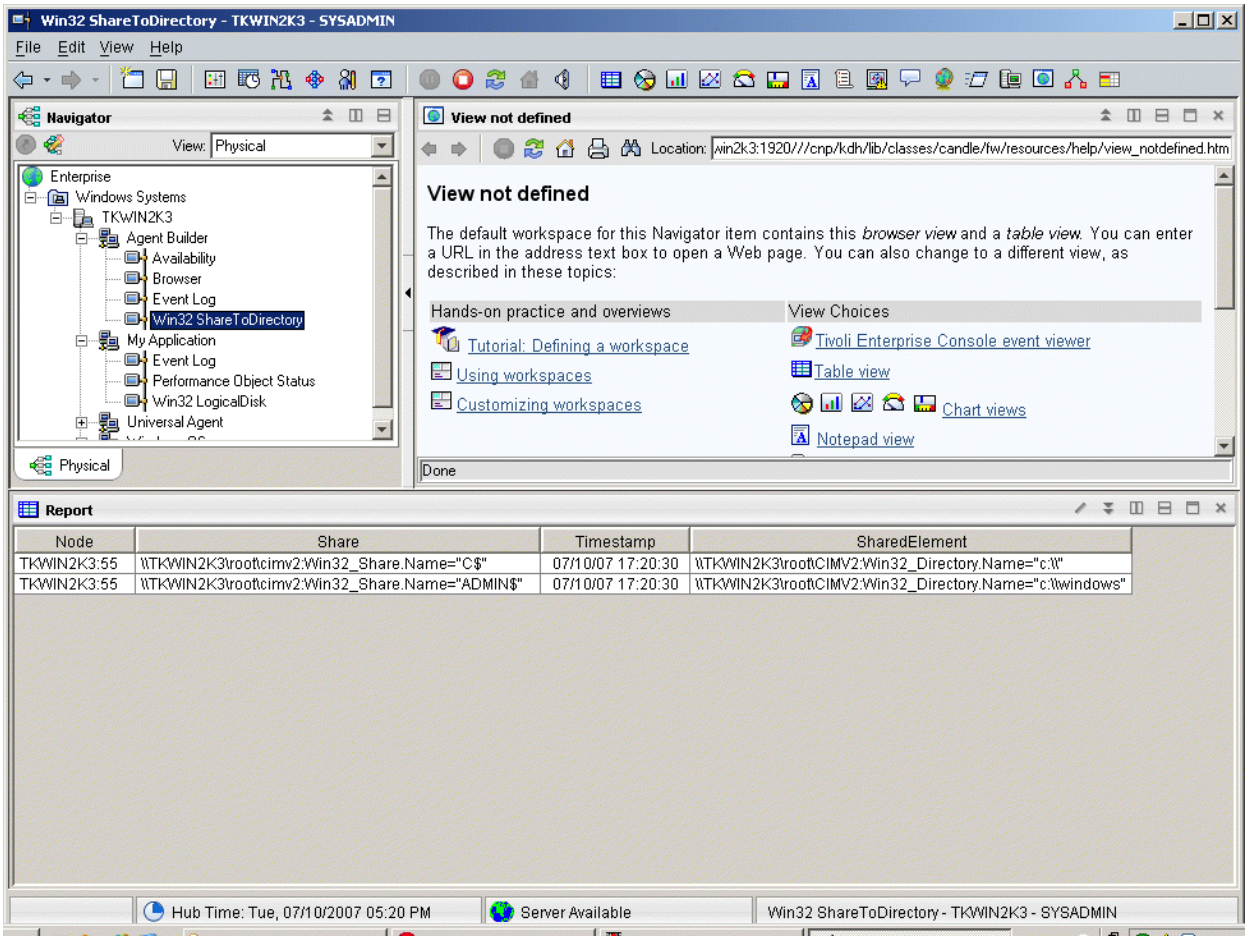


Figure 71. Noeuds des groupes d'attributs dans le nouvel agent.

- Si votre agent contient des sous-noeuds, un noeud extensible pour chaque sous-noeud est défini dans l'agent. Les noeuds suivants apparaissent sous le noeud extensible :
  - Statut de l'objet de performances xxx, où xxx représente le type de sous-noeud à trois lettres
  - Des noeuds pour chacun des groupes de navigation et sources de données que vous avez définis dans le sous-noeud
  - Noeud du journal des événements xxx si vous avez des journaux d'événements
  - Noeud des contrôleurs JMX xxx si vous disposez de JMX et que vous avez inclus des contrôleurs JMX
- Le noeud automatique suivant :
  - Un noeud de disponibilité, si votre agent contient une source de données de disponibilité (Figure 72, à la page 1443)

    Remarque : Le comportement de ce noeud varie selon le contenu de l'agent. Si l'agent ne surveille que la disponibilité, le noeud de disponibilité représente la source de données de disponibilité. S'il surveille la disponibilité et les performances, le noeud de disponibilité devient l'élément de navigateur qui représente la source de données de disponibilité et la source de données du statut de l'objet de performances.

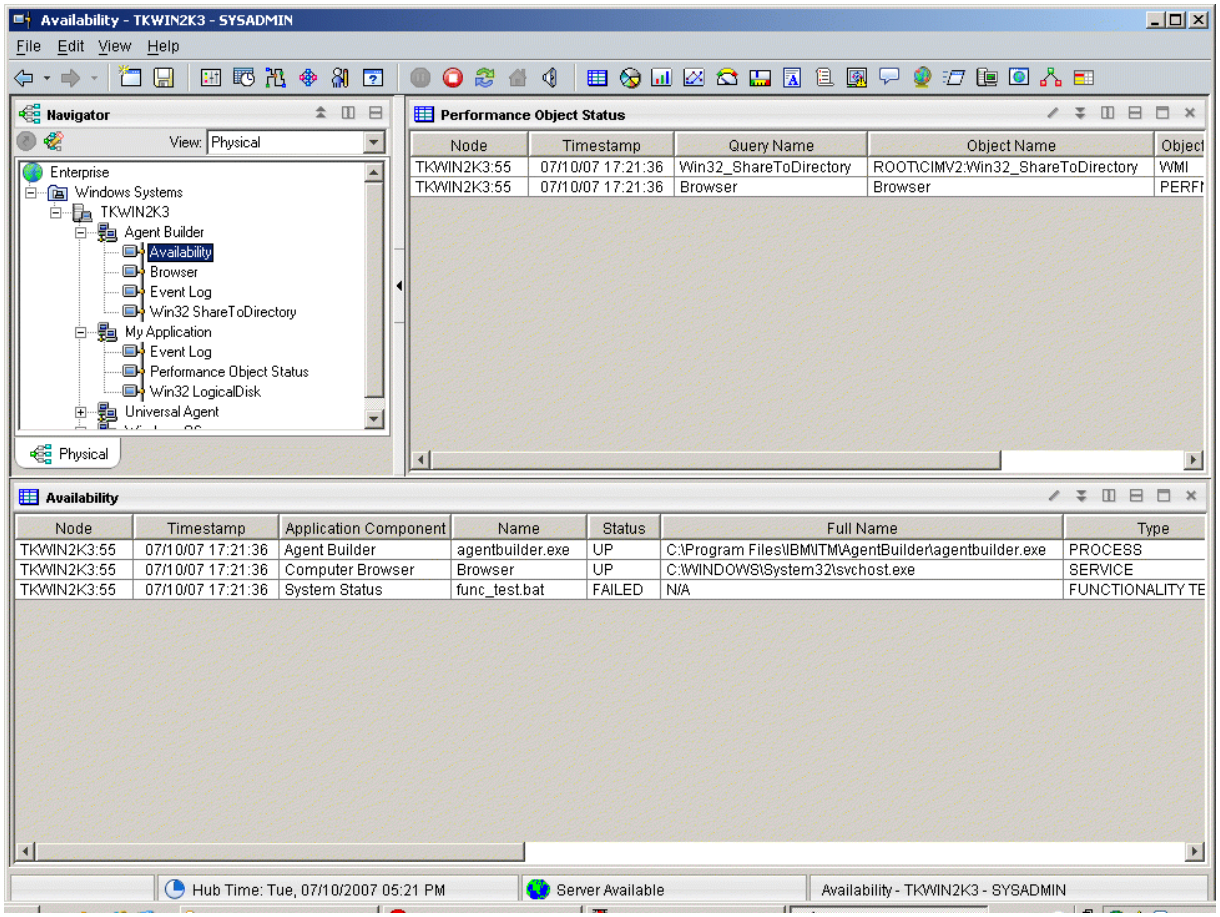


Figure 72. Noeud de disponibilité

– Statut des objets de performances, si l'agent intègre les sources de données de surveillance des performances (et non de disponibilité) (Figure 73, à la page 1444)

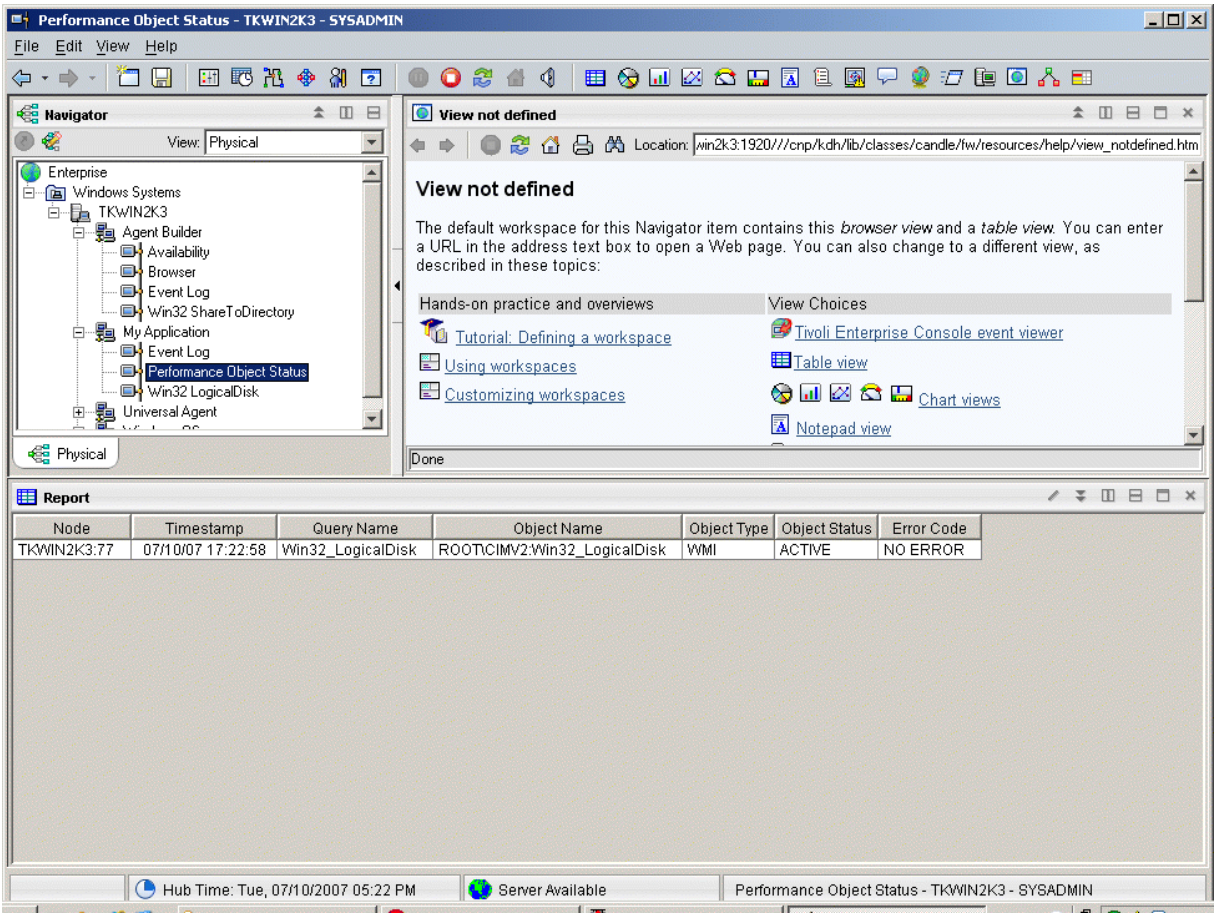


Figure 73. Noeud de statut d'objet de performances

– Journal des événements si l'agent contient des sources de données générant des données de journal (Figure 74, à la page 1445)

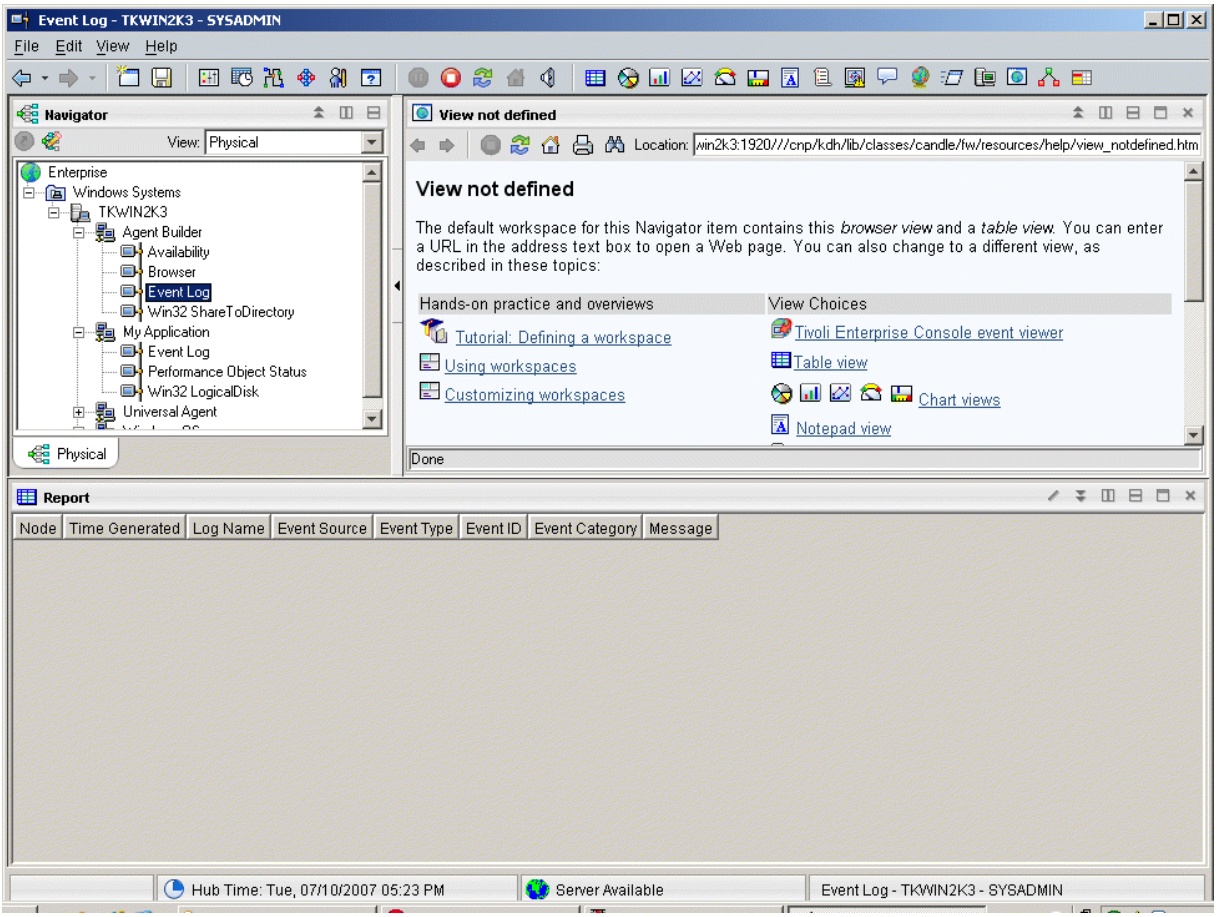


Figure 74. Noeud du journal des événements

Voir «Guide de référence des attributs», à la page 1461 pour consulter les descriptions des groupes d'attributs et des attributs d'Agent Builder.

Désinstallation d'un agent

Vous pouvez supprimer un agent généré par Agent Builder d'un hôte surveillé.

Pourquoi et quand exécuter cette tâche

Le processus de désinstallation désinstalle uniquement l'agent du système où il était installé. Ce processus ne désinstalle aucun autre agent et aucune autre infrastructure de surveillance.

Dans un environnement IBM Tivoli Monitoring, vous pouvez utiliser l'une des procédures suivantes pour supprimer un agent généré par Agent Builder :

- «Suppression d'un agent Tivoli Monitoring via Tivoli Enterprise Portal», à la page 1446
- «Suppression d'un agent Tivoli Monitoring sans Tivoli Enterprise Portal», à la page 1446

Après avoir supprimé l'agent à l'aide de l'une de ces procédures, effacez-le de Tivoli Enterprise Portal en suivant la procédure «Suppression d'un agent Tivoli Monitoring de Tivoli Enterprise Portal», à la page 1446.

Dans un environnement IBM Cloud Application Performance Management, suivez la procédure «Désinstallation d'un agent IBM Cloud Application Performance Management», à la page 1447.

Suppression d'un agent Tivoli Monitoring via Tivoli Enterprise Portal

Dans un environnement IBM Tivoli Monitoring, vous pouvez utiliser Tivoli Enterprise Portal pour supprimer un agent.

Avant de commencer

Votre agent de système d'exploitation doit être en cours d'exécution pour que l'agent créé puisse être supprimé.

Procédure

Pour utiliser Tivoli Enterprise Portal pour supprimer un agent, procédez comme suit :

- Dans l'arborescence de navigation Tivoli Enterprise Portal, cliquez avec le bouton droit de la souris sur l'agent et sélectionnez **Supprimer**.

Suppression d'un agent Tivoli Monitoring sans Tivoli Enterprise Portal

Si votre environnement IBM Tivoli Monitoring ne dispose pas de Tivoli Enterprise Portal, vous pouvez utiliser les scripts et les commandes du système d'exploitation pour supprimer un agent.

Procédure

Pour supprimer un agent qu'Agent Builder a généré à partir du système cible, mais que vous ne disposez pas de Tivoli Enterprise Portal, vous pouvez effectuer l'une des étapes suivantes :

- Windows

  Sur les systèmes Windows, utilisez les commandes :

  ```
  cd ITM_INSTALL/TMAITM6
  kxx_uninstall.vbs ITM_INSTALL
  ```

  où *xx* désigne le code produit de l'agent
- Windows

  Sinon, sur les systèmes Windows, vous pouvez utiliser la commande `cscript.exe` pour exécuter le script de désinstallation. Cette commande est l'analyseur syntaxique d'interface de ligne de commande pour les scripts vbs. L'analyseur n'affiche pas de fenêtre mais un message sur la console :

  ```
  cd ITM_INSTALL/TMAITM6
  cscript.exe kxx_uninstall.vbs ITM_INSTALL
  ```
- Linux AIX

  Sur les systèmes Linux ou UNIX, utilisez le fichier `uninstall.sh` du répertoire *ITM_INSTALL*`/bin`:

  ```
  uninstall.sh [-f] [-i] [-h ITM_INSTALL] [CodePlateforme produit]
  ```

Suppression d'un agent Tivoli Monitoring de Tivoli Enterprise Portal

Dans un environnement IBM Tivoli Monitoring, après la suppression de l'agent, des zones vides concernant des informations issues de l'agent peuvent rester dans Tivoli Enterprise Portal. Pour supprimer ces zones, supprimez l'agent dans Tivoli Enterprise Portal.

Procédure

1. Vérifiez que Tivoli Enterprise Monitoring Server et le serveur Tivoli Enterprise Portal sont actifs et en cours d'exécution.
2. Connectez-vous à votre client Tivoli Enterprise Portal.
3. Dans la vue du navigateur physique du client Tivoli Enterprise Portal, cliquez avec le bouton droit de la souris sur **Enterprise** et sélectionnez **Espace de travail** > **Statut du système géré**.

   L'espace de travail Statut du système géré s'affiche.
4. Sélectionnez tous les systèmes IBM Tivoli gérés pour votre agent.

5. Cliquez avec le bouton droit de la souris, puis sélectionnez **Effacer une entrée hors ligne** pour effacer toutes les entrées de cette table.

Désinstallation d'un agent IBM Cloud Application Performance Management
Vous pouvez désinstaller votre agent de n'importe quel système contrôlé dans un environnement IBM Cloud Application Performance Management.

Procédure

1. Sur le système où est installé l'agent, ouvrez une ligne de commande et accédez au répertoire *rép_install*/bin, où *rép_install* représente le répertoire d'installation des agents de surveillance.
2. Pour désinstaller un agent de surveillance spécifique, entrez le nom du script de l'agent et l'option de désinstallation où *nom* représente le nom du script de l'agent :
   - Sur les systèmes Windows, *nom*`-agent.bat uninstall`
   - Sur les systèmes Linux ou AIX, `./`*nom*`-agent.sh uninstall`

Importation des fichiers de prise en charge de l'application

Si un agent doit être utilisé dans un environnement IBM Tivoli Monitoring, les situations personnalisées, espaces de travail, commandes Action et requêtes peuvent être inclus dans le package d'installation.

Pourquoi et quand exécuter cette tâche

Pour disposer d'une seule image d'installation pour les situations, les espaces de travail et l'agent, les fichiers de situation et d'espace de travail doivent se trouver dans le même projet que l'agent. Agent Builder fournit un assistant pour créer les fichiers appropriés dans le projet d'agent.

Les définitions associées à un agent peuvent également être incluses dans le package d'installation. Le contenu de ces définitions diffère pour un agent selon qu'il est utilisé dans un environnement de surveillance d'entreprise ou de surveillance de système. Une image d'agent Tivoli Enterprise Monitoring peut inclure des situations personnalisées, des espaces de travail, des commandes Action et des requêtes. Une image d'agent Tivoli System Monitor peut inclure des situations privées, des définitions d'interruption et des informations de configuration d'agent.

Pour avoir un même package d'installation aussi bien pour les définitions que pour l'agent lui-même, il est nécessaire que les fichiers se trouvent dans le même projet que l'agent. Agent Builder fournit un assistant permettant de créer les fichiers appropriés pour une installation d'agent Tivoli Enterprise Monitoring. Les fichiers destinés à un environnement d'agent de surveillance sont créés selon le processus décrit dans le chapitre *Autonomie d'agent* du document *IBM Tivoli Monitoring - Guide d'administration*. Les fichiers résultants sont copiés dans la racine du projet Eclipse de l'agent.

Exportation et importation de fichiers pour les agents Tivoli Enterprise Monitoring

Pourquoi et quand exécuter cette tâche

Après avoir créé vos situations, espaces de travail, requêtes et commandes Action dans Tivoli Enterprise Portal, vous pouvez les exporter et les importer dans un autre environnement Tivoli Monitoring version 6.2. Pour plus d'informations sur la création de situations et d'espaces de travail, voir («Création d'espaces de travail, de commandes Action et de situations», à la page 1411). Procédez comme suit pour extraire les situations, espaces de travail, commandes Actions et requêtes :

Procédure

1. Dans l'onglet **Explorateur de projets**, cliquez avec le bouton droit de la souris sur le dossier du projet d'agent.
2. Sélectionnez **IBM Corporation** > **Importer les fichiers de prise en charge de l'application**.

3. Entrez le nom d'hôte du serveur Tivoli Enterprise Portal.
4. Entrez le nom d'utilisateur et le mot de passe de l'environnement Tivoli Monitoring auquel vous voulez vous connecter, puis cliquez sur **Terminer**.
5. Si vous avez défini des situations pour votre agent, une boîte de dialogue répertoriant les situations définies pour l'agent apparaît.
6. Sélectionnez dans la liste les situations que vous voulez exporter et cliquez sur **<<** pour les ajouter au tableau des situations sélectionnées, puis cliquez sur **OK**.

   L'importation peut prendre quelques minutes. Une fois la tâche terminée, vous voyez les fichiers SQL dans les dossiers appropriés du projet d'agent.
7. Si vous avez défini des commandes Action pour votre agent, une boîte de dialogue présente les commandes Action définies. Sélectionnez dans la liste les commandes Action que vous voulez exporter et cliquez sur **>>** pour les ajouter dans la table des commandes Action sélectionnées, puis cliquez sur **OK**.

   L'importation peut prendre quelques minutes. Une fois la tâche terminée, vous voyez les fichiers SQL dans les dossiers appropriés du projet d'agent.
8. Si vous avez défini des requêtes personnalisées pour votre agent, une boîte de dialogue présente les requêtes définies. Sélectionnez dans la liste les requêtes à exporter et cliquez sur **<<** pour les ajouter à la table des requêtes sélectionnées, puis cliquez sur le bouton **OK**.

   L'importation peut prendre quelques minutes. Une fois la tâche terminée, vous voyez les fichiers SQL dans les dossiers appropriés du projet d'agent. Les espaces de travail sont automatiquement importés.

Que faire ensuite
Re-créez votre agent personnalisé, installez-le sur l'hôte surveillé, puis installez le support Tivoli Enterprise Portal.

Exportation et importation de fichiers pour les agents Tivoli System Monitor

Pourquoi et quand exécuter cette tâche
Les définitions d'agent Tivoli System Monitor sont contenues dans trois types de fichier :

- Les situations privées sont définies dans le fichier *xx*`_situations.xml`, où *xx* est le code produit de deux caractères.
- Les informations de configuration d'alerte sont définies dans un fichier nommé *xx*`_trapcnfg.xml`, *xx* étant le code produit de deux caractères.
- Pour les agents qui nécessitent une configuration, celle-ci est définie dans un fichier pour chaque instance de l'agent. Lorsqu'il s'agit d'un agent à une seule instance, le fichier s'appelle *xx*`.cfg`. Lorsqu'il s'agit d'un agent multi-instance, il existe un fichier pour chaque instance. Les noms de fichier se présentent sous la forme *xx*`_`*nom d'instance*`.cfg`, *xx* étant le code produit à deux caractères et *nom d'instance* le nom de l'instance d'agent.

Procédure

- Créez les fichiers selon le processus décrit dans le chapitre *Autonomie d'agent* du document *IBM Tivoli Monitoring - Guide d'administration*. Copiez manuellement les fichiers à la racine du répertoire du projet ou utilisez la fonction d'importation Eclipse pour sélectionner les fichiers à importer : **Fichier** > **Importer** > **Général** > **Système de fichiers**.

  Ces fichiers seront inclus dans l'image d'agent et installés par le programme d'installation.

  Lorsque l'agent est installé, le programme d'installation :

  – Copie les fichiers inclus vers les emplacements appropriés.
  – Les situations privées définies dans le fichier `pc_situations.xml` sont exécutées sur l'agent.

– Les définitions d'interruption définies dans le fichier `pc_trapcnfg.xml` sont utilisées pour réacheminer des interruptions en fonction des situations.
– L'agent est configuré automatiquement et démarré si :
  - l'agent est un agent d'instance unique sans aucune configuration définie ;
  - L'agent est un agent à une seule instance avec une configuration définie avec l'agent et que l'image contient un fichier `pc.cfg`.
  - L'agent est un agent multi-instance (tous les agents multi-instances nécessitent une configuration) : le programme d'installation démarre une instance de l'agent pour chaque fichier `pc_`*`inst`*`.cfg`.

Filtrage et récapitulatif des événements

Un groupe d'attributs est défini comme *événement pur* ou *échantillonné*. Les groupes d'attributs d'événements purs contiennent des lignes de données exécutées en mode asynchrone. Chaque ligne de données est traitée immédiatement par Tivoli Monitoring dès son arrivée. Les groupes d'attributs échantillonnés collectent l'ensemble actuel de lignes de données chaque fois que les données sont demandées. Les groupes d'attribut suivants illustrent la différence :

- Un groupe d'attributs `SNMPEvent` est créé. Il représente toutes les alertes et informations SNMP envoyés à l'agent. Les alertes ou informations arrivent de manière asynchrone à mesure qu'elles sont envoyées par les systèmes contrôlés. Chaque événement qui arrive est transmis à Tivoli Monitoring.
- Un groupe d'attributs `Disk` est créé pour représenter des informations sur tous les disques d'un système. Les informations sur le disque sont collectées périodiquement. A chaque collecte, l'agent renvoie un certain nombre de lignes de données, une pour chaque disque.

La différence entre les groupes d'attributs événements purs et échantillonnés affectent plusieurs aspects de Tivoli Monitoring. Ces aspects sont les suivants : situations, données d'entrepôts et vues Tivoli Enterprise Portal.

Chaque situation est affectée (ou *distribuée*) à un ou plusieurs systèmes gérés qui sont surveillés pour détecter une condition ou un ensemble de conditions spécifique. Lorsque l'événement doit être déterminé en fonction des observations effectuées à des intervalles spécifiques, il est désigné par *événement échantillonné*. Lorsque son apparition est spontanée, l'événement est considéré comme un *événement pur*. Par conséquent, un intervalle est associé aux situations des événements échantillonnés alors qu'aucun intervalle n'est associé aux situations des événements purs. Une autre caractéristique des événements échantillonnés est le changement potentiel de la condition qui a entraîné l'événement, ce qui signifie qu'elle n'est plus vraie. Les événements purs ne changent pas. Par conséquent, les alertes générées pour des événements échantillonnés peuvent passer de l'état vrai à l'état faux alors qu'un événement pur reste vrai lorsqu'il se produit.

Un exemple d'événement échantillonné est `nombre de processus > 100`. Un événement est considéré vrai lorsque le nombre de processus dépasse 100 et l'événement est à nouveau considéré faux lorsque cette valeur passe en dessous du seuil 100. Une situation qui surveille les `tentatives de connexion non valides de l'utilisateur` est considérée comme un événement pur ; l'événement se produit lorsqu'une tentative de connexion non valide est détectée et il ne devient pas un événement faux. Bien que vous puissiez créer des situations évaluées sur une période spécifique pour des groupes d'attributs échantillonnés, les évaluations ne sont pas possibles pour les groupes d'attributs d'événement pur.

De la même manière, pour des données d'historique, vous pouvez configurer la fréquence de collecte des données échantillonnées. Toutefois, lorsque vous activez la collecte des données d'événements purs, vous pouvez obtenir chaque ligne lorsqu'elle arrive.

Les données échantillonnées affichées dans Tivoli Enterprise Portal correspondent à l'ensemble le plus récent de lignes collectées. Les données affichées pour un groupe d'attributs d'événement pur correspondent au contenu d'un cache local qui est géré par l'agent. Elles ne correspondent pas forcément aux données transmises à Tivoli Monitoring pour l'évaluation des situations et la collecte d'historique.

Contrôle des événements en double

Utilisez les options de filtrage et de récapitulatif des événements pour contrôler la façon dont les événements en double sont envoyés à Tivoli Monitoring.

Avant de commencer

Pour plus d'informations sur le filtrage et le récapitulatif des événements, voir «Filtrage et récapitulatif des événements», à la page 1449.

Pourquoi et quand exécuter cette tâche

Agent Builder définit des groupes d'attributs représentant des données d'événement sous la forme d'*événements purs* dans Tivoli Monitoring. Ces groupes d'attributs incluent Fichier journal, le journal binaire AIX, les groupes Evénements SNMP et Notifications JMX. Ils peuvent générer de nombreux événements en double. Vous pouvez contrôler la manière dont ces événements en double sont envoyés à Tivoli Monitoring. Vous pouvez activer ces contrôles pour les groupes d'attributs Fichier journal, Evénements SNMP et Notifications JMX dans l'onglet **Informations sur les événements** de la page **Propriétés avancées de la source de données** dans la fenêtre **Avancé**.

Le traitement d'un événement en tant que doublon d'autres événements est déterminé par les attributs de clé que vous définissez dans le groupe d'attributs. Un événement se produit si tous les attributs de clé de l'événement correspondent aux valeurs des mêmes attributs de clé d'un événement existant. Lorsque l'option de filtrage d'événement et de récapitulatif est activée, les attributs des fonctions `isSummary`, `occurrenceCount`, `summaryInterval` et `eventThreshold` sont automatiquement ajoutés.

Procédure

- Dans la zone **Options de filtrage et de récapitulatif des événements**, sélectionnez l'une des options suivantes :
  - **Aucun filtrage ou récapitulatif des événements** : Envoie tous les événements sans effectuer d'opération de filtrage d'événement ou de récapitulatif. Cette option est l'option par défaut.
  - **Filtrer et récapituler les événements** : crée un enregistrement récapitulatif pour chaque événement en double et chaque événement unique basé sur des attributs de clé. Permet également de sélectionner l'option de filtrage d'événement. Dans la zone **Options de récapitulatif**, entrez l'intervalle de récapitulatif. Vous pouvez entrer une valeur en secondes ou insérer une propriété de configuration.

    Les options de filtrage d'événement sont les suivantes :

    - **Envoyer uniquement des événements récapitulatifs** : Envoie uniquement les enregistrements récapitulatifs de l'intervalle indiqué.
    - **Envoyer tous les événements** : Envoie tous les événements et les enregistrements récapitulatifs.
    - **Envoyer le premier événement** : Pour chaque événement, envoie uniquement le premier événement reçu au cours de l'intervalle de récapitulatif indiqué et aucun événement en double. Cette option envoie également les enregistrements du récapitulatif.
    - **Seuil d'événements** : Envoie un événement à Tivoli Monitoring lorsque le nombre d'événements en double reçus dans l'intervalle est également divisible par la valeur de seuil. Par exemple, si vous définissez la valeur 5 pour le seuil d'événements et que vous recevez moins de cinq doublons (y compris le premier événement) au cours de l'intervalle, aucun événement n'est envoyé à Tivoli Monitoring. Si vous recevez 5, 6, 7, 8 ou 9 doublons, un événement est envoyé. Si vous recevez 10 doublons, 2 événements sont envoyés. Dans la zone **Seuil d'événements**, vous pouvez entrer un nombre ou insérer une propriété de configuration. Cette option envoie également les enregistrements du récapitulatif.

Affichage des données de filtrage et de récapitulation d'événements dans Tivoli Enterprise Portal

Cette section comporte des exemples qui expliquent la manière dont les données sont traitées en fonction de vos paramètres de filtrage et de récapitulation d'événements.

L'agent gère un cache dans lequel sont stockés les derniers événements reçus. Par défaut, la taille de cette mémoire cache correspond à 100. Si vous activez le filtrage et la récapitulation d'événements pour l'agent, le nombre d'événements dans le cache et le nombre d'événements transmis à IBM Tivoli Monitoring risquent de ne pas être cohérents. Des événements supplémentaires dans le cache risquent de ne pas atteindre le seuil défini pour l'envoi. Le cache peut également contenir moins d'événements si vous avez sélectionné l'option **Envoyer tous les événements**. Avec l'option **Envoyer tous les événements**, un événement est envoyé chaque fois qu'il se produit. Toutefois, une seule copie de l'événement est conservée dans le cache et le compteur d'occurrences est incrémenté chaque fois que l'événement se produit. Pour afficher les événements envoyés à IBM Tivoli Monitoring, vous devez créer une vue d'historique. Pour plus d'informations sur la création de vues d'historique, voir *Historical Reporting* dans le manuel Tivoli Enterprise Portal User's Guide. Vous pouvez comparer cette vue à la vue en temps réel de la mémoire cache dans Tivoli Enterprise Portal. Vous pouvez également utiliser des situations pour effectuer la même comparaison.

Les exemples suivants expliquent comment les données identiques du journal sont traitées en fonction du choix effectué, le cas échéant, pour le filtrage et le récapitulatif des événements. L'exemple d'agent a été créé pour décrire différents comportements. Chaque groupe d'attributs a été défini pour surveiller le même fichier journal. Dans chaque exemple, une vue d'historique et la vue en temps réel (mémoire cache) sont affichées. Les noms des noeuds dans Tivoli Enterprise Portal reflètent les paramètres sélectionnés. Par défaut, la vue d'historique affiche les derniers événements sur les lignes du bas. La vue en temps réel par défaut de la mémoire cache les affiche sur les lignes du haut. Dans ces exemples, la vue d'historique affiche la dernière heure.

Lorsque de nouveaux événements arrivent, ils apparaissent dans la vue de la mémoire cache. S'il s'agit de doublons, les données sont mises à jour sur la ligne existante. Lorsqu'un intervalle de récapitulatif s'écoule, les événements existants sont convertis en événements de récapitulatif avant d'être envoyés. De nouvelles lignes sont ensuite ajoutées pour l'intervalle de récapitulatif suivant.

La (Figure 75, à la page 1452) affiche une vue d'historique et une vue de la mémoire cache si vous n'avez pas activé l'option de filtrage ou de récapitulatif des événements. Les deux vues affichent les mêmes données mais l'ordre d'affichage est inversé. Pour afficher les événements correspondants, la partie inférieure de la vue d'historique et la partie supérieure de la vue en temps réel (cache) sont affichées.

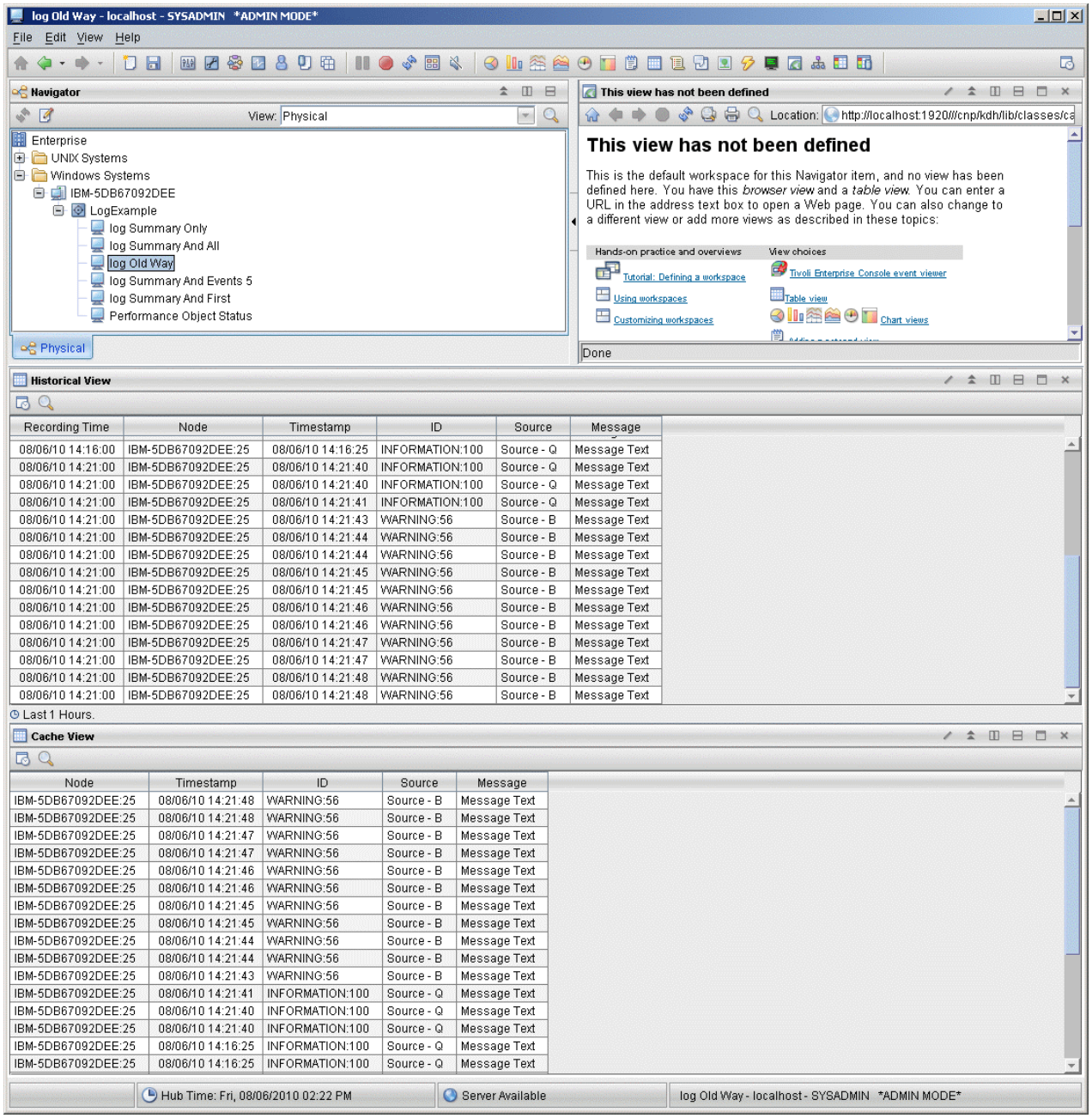


Figure 75. Vue d'historique et vue de la mémoire cache lorsque l'option de filtrage ou de récapitulatif des événements n'est pas activée

La (Figure 76, à la page 1453) affiche la vue d'historique et la vue de la mémoire cache si vous avez sélectionné l'option **Envoyer uniquement les événements** du récapitulatif dans l'onglet **Informations sur les événements**. Les événements du récapitulatif sont affichés dans les deux vues mais les nouveaux événements sont présentés uniquement dans la vue (mémoire cache) en temps réel.

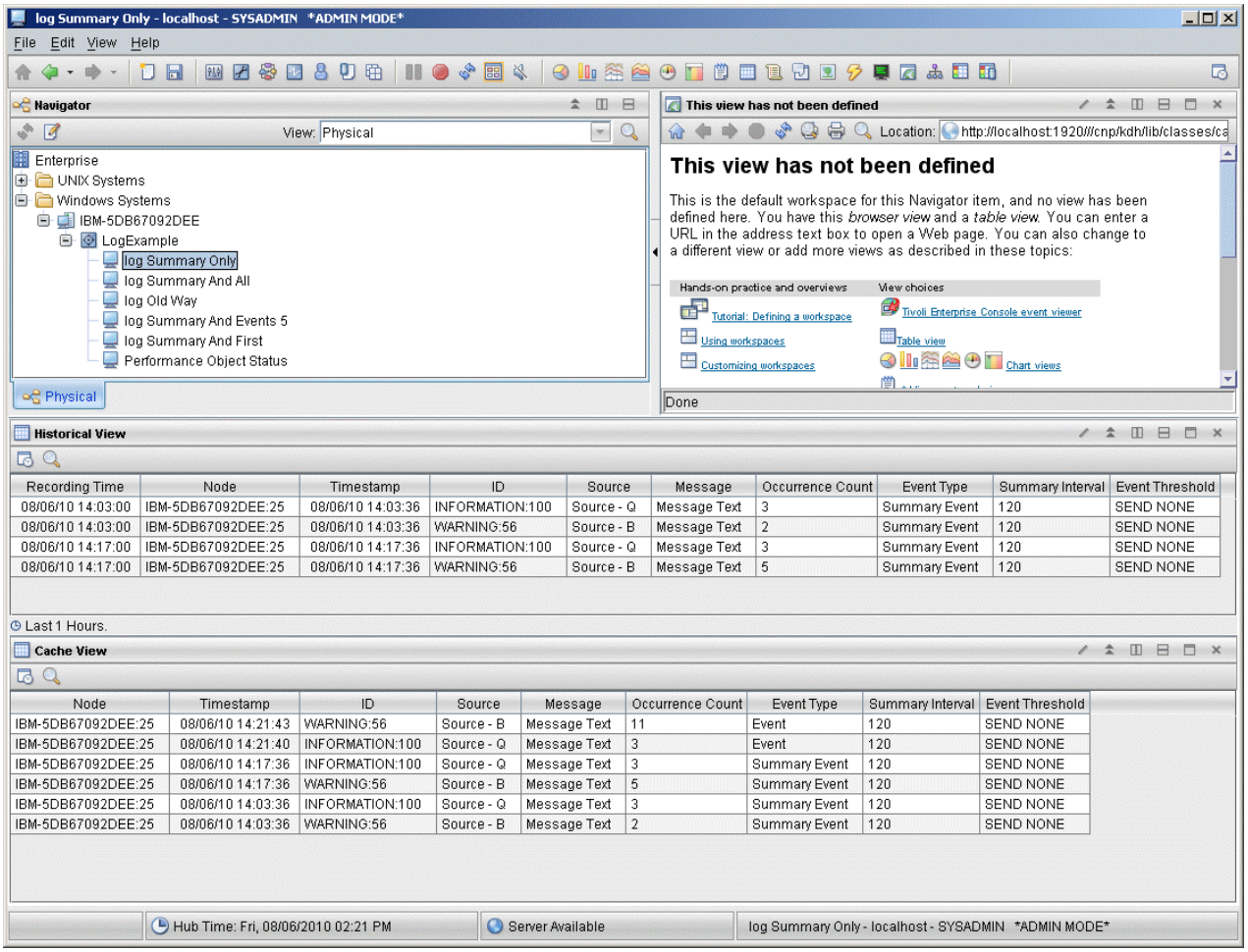


*Figure 76. Vue d'historique et vue de la mémoire cache lorsque l'option **Envoyer uniquement les événements du récapitulatif** est sélectionnée*

La (Figure 77, à la page 1454) affiche la vue d'historique et la vue de la mémoire cache si vous avez sélectionné l'option **Envoyer tous les événements** dans l'onglet **Informations sur les événements**. Tous les événements apparaissent dans les deux vues mais vous pouvez également afficher les événements du récapitulatif créés à la fin de chaque intervalle. La vue en temps réel change lorsque l'intervalle s'est écoulé. Les événements existants sont convertis en enregistrements récapitulatifs, puis les nouveaux événements sont ajoutés. L'ajout des deux autres attributs d'événement disponibles permet d'afficher l'intervalle de récapitulatif (120 secondes dans cet exemple) et le seuil *SEND ALL*.

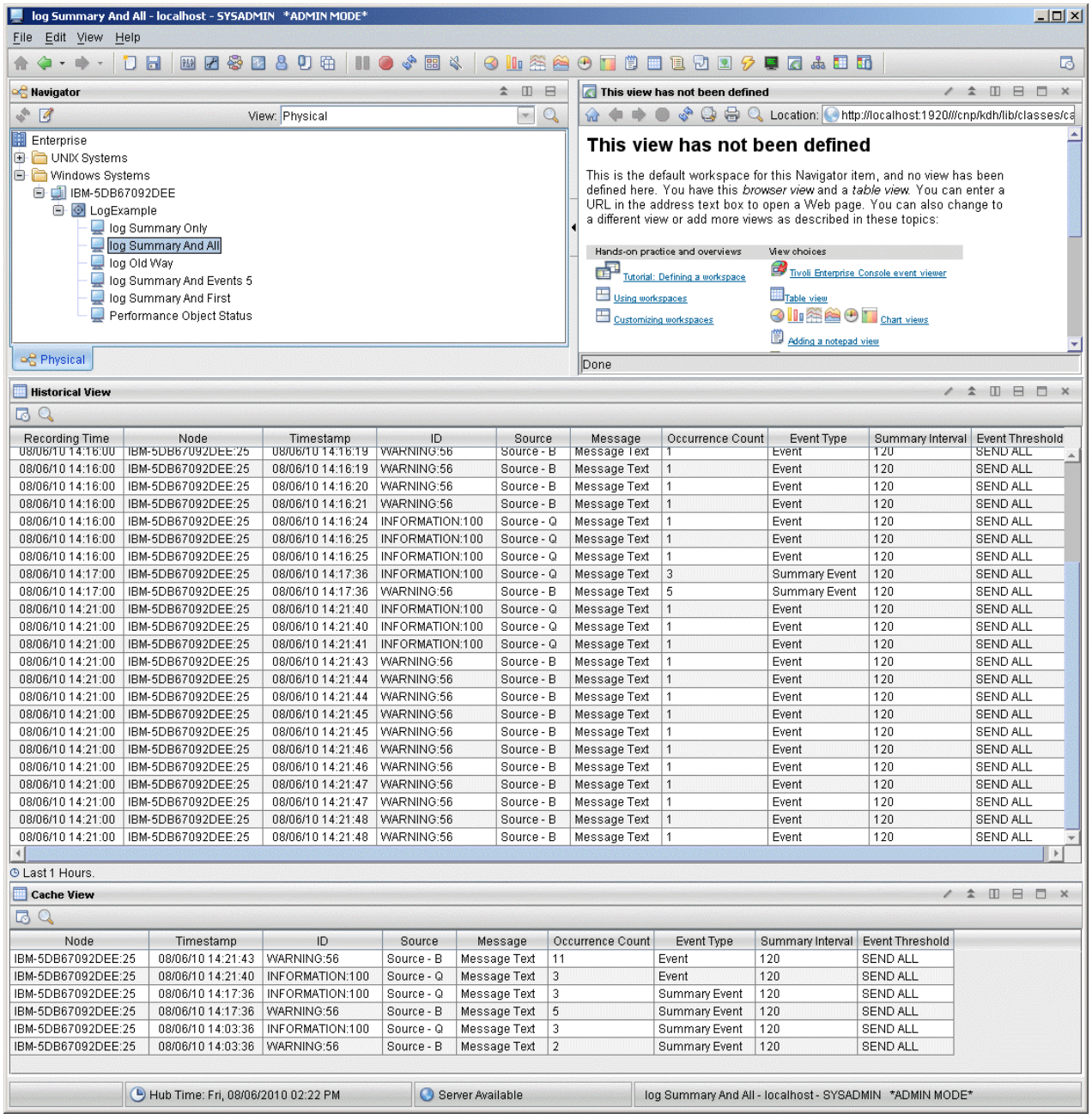


*Figure 77. Vue d'historique et vue de la mémoire cache lorsque l'option **Envoyer tous les événements** est sélectionnée*

La (Figure 78, à la page 1455) affiche la vue d'historique et la vue de la mémoire cache si vous avez sélectionné l'option **Envoyer le premier événement** dans l'onglet **Informations sur les événements**. Les événements récapitulatifs sont affichés dans les deux vues mais tous les nouveaux événements sont présentés uniquement dans la vue (mémoire cache) en temps réel. Pour chaque événement, la vue d'historique affiche uniquement le premier événement reçu au cours de l'intervalle et aucun événement en double.

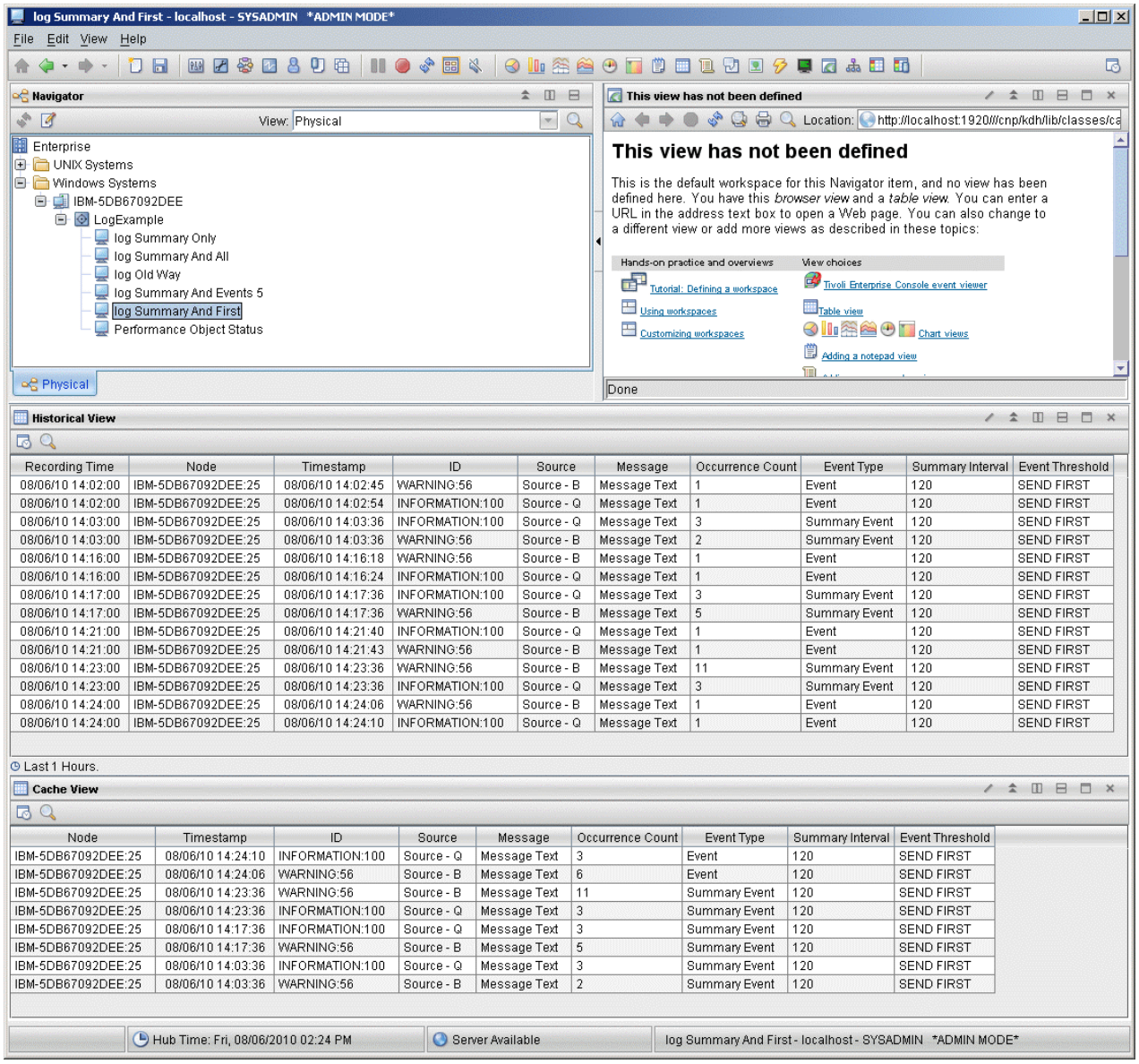


*Figure 78. Vue d'historique et vue de la mémoire cache lorsque l'option **Envoyer le premier événement** est sélectionnée*

La (Figure 79, à la page 1456) affiche la vue d'historique et la vue de la mémoire cache si vous avez sélectionné l'option **Seuil d'événements** et que vous avez entré la valeur 5. Les événements récapitulatifs sont affichés dans les deux vues mais tous les nouveaux événements sont présentés uniquement dans la vue (mémoire cache) en temps réel. Dans cet exemple, un seuil de 5 est spécifié. La vue d'historique affiche un événement uniquement lorsque cinq doublons de ce dernier (y compris la première occurrence) sont reçus au cours de l'intervalle. Si moins de 5 doublons sont reçus, aucun événement n'est affiché. Si 6, 7, 8 ou 9 doublons sont reçus dans l'intervalle, un événement est affiché. Si 10 doublons sont reçus, 2 événements sont affichés.

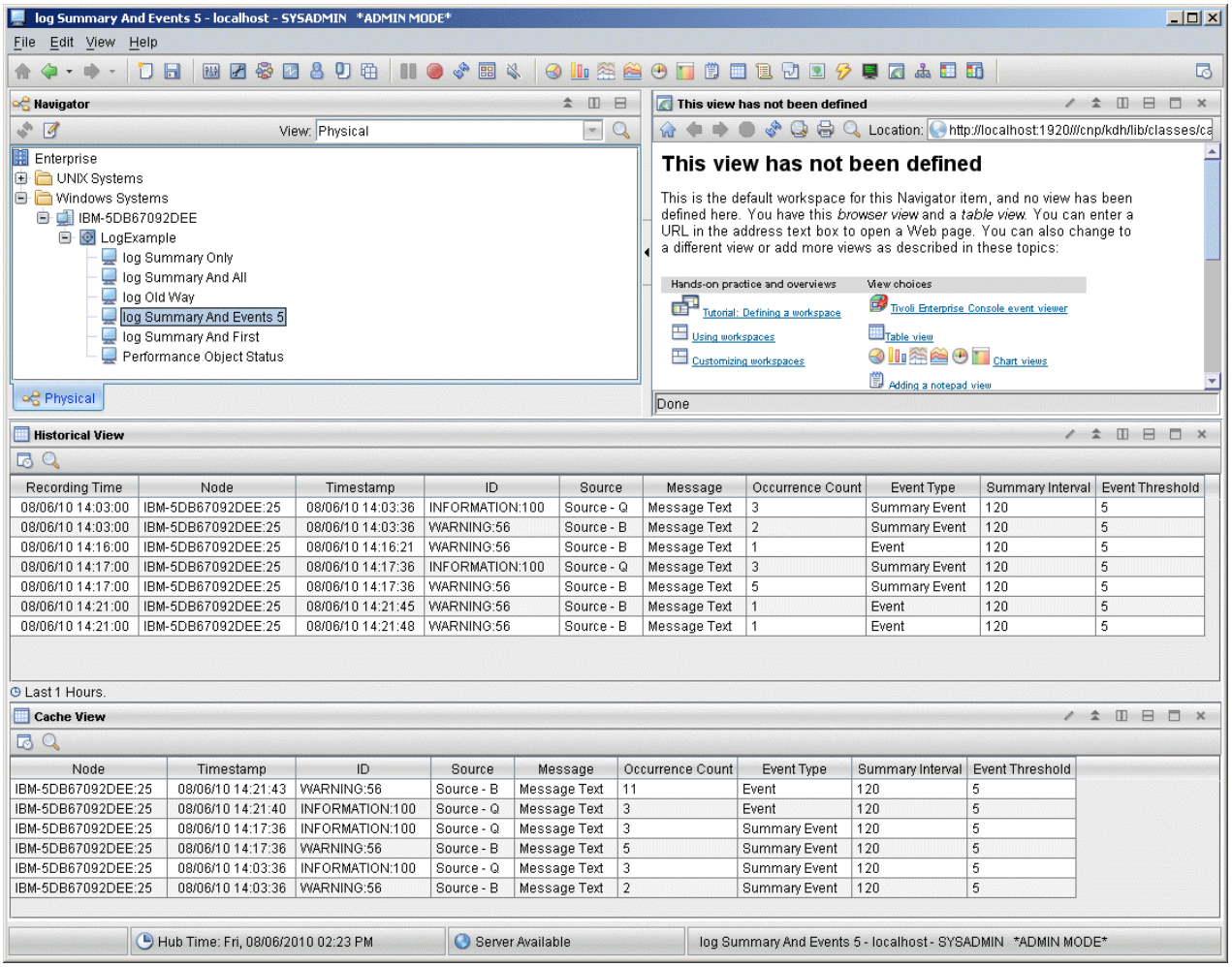


*Figure 79. Vue d'historique et vue de la mémoire cache lorsque l'option **Seuil d'événements** est sélectionnée*

Concepts associés

«Filtrage et récapitulatif des événements», à la page 1449

Traitement des incidents et support

Consultez les informations sur le traitement des incidents que vous pouvez rencontrer lors de l'installation, de la configuration ou de l'utilisation d'IBM Agent Builder.

Pour obtenir de l'aide lors du traitement des anomalies pendant le développement, l'installation ou l'utilisation des agents personnalisés dans l'environnement IBM Cloud Application Performance Management, consultez le forum Cloud Application Performance Management sur developerWorks. Vous pouvez rechercher la balise "agent_builder", répondre à une entrée pour poser une question connexe, ou créer une entrée avec votre question.

Pour des d'informations de référence sur la consignation et les messages, et pour obtenir de l'aide pour résoudre les anomalies liées à l'environnement IBM Tivoli Monitoring, consultez le guide de référence de traitement des incidents d'IBM Agent Builder.

Partage des fichiers de projet

Partagez un projet d'agent IBM Tivoli Monitoring avec quelqu'un.

Procédure

1. Obtenez leurs fichiers. Vous avez besoin du contenu complet du répertoire qui porte le nom du projet dans votre répertoire d'espace de travail.
   Par exemple, si le répertoire de votre espace de travail est `c:\Documents and Settings\User1\workspace` et que vous voulez partager votre projet nommé `TestProject`. Vous devez rendre le répertoire `c:\Documents and Settings\User1\workspace\TestProject Installer` et tout son contenu accessible à votre système.
2. Sélectionnez **Fichier** > **Importer**.
3. Ouvrez **IBM Tivoli Monitoring**.
4. Sélectionnez **Agent IBM Tivoli Monitoring** et cliquez sur **Suivant**.
5. Saisissez le chemin d'accès complet au fichier xml de l'agent ou cliquez sur **Parcourir** pour naviguer jusqu'au fichier.
6. Cliquez sur **Terminer**.

Résultats

A la fin de l'assistant, vous verrez le nouveau projet d'agent IBM Tivoli Monitoring dans votre espace de travail.

Partage d'un projet Solution Installer

Partagez un projet Solution Installer avec quelqu'un

Procédure

1. Obtenez leurs fichiers. La totalité du contenu du répertoire doit porter le même nom que le projet Solution Installer dans votre répertoire d'espace de travail.
   Par exemple, si le répertoire de l'espace de travail est `c:\Documents and Settings\User1\workspace` et que vous voulez partager votre projet Solution Installer nommé `TestProject Installer`. Vous devez rendre le répertoire `c:\Documents and Settings\User1\workspace\TestProject Installer` et tout son contenu accessible à votre système.
2. Cliquez sur **Fichier** > **Importer**.
3. Ouvrez l'onglet **Général**.
4. Sélectionnez **Projets existants dans l'espace de travail**, puis cliquez sur **Suivant**.
5. Entrez le chemin d'accès complet au répertoire principal du projet Solution Installer ou cliquez sur **Parcourir** pour naviguer jusqu'au répertoire principal du projet Solution Installer. (Dans cet exemple, il s'agit du répertoire `TestProject Installer`). Le projet de ce répertoire s'affiche dans la liste des projets et est sélectionné par défaut.
6. Facultatif : Cliquez sur **Copier les projets dans l'espace de travail**.
7. Cliquez sur **Terminer**.

Options de ligne de commande

Commandes disponibles à partir de l'interface de ligne de commande d'Agent Builder.

Tivoli Monitoring Agent Builder contient une interface de ligne de commande (CLI) que vous pouvez utiliser pour générer l'agent Tivoli Monitoring sans lancer l'interface graphique Eclipse. Vous pouvez générer l'agent dans le cadre d'une construction, par exemple :

Sur les systèmes Windows, vous pouvez utiliser un fichier de traitement par lots dans le répertoire suivant pour accéder à l'interface CLI :

```
emplacement_installation\agenttoolkit.bat
```

Sur les systèmes UNIX et Linux, vous pouvez utiliser un script dans le répertoire suivant pour accéder à l'interface CLI :

```
emplacement_installation/agenttoolkit.sh
```

Les commandes décrites dans la présente documentation sont mises en forme pour les systèmes Windows, qui utilisent une barre oblique inversée (\) pour les chemins de répertoire.

Pour les systèmes UNIX® ou Linux®, utilisez les mêmes commandes que pour les systèmes Windows, mais en apportant les modifications suivantes :

- Utilisez une barre oblique (/) pour les chemins de répertoire à la place d'une barre oblique inversée (\).
- Utilisez le script `agenttoolkit.sh` à la place du script `agenttoolkit.bat`.

Commandes

Le Tableau 300, à la page 1458 indique le nom et l'objectif de chacune des options de la commande text :

Tableau 300. Tableau de référence des commandes

Commande	Objectif
generatelocal	Charge/valide le fichier `itm_toolkit_agent.xml` et génère les fichiers qui exécutent l'agent Tivoli Monitoring. L'installation est effectuée dans un environnement Tivoli Monitoring local.
generatemappingfile	Crée le fichier de mappage pour la migration des modèles de ressource IBM Tivoli Monitoring version 5.x personnalisés vers des agents IBM Tivoli Monitoring version 6.
generatezip	Génère un fichier compressé intitulé *code_produit*`.zip` ou *code_produit*`.tgz`.

Les descriptions de commandes référencées à partir du tableau décrivent comment exécuter les commandes en indiquant les informations suivantes :

Objectif
Indique l'objet de la commande.

Format
Indique la syntaxe que vous entrez dans la ligne de commande. La syntaxe contient le nom de la commande et la liste de ses paramètres. Une définition de chaque paramètre suit le nom de la commande.

Exemples
L'exemple d'utilisation de la commande contient une brève description et un exemple de syntaxe.

Utilisation
Explique la commande et son objet.

Commentaires
Indique des commandes ou textes susceptibles de vous apporter de plus amples informations.

Commande - generatelocal

Cette commande permet de charger et de valider XML, et de générer les fichiers pour exécuter Tivoli Monitoring Agent.

Objectif

Charge/valide le fichier `itm_toolkit_agent.xml` et génère les fichiers qui exécutent l'agent Tivoli Monitoring. L'installation est effectuée dans un environnement Tivoli Monitoring local.

Format

Pour les systèmes Windows :

```
emplacement_installation\agenttoolkit.bat  rép_projet -generatelocal rép_install_itm
```

Où :

emplacement_installation
Répertoire dans lequel Agent Builder est installé

rép_projet
Nom du répertoire contenant le fichier `itm_toolkit_agent.xml`

rép_install_itm
Emplacement d'installation de Tivoli Monitoring (par exemple, `c:\IBM\ITM`)

Exemples

Dans l'exemple suivant pour Windows, la définition d'agent dans `C:\ABCAgent` est validée et les fichiers nécessaires pour exécuter `ABCAgent` sont générés dans `C:\IBM\ITM` :

```
emplacement_installation\agenttoolkit.bat C:\ABCAgent -generatelocal C:\IBM\ITM
```

Commande - generatemappingfile

Utilisez cette commande pour migrer des modèles de ressource IBM Tivoli Monitoring version 5.x personnalisés vers des agents IBM Tivoli Monitoring version 6.

Objectif

Cette commande crée le fichier de mappage pour la migration des modèles de ressource IBM Tivoli Monitoring version 5.x personnalisés vers des agents IBM Tivoli Monitoring version 6.

Format

Pour les systèmes Windows :

```
emplacement_installation\agenttoolkit.bat rép_projet -generatemappingfile rép_sortie
   liste_interp_itm5
```

Où :

emplacement_installation
Répertoire dans lequel Agent Builder est installé

rép_projet
Nom du répertoire contenant `itm_toolkit_agent.xml`

rép_sortie
Nom du répertoire dans lequel le fichier de mappage est enregistré

liste_interp_itm5
Liste des systèmes d'exploitation ITM 5x, séparés par des virgules, sur lesquels le modèle de ressource personnalisé a été exécuté. Les valeurs suivantes sont admises :

- aix4-r1
- hpux10
- linux-ix86
- linux-ppc
- linux-s390
- os2-ix86
- os400
- solaris2
- solaris2-ix86
- w32-ix86

Exemples

Pour les systèmes Windows

```
emplacement_installation\agenttoolkit.bat c:\ABCAgent -generatemappingfile c:\output
   linux-ix86,linux-ppc,linux-s390
```

Commande - generatezip

Cette commande permet de charger et de valider XML, et de générer un fichier compressé qui peut être utilisé pour installer l'agent sur un autre système.

Objectif

Elle charge et valide le fichier itm_toolkit_agent.xml et génère un fichier compressé intitulé *productcode*.zip ou *productcode*.tgz. Le fichier compressé généré peut être utilisé pour installer l'agent sur un autre système. En fonction de votre environnement, les deux types de fichier peuvent être générés.

Format

Pour les systèmes Windows :

```
emplacement_installation\agenttoolkit.bat  rép_projet -generatezip rép_sortie
```

Où :

rép_projet
Nom d'un répertoire contenant le fichier itm_toolkit_agent.xml

rép_sortie
Nom du répertoire dans lequel le fichier compressé est enregistré

Exemples

Dans l'exemple suivant pour Windows, la définition d'agent dans C:\ABCAgent est validée et un fichier compressé contenant les fichiers nécessaires à l'exécution de ABCAgent est généré dans C:\Output :

```
emplacement_installation\agenttoolkit.bat\ C:\ABCAgent -generatezip C:\Output
```

Guide de référence des attributs

Ce guide contient des descriptions des attributs de chaque groupe d'attributs généré, inclus dans Agent Builder.

Noeud de disponibilité

Le groupe d'attributs Disponibilité comporte les données de disponibilité pour l'application.

Le tableau fournit un format commun pour représenter la disponibilité de l'application, qui comprend les informations relatives aux trois aspects d'une application : les services (Windows uniquement), les processus et les codes retour de commande.

La liste suivante contient des informations sur chaque attribut du groupe d'attributs Disponibilité :

Attribut Noeud - Cet attribut est un attribut de clé

Description
Nom du système géré de l'agent

Type
Chaîne

Noms

Nom de l'attribut
Node

Nom de la colonne
ORIGINNODE

Attribut Horodatage

Description
Date et heure locales de l'agent lors de la collecte de données

Type
Date et heure

Noms

Nom de l'attribut
Timestamp

Nom de la colonne
TIMESTAMP

Attribut Composant d'application - Cet attribut est un attribut de clé

Description
Nom descriptif d'un composant de l'application

Type
Chaîne

Noms

Nom de l'attribut
Application_Component

Nom de la colonne
COMPONENT

Attribut Nom

Description
Nom du processus, du service ou du test fonctionnel. Ce nom correspond au nom exécutable du processus, au nom abrégé du service ou au nom du processus utilisé pour tester l'application.

Type
Chaîne

Noms

Nom de l'attribut
Name

Nom de la colonne
NAME

Attribut Statut

Description
Statut du composant d'application.

- Pour les processus, les valeurs sont `UP`, `DOWN`, `WARNING` ou `PROCESS_DATA_NOT_AVAILABLE`. `PROCESS_DATA_NOT_AVAILABLE` est affiché pour un processus lorsque le processus correspondant est en cours d'exécution, mais que les informations d'utilisation des ressources ne peuvent être collectées pour ce processus.
- Pour les services, les valeurs sont `UP`, `DOWN` ou `UNKNOWN`. `UNKNOWN` s'affiche si le service n'est pas installé.
- Pour les codes retour de commande, les valeurs sont `PASSED` ou `FAILED`.

Type
Chaîne

Noms

Nom de l'attribut
Status

Nom de la colonne
STATUS

Attribut Nom complet

Description
Nom complet du processus comprenant les informations dépendantes du processus. Le nom peut inclure le chemin d'accès complet si le processus a été démarré avec ce chemin-là. Il peut également inclure un chemin d'accès partiel ou même un chemin d'accès qui a été modifié par le processus.

Type
Chaîne

Noms

Nom de l'attribut
Full_Name

Nom de la colonne
FULLNAME

Attribut Type

Description
Identifie le type de composant d'application. Les composants sont les processus, les services ou les codes retour de commande.

Type
Entier (jauge)

Noms

Nom de l'attribut
Type

Nom de la colonne
TYPE

Attribut Taille virtuelle

Description
Taille virtuelle (en mégaoctets) du processus

Type
Entier (jauge)

Noms

Nom de l'attribut
Virtual_Size

Nom de la colonne
VIRTSIZE

Attribut Défauts de page par sec

Description
Taux de défauts de page pour le processus mesuré en défauts par seconde. Cette valeur ne contient que les données valides des processus.

Type
Entier (jauge)

Noms

Nom de l'attribut
Page_Faults_Per_Sec

Nom de la colonne
PAGEFAULTS

Attribut Taille de la partie active d'un programme

Description
Taille du jeu de documents du processus, en mégaoctets. Cette valeur ne contient que les données valides des processus.

Type
Entier (jauge)

Noms

Nom de l'attribut
Working_Set_Size

Nom de la colonne
WORKSET

Attribut Nombre d'unités d'exécution

Description
Nombre d'unités d'exécution actuellement attribuées par ce processus. Cette valeur ne contient que les données valides des processus.

Type
Entier (jauge)

Noms

Nom de l'attribut
Thread_Count

Nom de la colonne
THREADS

Attribut PID

Description
ID processus associé au processus. Cette valeur ne contient que les données valides des processus.

Type
Entier (jauge)

Noms

Nom de l'attribut
PID

Nom de la colonne
PID

Attribut Pourcentage de temps privilégié

Description
Pourcentage de temps de processeur disponible qui est utilisé par ce processus pour des opérations privilégiées

Type
Entier (jauge)

Noms

Nom de l'attribut
Percent_Privileged_Time

Nom de la colonne
PERCPRIV

Attribut Pourcentage du temps de mode utilisateur

Description
Pourcentage de temps de processeur disponible qui est utilisé par ce processus pour des opérations en mode utilisateur

Type
Entier (jauge)

Noms

Nom de l'attribut
Percent_User_Mode_Time

Nom de la colonne
PERCUSER

Attribut Pourcentage de temps processeur

Description
Pourcentage du temps écoulé pendant lequel un processus a utilisé le processeur pour exécuter des instructions

Type
Entier (jauge)

Noms

Nom de l'attribut
Percent_Processor_Time

Nom de la colonne
PERCPROC

Attribut Ligne de commande

Description
Nom du programme et arguments indiqués sur la ligne de commande lorsque le processus a été démarré. La valeur de cet attribut est *N/A* en cas d'exécution d'un test de service ou de fonctionnalité.

Type
Chaîne

Noms

Nom de l'attribut
Command_Line

Nom de la colonne
CMDLINE

Attribut Statut du test de fonctionnalité

Description
Code retour du test de fonctionnalité. Si l'application surveillée s'exécute correctement, le statut SUCCESS est renvoyé. Sinon, le statut NOT_RUNNING est renvoyé. Lorsque la ligne ne représente pas de test de fonctionnalité, le statut N/A est renvoyé.

Type
Entier avec valeurs énumérées. Les chaînes sont affichées dans Tivoli Enterprise Portal, l'entrepôt de données et les requêtes renvoient les nombres. Les valeurs définies sont : N/A(1), SUCCESS (0), GENERAL_ERROR (2), WARNING (3), NOT_RUNNING (4), DEPENDENT_NOT_RUNNING (5), ALREADY_RUNNING (6), PREREQ_NOT_RUNNING (7), TIMED_OUT (8), DOESNT_EXIST (9), UNKNOWN (10), DEPENDENT_STILL_RUNNING (11) ou INSUFFICIENT_USER_AUTHORITY (12). Les autres valeurs affichent la valeur numérique dans Tivoli Enterprise Portal.

Noms

Nom de l'attribut
Functionality_Test_Status

Nom de la colonne
FUNCSTATUS

Attribut Message du test de fonctionnalité

Description
Le message de texte qui correspond au statut du test de fonctionnalité. Cet attribut n'est valide que pour les codes retour de commande.

Type
Chaîne

Noms

Nom de l'attribut
Functionality_Test_Message

Nom de la colonne
FUNCMSG

Noeud de statut d'objet de performances

Le groupe d'attributs Statut de l'objet de performances permet de visualiser le statut de tous les groupes d'attributs qui composent l'agent. Chacun des groupes d'attributs est représenté par une ligne dans cette table ou dans un autre type de vue. Le statut d'un groupe d'attributs reflète le résultat de la dernière tentative de collecte de données, ou le dernier événement de réception de données, concernant le groupe d'attributs. Les informations sur le statut indiquent si l'agent fonctionne correctement. Si votre agent ne collecte aucune donnée mais en reçoit (données d'événement), les attributs associés aux données échantillonnées ne contiennent aucune donnée utile. Seuls les sept premiers attributs répertoriés sont pertinents pour les données d'événement.

Groupe historique

Ce groupe d'attributs peut être utilisé avec Tivoli Data Warehouse.

Description des attributs

La liste suivante contient des informations sur chaque attribut dans le groupe d'attributs Statut des objets de performances :

Attribut Noeud : Cet attribut est un attribut de clé.

Description

Nom du système géré de l'agent.

Type

Chaîne

Nom d'entrepôt de données

NODE

Attribut Horodatage

Description

L'heure locale sur l'agent à laquelle les données ont été collectées.

Type

Chaîne

Nom d'entrepôt de données

TIMESTAMP

Attribut Nom de requête - Cet attribut est un attribut de clé.

Description

Nom du groupe d'attributs.

Type

Chaîne

Nom d'entrepôt de données

QUERY_NAME ou ATTRGRP

Attribut Nom d'objet

Description

Nom de l'objet de performances.

Type

Chaîne

Nom d'entrepôt de données

OBJECT_NAME ou OBJNAME

Attribut Type d'objet

Description
Type de l'objet de performances.

Type
Entier avec valeurs énumérées. Les chaînes sont affichées dans Tivoli Enterprise Portal. L'entrepôt et les requêtes renvoient les valeurs indiquées entre parenthèses. Les valeurs définies sont les suivantes :

- WMI (0)
- PERFMON (1)
- WMI ASSOCIATION GROUP - GROUPE D'ASSOCIATION WMI (2)
- JMX (3)
- SNMP - Protocole SNMP (4)
- SHELL COMMAND - COMMANDE SHELL (5)
- JOINED GROUPS - GROUPES JOINTS (6)
- CIMOM - GESTIONNAIRE D'OBJETS CIM (7)
- CUSTOM - PERSONNALISE (8)
- ROLLUP DATA - DONNEES CUMULEES (9)
- WMI REMOTE DATA - DONNEES DISTANTES WMI (10)
- LOG FILE - FICHIER JOURNAL (11)
- JDBC - CONNECTIVITE JDBC (12)
- CONFIG DISCOVERY - RECONNAISSANCE CONFIG (13)
- NT EVENT LOG - JOURNAL DES EVENEMENTS (14)
- FILTER - FILTRE (15)
- SNMP EVENT - EVENEMENT PROTOCOLE SNMP (16)
- PING (17)
- DIRECTOR DATA - DONNEES DIRECTRICES (18)
- DIRECTOR EVENT - EVENEMENT DIRECTEUR (19)
- SSH REMOTE SHELL COMMAND - COMMANDE RSH SECURE SHELL (20)

Toute autre valeur est la valeur qui est renvoyée par l'agent dans Tivoli Enterprise Portal.

Nom d'entrepôt de données
OBJECT_TYPE ou OBJTYPE

Attribut Statut d'objet

Description
Statut de l'objet de performances.

Type
Entier avec valeurs énumérées. Les chaînes sont affichées dans Tivoli Enterprise Portal. L'entrepôt et les requêtes renvoient les valeurs indiquées entre parenthèses. Les valeurs définies sont les suivantes :

- ACTIVE - ACTIF (0)
- INACTIVE - INACTIF (1)

Toute autre valeur est la valeur qui est renvoyée par l'agent dans Tivoli Enterprise Portal.

Nom d'entrepôt de données
OBJECT_STATUS ou OBJSTTS

Attribut Code d'erreur

Description
Code d'erreur associé à la requête.

Type
Entier avec valeurs énumérées. Les chaînes sont affichées dans Tivoli Enterprise Portal. L'entrepôt et les requêtes renvoient les valeurs indiquées entre parenthèses. Les valeurs définies sont les suivantes :

- NO ERROR (0)
- GENERAL ERROR - ERREUR GENERALE (1)
- OBJECT NOT FOUND - OBJET INTROUVABLE (2)
- COUNTER NOT FOUND - COMPTEUR INTROUVABLE (3)
- NAMESPACE ERROR - ERREUR ESPACE DE NOM (4)
- OBJECT CURRENTLY UNAVAILABLE - OBJET ACTUELLEMENT INDISPONIBLE (5)
- COM LIBRARY INIT FAILURE - ERREUR INIT BIBLIOTHEQUE COM (6)
- SECURITY INIT FAILURE - ERREUR INIT SECURITE (7)
- PROXY SECURITY FAILURE - ERREUR SECURITE PROXY (9)
- NO INSTANCES RETURNED - AUCUNE INSTANCE RENVOYEE (10)
- ASSOCIATOR QUERY FAILED - ECHEC REQUETE D'ASSOCIATEUR (11)
- REFERENCE QUERY FAILED - ECHEC REQUETE DE REFERENCE (12)
- NO RESPONSE RECEIVED - AUCUNE REPONSE REÇUE (13)
- CANNOT FIND JOINED QUERY - REQUETE JOINTE INTROUVABLE (14)
- CANNOT FIND JOIN ATTRIBUTE IN QUERY 1 RESULTS - ATTRIBUT DE JOINTURE INTROUVABLE DANS RESULTATS DE LA REQUETE 1 (15)
- CANNOT FIND JOIN ATTRIBUTE IN QUERY 2 RESULTS - ATTRIBUT DE JOINTURE INTROUVABLE DANS RESULTATS DE LA REQUETE 2 (16)
- QUERY 1 NOT A SINGLETON - LA REQUETE 1 N'EST PAS UN SINGLETON (17)
- QUERY 2 NOT A SINGLETON - LA REQUETE 2 N'EST PAS UN SINGLETON (18)
- NO INSTANCES RETURNED IN QUERY 1 - AUCUNE INSTANCE RENVOYEE DANS LA REQUETE 1 (19)
- NO INSTANCES RETURNED IN QUERY 2 - AUCUNE INSTANCE RENVOYEE DANS LA REQUETE 2 (20)
- CANNOT FIND ROLLUP QUERY - REQUETE DE CUMUL INTROUVABLE (21)
- CANNOT FIND ROLLUP ATTRIBUTE - ATTRIBUT DE CUMUL INTROUVABLE (22)
- FILE OFFLINE - FICHIER HORS LIGNE (23)
- NO HOSTNAME - AUCUN NOM D'HOTE (24)
- MISSING LIBRARY - BIBLIOTHEQUE ABSENTE (25)
- ATTRIBUTE COUNT MISMATCH - NON-CONCORDANCE DU NOMBRE D'ATTRIBUTS (26)
- ATTRIBUTE NAME MISMATCH - NON-CONCORDANCE DU NOM D'ATTRIBUT (27)
- COMMON DATA PROVIDER NOT STARTED - FOURNISSEUR DE DONNEES COMMUNES NON DEMARRE (28)
- CALLBACK REGISTRATION ERROR - ERREUR D'ENREGISTREMENT DE RAPPEL (29)
- MDL LOAD ERROR - ERREUR DE CHARGEMENT MDL (30)
- AUTHENTICATION FAILED - ECHEC DE L'AUTHENTIFICATION (31)
- CANNOT RESOLVE HOST NAME - IMPOSSIBLE DE RESOUDRE LE NOM D'HOTE (32)
- SUBNODE UNAVAILABLE - SOUS-NOEUD NON DISPONIBLE (33)
- SUBNODE NOT FOUND IN CONFIG - SOUS-NOEUD INTROUVABLE DANS CONFIG (34)

- ATTRIBUTE ERROR - ERREUR D'ATTRIBUT (35)
- CLASSPATH ERROR - ERREUR DE CHEMIN DE CLASSE (36)
- CONNECTION FAILURE - ECHEC DE LA CONNEXION (37)
- FILTER SYNTAX ERROR - ERREUR DE SYNTAXE DU FILTRE (38)
- FILE NAME MISSING - NOM DE FICHIER MANQUANT (39)
- SQL QUERY ERROR - ERREUR DE REQUETE SQL (40)
- SQL FILTER QUERY ERROR - ERREUR DE REQUETE DE FILTRAGE SQL (41)
- SQL DB QUERY ERROR - ERREUR DE REQUETE DE BASE DE DONNEES SQL (42)
- SQL DB FILTER QUERY ERROR - ERREUR DE REQUETE DE FILTRAGE DE BASE DE DONNEES SQL (43)
- PORT OPEN FAILED - ECHEC DE L'OUVERTURE DU PORT (44)
- ACCESS DENIED - ACCES REFUSE (45)
- TIMEOUT - DEPASSEMENT DE DELAI (46)
- NOT IMPLEMENTED - NON IMPLEMENTE (47)
- REQUESTED A BAD VALUE - VALEUR DEMANDEE INCORRECTE (48)
- RESPONSE TOO BIG - REPONSE TROP LONGUE (49)
- GENERAL RESPONSE ERROR - ERREUR DE REPONSE GENERALE (50)
- SCRIPT NONZERO RETURN - LE SCRIPT A RENVOYE UNE VALEUR DIFFERENTE DE ZERO (51)
- SCRIPT NOT FOUND - SCRIPT INTROUVABLE (52)
- SCRIPT LAUNCH ERROR - ERREUR DE LANCEMENT DU SCRIPT (53)
- CONF FILE DOES NOT EXIST - LE FICHIER CONF N'EXISTE PAS (54)
- CONF FILE ACCESS DENIED - ACCES REFUSE AU FICHIER CONF (55)
- INVALID CONF FILE - FICHIER CONF NON VALIDE (56)
- EIF INITIALIZATION FAILED - L'INITIALISATION D'EIF A ECHOUE (57)
- CANNOT OPEN FORMAT FILE - IMPOSSIBLE D'OUVRIR LE FICHIER DE FORMAT (58)
- FORMAT FILE SYNTAX ERROR - ERREUR DE SYNTAXE DU FICHIER DE FORMAT (59)
- REMOTE HOST UNAVAILABLE - HOTE DISTANT NON DISPONIBLE (60)
- EVENT LOG DOES NOT EXIST - LE JOURNAL DES EVENEMENTS N'EXISTE PAS (61)
- PING FILE DOES NOT EXIST - LE FICHIER PING N'EXISTE PAS (62)
- NO PING DEVICE FILES - AUCUN FICHIER DE PERIPHERIQUES A PINGUER (63)
- PING DEVICE LIST FILE MISSING - FICHIER-LISTE DE PERIPHERIQUES A PINGUER MANQUANT (64)
- SNMP MISSING PASSWORD - MOT DE PASSE MANQUANT SNMP (65)
- DISABLED - DESACTIVE (66)
- URLS FILE NOT FOUND - FICHIER URLS INTROUVABLE (67)
- XML PARSE ERROR - ERREUR D'ANALYSE XML (68)
- NON INITIALISE (69)
- ECHEC DES SOCKETS ICMP (70)

Toute autre valeur est la valeur qui est renvoyée par l'agent dans Tivoli Enterprise Portal.

Nom d'entrepôt de données
ERROR_CODE ou ERRCODE

Attribut Démarrage de la dernière collecte

Description
Date et heure du dernier démarrage d'une collecte de données de ce groupe.

Type
Horodatage avec des valeurs énumérées. Les chaînes sont affichées dans Tivoli Enterprise Portal. L'entrepôt et les requêtes renvoient les valeurs indiquées entre parenthèses. Les valeurs définies sont les suivantes :

- NOT COLLECTED (0691231190000000)
- NON COLLECTE (0000000000000001)

Toute autre valeur est la valeur qui est renvoyée par l'agent dans Tivoli Enterprise Portal.

Nom d'entrepôt de données
LAST_COLLECTION_START ou COLSTRT

Attribut Dernière collecte terminée

Description
Date et heure de la dernière fin de collecte de données de ce groupe.

Type
Horodatage avec des valeurs énumérées. Les chaînes sont affichées dans Tivoli Enterprise Portal. L'entrepôt et les requêtes renvoient les valeurs indiquées entre parenthèses. Les valeurs définies sont les suivantes :

- NOT COLLECTED (0691231190000000)
- NON COLLECTE (0000000000000001)

Toute autre valeur est la valeur qui est renvoyée par l'agent dans Tivoli Enterprise Portal.

Nom d'entrepôt de données
LAST_COLLECTION_FINISHED ou COLFINI

Attribut Durée de la dernière collecte

Description
Durée de la dernière collecte de données terminée de ce groupe (en secondes).

Type
Nombre réel (compteur 32 bits) avec une précision de deux décimales.

Nom d'entrepôt de données
LAST_COLLECTION_DURATION ou COLDURA

Attribut Durée moyenne de la collecte

Description
Durée moyenne de toutes les collectes de données de ce groupe (en secondes).

Type
Nombre réel (compteur 32 bits) avec une précision de deux décimales et des valeurs énumérées. Les chaînes sont affichées dans Tivoli Enterprise Portal. L'entrepôt et les requêtes renvoient les valeurs indiquées entre parenthèses. Les valeurs définies sont les suivantes :

- NO DATA (-100)

Toute autre valeur est la valeur qui est renvoyée par l'agent dans Tivoli Enterprise Portal.

Nom d'entrepôt de données
AVERAGE_COLLECTION_DURATION ou COLAVGD

Attribut Fréquence de régénération

Description
Fréquence de régénération de ce groupe (en secondes).

Type
Entier (compteur 32 bits)

Nom d'entrepôt de données
REFRESH_INTERVAL ou REFRINT

Attribut Nombre de collectes

Description
Nombre de collectes de ce groupe depuis le démarrage de l'agent.

Type
Entier (compteur 32 bits)

Nom d'entrepôt de données
NUMBER_OF_COLLECTIONS ou NUMCOLL

Attribut Accès au cache

Description
Nombre de fois où une demande de données externes pour ce groupe a été satisfaite à partir de la mémoire cache.

Type
Entier (compteur 32 bits)

Nom d'entrepôt de données
CACHE_HITS ou CACHEHT

Attribut Echecs d'accès au cache

Description
Nombre de fois où une demande de données pour ce groupe n'était pas disponible dans la mémoire cache.

Type
Entier (compteur 32 bits)

Nom d'entrepôt de données
CACHE_MISSES ou CACHEMS

Attribut Pourcentage des accès au cache

Description
Pourcentage des demandes de données externes pour ce groupe qui ont été satisfaites à partir de la mémoire cache.

Type
Nombre réel (compteur 32 bits) avec une précision de deux décimales.

Nom d'entrepôt de données
CACHE_HIT_PERCENT ou CACHPCT

Attribut Intervalles ignorés

Description
Nombre de fois où une collecte de données d'arrière-plan pour ce groupe a été ignorée, car la précédente collecte était encore en cours d'exécution lorsque la suivante devait démarrer.

Type
Entier (compteur 32 bits)

Nom d'entrepôt de données
INTERVALS_SKIPPED ou INTSKIP

Groupe d'attributs de statut du pool d'unités d'exécution

Le groupe d'attributs Statut du pool d'unités d'exécution contient des informations reflétant le statut du pool d'unités d'exécution interne utilisé pour la collecte asynchrone des données.

La section ci-dessous contient la liste des attributs de ce groupe d'attributs. Le nom en gras montre comment l'attribut s'affiche dans Tivoli Enterprise Portal.

La liste suivante contient des informations sur chaque attribut dans le groupe d'attributs Statut du pool d'unités d'exécution :

Attribut Noeud - Cet attribut est un attribut de clé

Description
Nom du système géré de l'agent

Type
Chaîne

Noms

Nom de l'attribut
Node

Nom de la colonne
ORIGINNODE

Attribut Horodatage

Description
Heure collectée du système d'agent à laquelle la ligne de données a été générée et envoyée de l'agent à Tivoli Enterprise Monitoring Server. ou stockée à des fins d'historique. Elle représente le fuseau horaire local du système d'agent.

Type
Date et heure

Noms

Nom de l'attribut
Timestamp

Nom de la colonne
TIMESTAMP

Attribut Taille du pool d'unités d'exécution

Description
Nombre d'unités d'exécution existantes dans le pool d'unités d'exécution.

Type
Entier

Noms

Nom de l'attribut
Thread_Pool_Size

Nom de la colonne
THPSIZE

Attribut Taille maximale du pool d'unités d'exécution

Description
Nombre maximal d'unités d'exécution admises dans le pool d'unités d'exécution.

Type
Entier

Noms

Nom de l'attribut
Thread_Pool_Max_Size

Nom de la colonne
TPMAXSZ

Attribut Unités d'exécution actives du pool d'unités d'exécution

Description
Nombre d'unités d'exécution actuellement actives dans le pool d'unités d'exécution.

Type
Entier

Noms

Nom de l'attribut
Thread_Pool_Active_Threads

Nom de la colonne
TPACTTH

Attribut Nombre moyen d'unités d'exécution actives du pool d'unités d'exécution

Description
Nombre moyen d'unités d'exécution simultanément actives dans le pool d'unités d'exécution.

Type
Entier

Noms

Nom de l'attribut
Thread_Pool_Avg_Active_Threads

Nom de la colonne
TPAVGAT

Attribut Nombre minimal d'unités d'exécution actives du pool d'unités d'exécution

Description
Nombre minimal d'unités d'exécution simultanément actives dans le pool d'unités d'exécution.

Type
Entier

Noms

Nom de l'attribut
Thread_Pool_Min_Active_Threads

Nom de la colonne
TPMINAT

Attribut Nombre maximal d'unités d'exécution actives du pool d'unités d'exécution

Description
Nombre maximal d'unités d'exécution simultanément actives dans le pool d'unités d'exécution.

Type
Entier

Noms

Nom de l'attribut
Thread_Pool_Max_Active_Threads

Nom de la colonne
TPMAXAT

Attribut Longueur de file d'attente du pool d'unités d'exécution

Description
Nombre de travaux en attente dans la file d'attente du pool d'unités d'exécution.

Type
Entier

Noms

Nom de l'attribut
Thread_Pool_Queue_Length

Nom de la colonne
TPQLGTH

Attribut Longueur moyenne de file d'attente du pool d'unités d'exécution

Description
Longueur moyenne de la file d'attente du pool d'unités d'exécution pendant cette exécution.

Type
Entier

Noms

Nom de l'attribut
Thread_Pool_Avg_Queue_Length

Nom de la colonne
TPAVGQL

Attribut Longueur minimale de file d'attente du pool d'unités d'exécution

Description
Longueur minimale atteinte par la file d'attente du pool d'unités d'exécution.

Type
Entier

Noms

Nom de l'attribut
Thread_Pool_Min_Queue_Length

Nom de la colonne
TPMINQL

Attribut Longueur maximale de file d'attente du pool d'unités d'exécution

Description
Longueur maximale atteinte par la file d'attente du pool d'unités d'exécution.

Type
Entier

Noms

Nom de l'attribut
Thread_Pool_Max_Queue_Length

Nom de la colonne
TPMAXQL

Attribut Délai d'attente moyen des travaux du pool d'unités d'exécution

Description
Délai d'attente moyen d'un travail dans la file d'attente du pool d'unités d'exécution.

Type
Entier

Noms

Nom de l'attribut
Thread_Pool_Avg_Job_Wait

Nom de la colonne
TPAVJBW

Attribut Nombre total de travaux du pool d'unités d'exécution

Description
Nombre de travaux terminés par toutes les unités d'exécution du pool depuis le démarrage de l'agent.

Type
Entier

Noms

Nom de l'attribut
Thread_Pool_Total_Jobs

Nom de la colonne
TPTJOBS

Groupe d'attributs Journal des événements

Le groupe d'attributs Journal des événements contient les entrées récentes du journal des événements qui concernent l'application.

Par défaut, l'agent affiche uniquement les événements qui se produisent après le démarrage de l'agent. Les événements sont supprimés de la vue Journal des événements 1 heure après s'être produits.

La liste suivante contient des informations sur chaque attribut dans le groupe d'attributs Journal des événements :

Attribut Noeud - Cet attribut est un attribut de clé

Description
Nom du système géré de l'agent

Type
Chaîne

Noms

Nom de l'attribut
Node

Nom de la colonne
ORIGINNODE

Attribut Nom du journal

Description
Journal des événements - Application, Système, Sécurité ou journal propre à l'application

Type
Chaîne

Noms

Nom de l'attribut
Log_Name

Nom de la colonne
LOGNAME

Attribut Source d'événement

Description
Source d'événement définie par l'application

Type
Chaîne

Noms

Nom de l'attribut
Event_Source

Nom de la colonne
EVTSOURCE

Attribut Type d'événement

Description
Type d'événement - Error(0), Warning(1), Informational(2), Audit_Success(3), Audit_Failure(4), Unknown(5)

Type
Entier

Noms

Nom de l'attribut
Event_Type

Nom de la colonne
EVTTYPE

Attribut ID de l'événement

Description
Identificateur de l'événement

Type
Entier

Noms

Nom de l'attribut
Event_ID

Nom de la colonne
EVTID

Attribut Catégorie d'événement

Description
Catégorie de l'événement

Type
Chaîne

Noms

Nom de l'attribut
Event_Category

Nom de la colonne
EVTCATEG

Attribut Message

Description
Message de l'événement

Type
Chaîne

Noms

Nom de l'attribut
Message

Nom de la colonne
MESSAGE

Attribut Heure de génération

Description
Date et heure auxquelles l'événement a été généré

Type
Date et heure

Noms

Nom de l'attribut
Time_Generated

Nom de la colonne
TIMESTAMP

Synthèse du fichier journal

Les attributs de ce groupe sont inclus dans des groupes d'attributs récapitulatifs si cette option est sélectionnée dans les propriétés avancées de la source de données.

Un noeud récapitulatif est créé pour chaque source de données de fichier journal lorsque l'option **Inclure l'attribut dans le groupe d'attributs récapitulatif** est sélectionnée dans les propriétés avancées de la source de données. Le nom du noeud récapitulatif est le nom de la source de données auquel est ajouté Récapitulatif.

La liste suivante contient des informations relatives à chacun des attributs par défaut du groupe d'attributs Synthèse de fichier journal. Ces attributs sont toujours inclus dans les groupes d'attributs récapitulatifs. Si vous sélectionnez **Inclure l'attribut dans le groupe d'attributs récapitulatif**, voir l'étape «9», à la page 1304 dans «Surveillance d'un fichier journal», à la page 1299. Le groupe d'attributs récapitulatif pour ce groupe d'attributs de journal contient également chacun des attributs que vous avez sélectionnés. Les valeurs sont une copie de l'attribut correspondant dans le groupe d'attributs de fichier journal.

Tous les attributs ajoutés forment collectivement une clé et la table récapitulative va inclure une ligne par ensemble unique de clés. La ligne indique le nombre d'enregistrements de journal reçus pendant l'intervalle où toutes les clés fournies correspondaient à la valeur signalée dans les attributs correspondants.

Attribut Noeud - Cet attribut est un attribut de clé

Description
Nom du système géré de l'agent

Type
Chaîne

Noms

Nom de l'attribut
Node

Nom de la colonne
ORIGINNODE

Attribut Horodatage

Description
Date et heure locales de l'agent lors de la collecte de données

Type
Date et heure

Noms

Nom de l'attribut
Timestamp

Nom de la colonne
TIMESTAMP

Attribut Unité d'intervalle

Description
Nombre de secondes entres les générations de l'attribut de synthèse

Type
Entier (jauge)

Noms

Nom de l'attribut
_Interval_Unit

Nom de la colonne
IU

Attribut Intervalle

Description
Décalage de l'intervalle en cours dans l'unité de temps suivante la plus grande (par exemple, minutes dans une heure)

Type
Entier (jauge)

Noms

Nom de l'attribut
_Interval

Nom de la colonne
INV

Attribut Occurrences

Description
Nombre d'occurrences enregistrées dans l'intervalle

Type
Entier (jauge)

Noms

Nom de l'attribut
_Occurrences

Nom de la colonne
OCC

Attribut Horodatage local

Description
Date et heure auxquelles les données de synthèse ont été générées

Type
Horodatage

Noms

Nom de l'attribut
_LocalTimeStamp

Nom de la colonne
LTS

Attribut Date et heure

Description
Date et heure auxquelles les données de synthèse ont été générées

Type
Chaîne

Noms

Nom de l'attribut
_Date_Time

Nom de la colonne
DT

Attribut Nom de l'unité d'intervalle

Description
Description textuelle de l'unité d'intervalle

Type
Chaîne

Noms

Nom de l'attribut
_Interval_Unit_Name

Nom de la colonne
IUN

Groupe d'attributs du journal binaire AIX

Le groupe d'attributs du journal binaire AIX affiche les événements du journal binaire AIX fournis par la chaîne de commande `errpt`.

La liste suivante contient des informations sur chaque attribut du groupe d'attributs du journal binaire AIX :

Remarque : Agent Builder empêche la suppression, la réorganisation ou le changement de la taille des attributs `Identificateur`, `ErrptTimestamp`, `Type`, `Classe`, `ResourceName` et `Description`. L'agent effectue une analyse syntaxique des données issues d'une commande `errpt`, en fonction des colonnes dans la ligne de texte. Ces colonnes sont définies selon l'ordre et la taille des attributs `Identificateur`, `ErrptTimestamp`, `Type`, `Classe`, `ResourceName` et `Description`. La suppression, la réorganisation ou le changement de la taille de ces attributs modifient l'attribut de destination des différentes colonnes. La ligne résultante affichée dans Tivoli Monitoring est alors incorrecte.

Cependant, vous pouvez renommer ces attributs.

Attribut Noeud - Cet attribut est un attribut de clé

Description
Nom du système géré de l'agent

Type
Chaîne

Noms

Nom de l'attribut
Node

Nom de la colonne
ORIGINNODE

Attribut Identificateur - Cet attribut est un attribut de clé

Description
Identificateur d'événement signalé par `errpt`

Type
Chaîne

Noms

Nom de l'attribut
Identifier

Nom de la colonne
IDENTIFIER

Attribut ErrptTimestamp

Description
Heure à laquelle l'événement est enregistré, comme signalé par `errpt`.

Remarque : Cet attribut est masqué lors de l'exécution. Il contient une valeur brute. Les autres attributs dérivés de celui-ci affichent la valeur dans un format plus utilisable. Cet attribut est disponible dans Agent Builder dans cet objectif, mais n'apparaît pas par défaut dans l'environnement Tivoli Monitoring lors de l'exécution. Si vous souhaitez le faire apparaître, sélectionnez l'attribut dans la page **Définition de la source de données** de l'éditeur d'agent et sélectionnez **Afficher l'attribut dans Tivoli Enterprise Portal**.

Type
Chaîne

Noms

Nom de l'attribut
ErrptTimestamp

Nom de la colonne
ERRPTTIMES

Type

Description
Type d'événement à caractère unique signalé par `errpt` : `I(NFO)`, `P(END/ERF/ERM)`, `T(EMP)` ou `U(NKN)`

Type
Chaîne

Noms

Nom de l'attribut
Type

Nom de la colonne
TYPE

Attribut Classe - Cet attribut est un attribut de clé

Description
Classe d'événement signalée par `errpt` : `Matériel`, `Logiciel`, `Opérateur` ou `Indéterminé`. Ces valeurs sont énumérées. Les valeurs brutes à utiliser avec les situations sont H, S, O et U.

Type
Chaîne

Noms

Nom de l'attribut
Class

Nom de la colonne
CLASS

ResourceName

Description
Le nom de ressource signalé par `errpt` identifie l'origine de l'enregistrement d'erreur

Type
Chaîne

Noms

Nom de l'attribut
ResourceName

Nom de la colonne
RESOURCENA

Attribut Description

Description
Description signalée par `errpt`, généralement un message texte court décrivant la nature de l'erreur

Type
Chaîne

Noms

Nom de l'attribut
Description

Nom de la colonne
DESCRIPTION

Attribut LogFile

Description
Nom complet du journal `errpt` binaire, comprenant le chemin.

Remarque : Cet attribut est masqué lors de l'exécution. Il contient une valeur brute. Les autres attributs dérivés de celui-ci affichent la valeur dans un format plus utilisable. Cet attribut est disponible dans Agent Builder dans cet objectif, mais n'apparaît pas par défaut dans l'environnement Tivoli Monitoring lors de l'exécution. Si vous souhaitez le faire apparaître,

sélectionnez l'attribut dans la page **Définition de la source de données** de l'éditeur d'agent et sélectionnez **Afficher l'attribut dans Tivoli Enterprise Portal**.

Type
Chaîne

Noms

Nom de l'attribut
LogFile

Nom de la colonne
LOGFILE

Attribut Système

Description
Nom d'hôte du système où l'erreur a été collectée

Type
Chaîne

Noms

Nom de l'attribut
System

Nom de la colonne
SYSTEM

Attribut LogName

Description
Nom de base du journal `errpt` binaire depuis lequel l'enregistrement a été collecté

Type
Chaîne

Noms

Nom de l'attribut
LogName

Nom de la colonne
LOGNAME

Attribut LogPath

Description
Nom du répertoire contenant le journal `errpt` binaire à partir duquel l'enregistrement a été collecté

Type
Chaîne

Noms

Nom de l'attribut
LogPath

Nom de la colonne
LOGPATH

Attribut EntryTime

Description
Heure d'enregistrement de l'événement, signalée par `errpt` au format d'horodatage Tivoli. Cette heure n'est pas nécessairement identique à l'heure à laquelle l'agent a reçu l'événement, enregistrée dans la zone **`Horodatage`**.

Type
Horodatage

Noms

Nom de l'attribut
EntryTime

Nom de la colonne
ENTRYTIME

Groupes d'attributs Surveillance et notification

Définitions associées aux groupes d'attributs Surveillance et notification.

Les 4 premiers sont propres aux contrôleurs et le dernier aux notifications (tous étant liés à JMX).

Chaque groupe d'attributs est répertorié à l'aide d'une indication précisant s'il est basé ou non sur des événements. Pour les groupes d'attributs autres que ceux basés sur des événements, les données sont collectées si nécessaire. Pour les groupes d'attributs basés sur des événements, l'agent gère une mémoire cache des 100 derniers événements reçus. Ces événements servent à répondre aux demandes émanant de Tivoli Enterprise Portal. Les événements sont immédiatement réacheminés pour être analysés par des situations et l'entreposage.

Notifications de compteur
Le groupe d'attributs Notifications de compteur est un groupe d'attributs autre que les groupes d'attributs basés sur des événements, qui envoie des événements reçus par tous les contrôleurs de compteur.

La liste suivante contient des informations sur chaque attribut du groupe d'attributs Notifications de compteur :

Attribut Noeud - Cet attribut est un attribut de clé

Description
Nom du système géré de l'agent

Type
Chaîne

Noms

Nom de l'attribut
Node

Nom de la colonne
ORIGINNODE

Attribut Horodatage

Description
Date et heure locales de l'agent lors de la collecte de données

Type
Date et heure

Noms

Nom de l'attribut
Timestamp

Nom de la colonne
TIMESTAMP

Attribut Type de notification

Description
Type de la notification reçue. Décrit comment l'attribut observé de MBean a déclenché la notification.

Type
Chaîne

Noms

Nom de l'attribut
Notification_Type

Nom de la colonne
NOTIFICATI

Attribut ID contrôleur

Description
ID du contrôleur ayant généré cette notification

Type
Entier

Noms

Nom de l'attribut
Monitor_ID

Nom de la colonne
MONITOR_ID

Attribut MBean observé

Description
Le MBean dont l'attribut est en cours de surveillance

Type
Chaîne

Noms

Nom de l'attribut
Observed_MBean

Nom de la colonne
OBSERVED_M

Attribut Attribut observé

Description
Nom de l'attribut surveillé dans le MBean observé

Type
Chaîne

Noms

Nom de l'attribut
Observed_Attribute

Nom de la colonne
OBSERVED_A

Attribut Seuil

Description
Seuil en cours du contrôleur

Type
Chaîne

Noms

Nom de l'attribut
Threshold

Nom de la colonne
THRESHOLD

Attribut Décalage

Description
Valeur ajoutée au seuil chaque fois que l'attribut dépasse le seuil. Cette valeur forme un nouveau seuil.

Type
Chaîne

Noms

Nom de l'attribut
Offset

Nom de la colonne
OFFSET

Attribut Modulo

Description
Valeur maximale de l'attribut. Lorsque ce dernier atteint cette valeur, il est remplacé et reprend le comptage à partir de zéro.

Type
Entier

Noms

Nom de l'attribut
Modulus

Nom de la colonne
MODULUS

Attribut Valeur de compteur

Description
Valeur du compteur ayant déclenché la notification

Type
Entier

Noms

Nom de l'attribut
Counter_Value

Nom de la colonne
COUNTER_VA

Attribut Horodatage de notification

Description
Date et heure du déclenchement de la notification

Type
Date et heure

Noms

Nom de l'attribut
Notification_Time_Stamp

Nom de la colonne
NOTIFICAT0

Attribut Message de notification

Description
Message figurant dans la notification

Type
Chaîne

Noms

Nom de l'attribut
Notification_Message

Nom de la colonne
NOTIFICAT1

Notifications de jauge
Le groupe d'attributs Notifications de jauge est un attribut autre que les attributs basés sur des événements, qui envoie des événements reçus par tous les contrôleurs de jauge.

La liste suivante contient des informations sur chaque attribut du groupe d'attributs Notifications de jauge :

Attribut Noeud - Cet attribut est un attribut de clé

Description
Nom du système géré de l'agent

Type
Chaîne

Noms

Nom de l'attribut
Node

Nom de la colonne
ORIGINNODE

Attribut Horodatage

Description
Date et heure locales de l'agent lors de la collecte de données

Type
Date et heure

Noms

Nom de l'attribut
Timestamp

Nom de la colonne
TIMESTAMP

Attribut Type de notification

Description
Type de la notification reçue. Décrit comment l'attribut observé de MBean a déclenché la notification.

Type
Chaîne

Noms

Nom de l'attribut
Notification_Type

Nom de la colonne
NOTIFICATI

Attribut ID contrôleur

Description
ID du contrôleur ayant généré cette notification

Type
Entier

Noms

Nom de l'attribut
Monitor_ID

Nom de la colonne
MONITOR_ID

Attribut MBean observé

Description
Le MBean dont l'attribut est en cours de surveillance

Type
Chaîne

Noms

Nom de l'attribut
Observed_MBean

Nom de la colonne
OBSERVED_M

Attribut Attribut observé

Description
Nom de l'attribut surveillé dans le MBean observé

Type
Chaîne

Noms

Nom de l'attribut
Observed_Attribute

Nom de la colonne
OBSERVED_A

Attribut Seuil bas

Description
Seuil au-dessous duquel le contrôleur surveille l'attribut observé

Type
Chaîne

Noms

Nom de l'attribut
Low_Threshold

Nom de la colonne
LOW_THRESH

Attribut Seuil haut

Description
Seuil au-dessous duquel le contrôleur surveille l'attribut observé

Type
Chaîne

Noms

Nom de l'attribut
High_Threshold

Nom de la colonne
HIGH_THRES

Attribut Valeur de jauge

Description
Valeur de la jauge ayant déclenché la notification

Type
Chaîne

Noms

Nom de l'attribut
Gauge_Value

Nom de la colonne
MODULUSGAUGE_VALU

Attribut Horodatage de notification

Description
Date et heure du déclenchement de la notification

Type
Date et heure

Noms

Nom de l'attribut
Notification_Time_Stamp

Nom de la colonne
NOTIFICAT0

Attribut Message de notification

Description
Message figurant dans la notification

Type
Chaîne

Noms

Nom de l'attribut
Notification_Message

Nom de la colonne
NOTIFICAT1

Moniteurs enregistrés
Le groupe d'attributs Moniteurs enregistrés est basé sur des événements, et affiche une liste de tous les contrôleurs JMX créés par l'agent.

La liste suivante contient des informations sur chaque attribut du groupe d'attributs Moniteurs enregistrés :

Attribut Noeud - Cet attribut est un attribut de clé

Description
Nom du système géré de l'agent

Type
Chaîne

Noms

Nom de l'attribut
Noeud

Nom de la colonne
ORIGINNODE

Attribut Horodatage

Description
Date et heure locales de l'agent lors de la collecte de données

Type
Date et heure

Noms

Nom de l'attribut
Horodatage

Nom de la colonne
TIMESTAMP

Attribut ID contrôleur - cet attribut est un attribut de clé

Description
Identificateur entier unique d'un contrôleur

Type
Entier

Noms

Nom de l'attribut
Monitor_ID

Nom de la colonne
MONITOR_ID

Attribut Paramètres de contrôleur

Description
Paramètres servant à créer le contrôleur

Type
Chaîne

Noms

Nom de l'attribut
Monitor_Parameters

Nom de la colonne
MONITOR_PA

Attribut Nom de contrôleur

Description
Nom d'objet JMX du MBean de contrôleur

Type
Chaîne

Noms

Nom de l'attribut
Monitor_Name

Nom de la colonne
MONITOR_NA

Notifications de chaîne
Le groupe d'attributs Notifications de chaîne est un groupe d'attributs autre que les attributs basés sur des événements qui sont reçus par tous les contrôleurs de chaînes.

La liste suivante contient des informations sur chaque attribut du groupe d'attributs Notifications de chaîne :

Attribut Noeud - Cet attribut est un attribut de clé

Description
Nom du système géré de l'agent

Type
Chaîne

Noms

Nom de l'attribut
Node

Nom de la colonne
ORIGINNODE

Attribut Horodatage

Description
Date et heure locales de l'agent lors de la collecte de données

Type
Date et heure

Noms

Nom de l'attribut
Timestamp

Nom de la colonne
TIMESTAMP

Attribut Type de notification

Description
Type de la notification reçue. Décrit comment l'attribut observé de MBean a déclenché la notification.

Type
Chaîne

Noms

Nom de l'attribut
Notification_Type

Nom de la colonne
NOTIFICATI

Attribut ID contrôleur - cet attribut est un attribut de clé

Description
Identificateur entier unique d'un contrôleur

Type
Entier

Noms

Nom de l'attribut
Monitor_ID

Nom de la colonne
MONITOR_ID

Attribut MBean observé

Description
Le MBean dont l'attribut est en cours de surveillance

Type
Chaîne

Noms

Nom de l'attribut
Observed_MBean

Nom de la colonne
OBSERVED_M

Attribut Attribut observé

Description
Nom de l'attribut surveillé dans le MBean observé

Type
Chaîne

Noms

Nom de l'attribut
Observed_Attribute

Nom de la colonne
OBSERVED_A

Attribut Chaîne de comparaison

Description
Chaîne utilisée dans l'opération de comparaison

Type
Chaîne

Noms

Nom de l'attribut
Compare_String

Nom de la colonne
COMPARE_ST

Attribut Valeur de chaîne

Description
Valeur de l'attribut ayant déclenché la notification

Type
Chaîne

Noms

Nom de l'attribut
String_Value

Nom de la colonne
STRING_VAL

Attribut Horodatage de notification

Description
Date et heure du déclenchement de la notification

Type
Date et heure

Noms

Nom de l'attribut
Notification_Time_Stamp

Nom de la colonne
NOTIFICAT0

Attribut Message de notification

Description
Message figurant dans la notification

Type
Chaîne

Noms

Nom de l'attribut
Notification_Message

Nom de la colonne
NOTIFICAT1

Groupes d'attributs d'événements SNMP

Les groupes d'attributs d'événements SNMP servent à recevoir des messages d'alerte et des informations. Ce sont des groupes d'attributs basés sur des événements.

La liste suivante contient des informations sur chaque attribut appartenant aux groupes d'attributs d'événements SNMP :

Remarque : Vous pouvez modifier le nom affiché par défaut de ces attributs. Les noms affichés sont distincts de l'ID interne de chaque attribut.

ID_Objet_Entreprise
ID objet de l'entreprise qui a généré l'alerte.

Adresse_Source
Nom d'hôte ou adresse IP de l'agent SNMP ayant envoyé l'alerte.

Alerte_Générique
Numéro d'alerte générique extrait de l'alerte reçue. Les valeurs possibles sont :

```
0 ColdStart (Démarrage à froid)
1 WarmStart (Démarrage à chaud)
2 LinkDown (Liaison brisée)
3 LinkUp (Liaison établie)
4 Authentication Failure (Echec d'authentification)
5 EGPNeighborLoss (Perte d'un EGP voisin)
```

Alerte_Spécifique
Numéro d'alerte spécifique à l'entreprise qui est extrait de l'alerte reçue. S'applique uniquement lorsque la valeur de Alerte_Générique = 6.

Nom_Alerte
Nom de l'alerte tel que spécifié dans la définition du fichier de configuration des alertes.

Catégorie
Catégorie de l'alerte telle que spécifiée dans la définition du fichier de configuration des alertes.

Description
Description de l'alerte telle que spécifiée dans la définition du fichier de configuration des alertes. La longueur maximale de la description est de 256 caractères.

Nom_Entreprise
Nom d'entreprise associé à l'alerte tel que spécifié dans le fichier de configuration des alertes et déterminé via l'ID objet de l'alerte.

Statut_Source
Statut de l'agent déclencheur de l'alerte après l'avoir envoyée, tel que spécifié dans la définition d'alerte du fichier de configuration des alertes.

Type_Source
Type de l'agent ayant généré l'alerte tel que spécifié dans la définition d'alerte du fichier de configuration des alertes.

Variables_Evénement
Données VarBind reçues dans l'unité de données de protocole (PDU) de l'alerte. La chaîne est structurée comme suit :

```
{OID[type]=valeur}{OID[type]=valeur}{oid[type]=valeur}...
```

Où :

oid
ID objet de variable MIB

type
Type de données SMI

valeur
Valeur de la variable

{}
Chaque triplet est encadré par des accolades ({}).

Remarque : Les attributs Nom_Alerte, Catégorie, Description, Nom_Entreprise, Statut_Source et Type_Source fournissent des informations supplémentaires. Dans la fenêtre **Navigateur MIB SNMP**, cochez la case **Inclure les attributs qui présentent les informations définies dans le fichier de configuration d'alerte** pour inclure ces attributs.

Groupes d'attributs d'événements JMX

Les groupes d'attributs d'événements JMX servent à recevoir des notifications d'un serveur MBean.

Ils correspondent à des groupes d'attributs autres que ceux basés sur des événements et sont générés à l'aide des attributs ci-dessous qui peuvent être modifiés par le développeur d'agent.

La liste suivante contient des informations relatives à chaque attribut dans les groupe d'attributs d'événements JMX :

Attribut Noeud - Cet attribut est un attribut de clé

Description
Nom du système géré de l'agent

Type
Chaîne

Noms

Nom de l'attribut
Node

Nom de la colonne
ORIGINNODE

Attribut Horodatage

Description
Date et heure locales de l'agent lors de la collecte de données

Type
Date et heure

Noms

Nom de l'attribut
Timestamp

Nom de la colonne
TIMESTAMP

Attribut Type

Description
Type de notification

Type
Chaîne

Noms

Nom de l'attribut
Type

Nom de la colonne
TYPE

Attribut Source

Description
MBean ayant été à l'origine de l'envoi de la notification

Type
Chaîne

Noms

Nom de l'attribut
Source

Nom de la colonne
SOURCE

Attribut Numéro de séquence

Description
Numéro de séquence de l'objet de notification

Type
Chaîne

Noms

Nom de l'attribut
Sequence_Number

Nom de la colonne
SEQUENCE_N

Attribut Message

Description
Message de notification

Type
Chaîne

Noms

Nom de l'attribut
Message

Nom de la colonne
MESSAGE

Attribut Données utilisateur

Description
Objet de données utilisateur issu de la notification

Type
Chaîne

Noms

Nom de l'attribut
User_Data

Nom de la colonne
USER_DATA

Groupe d'attributs Ping

Le groupe d'attributs Ping contient les résultats des pings ICMP envoyés aux listes de périphériques.

La liste suivante contient des informations sur chaque attribut du groupe d'attributs Ping :

Attribut Noeud - Cet attribut est un attribut de clé

Description
Nom du système géré de l'agent.

Type
Chaîne

Noms

Nom de l'attribut
Node

Nom de la colonne
ORIGINNODE

Attribut Horodatage

Description
Heure collectée du système d'agent à laquelle la ligne de données a été générée et envoyée de l'agent à Tivoli Enterprise Monitoring Server. ou stockée à des fins d'historique. Elle représente le fuseau horaire local du système d'agent.

Type
Date et heure

Noms

Nom de l'attribut
Timestamp

Nom de la colonne
TIMESTAMP

Attribut Adresse - Cet attribut est un attribut de clé

Description
Adresse IP de l'hôte surveillé.

Type
Chaîne avec valeur énumérée. La valeur UNKNOWN_ADDRESS est affichée si l'adresse IP est inconnue. L'entrepôt de données et les requêtes renvoient 0.0.0.0 pour cette énumération. Toute autre valeur d'adresse IP est affichée telle quelle.

Noms

Nom de l'attribut
Address

Nom de la colonne
PNGADDR

Attribut Entrée de périphérique - Cet attribut est un attribut de clé

Description
Entrée du fichier liste de périphériques associé à ce noeud.

Type
Chaîne

Noms

Nom de l'attribut
Device_Entry

Nom de la colonne
PINGDEVC

Attribut Temps de réponse actuel

Description
Temps de réponse actuel du réseau pour les demandes ICMP adressées au noeud géré (en millisecondes).

Type
Entier avec valeurs énumérées. Les chaînes sont affichées dans Tivoli Enterprise Portal. L'entrepôt de données et les requêtes renvoient des nombres. Les valeurs définies sont `TIMEOUT(-1)` et `SEND_FAILURE(-2)`. Les autres valeurs affichent la valeur numérique.

Noms

Nom de l'attribut
Current_Response_Time

Nom de la colonne
PINGRSTM

Attribut Nom

Description
Nom d'hôte du noeud géré. Si l'adresse du noeud ne peut pas être résolue par le DNS, l'adresse IP en notation décimale à point est alors affichée.

Type
Chaîne avec valeur énumérée. La valeur UNKNOWN_HOSTNAME est affichée si le nom d'hôte est inconnu. L'entrepôt de données et les requêtes renvoient 0.0.0.0 pour cette énumération. Toute autre valeur de nom d'hôte est affichée telle quelle.

Noms

Nom de l'attribut
Name

Nom de la colonne
PNGNAME

Attribut Description du noeud

Description
Description du noeud géré.

Type
Chaîne

Noms

Nom de l'attribut
Node_Description

Nom de la colonne
PNGDESC

Attribut Statut du noeud

Description
Statut de fonctionnement courant du noeud géré.

Type
Entier avec valeurs énumérées. Les chaînes sont affichées dans Tivoli Enterprise Portal. L'entrepôt de données et les requêtes renvoient des nombres. Les valeurs définies sont `INVALID(-2)`, `UNKNOWN(-1)`, `INACTIVE(0)` et `ACTIVE(1)`.

Noms

Nom de l'attribut
Node_Status

Nom de la colonne
PNGSTAT

Attribut Type de noeud

Description
Type du noeud géré. Si le noeud est en ligne, il s'agit d'un noeud IP. S'il est hors ligne, il est de type Inconnu.

Type
Entier avec valeurs énumérées. Les chaînes sont affichées dans Tivoli Enterprise Portal. L'entrepôt de données et les requêtes renvoient des nombres. Les valeurs définies sont `UNKNOWN(0)` et `IP NODE(1)`.

Noms

Nom de l'attribut
Node_Type

Nom de la colonne
PNGTYPE

Attribut Horodatage de statut

Description
Date et heure auxquelles le noeud a été contrôlé pour la dernière fois.

Type
Date et heure

Noms

Nom de l'attribut
Status_Timestamp

Nom de la colonne
PNGTMSP

Groupes d'attributs HTTP

Les deux groupes d'attributs HTTP, `URL gérées` et `Objets d'URL`, permettent de recevoir des informations depuis les URL et les objets qu'elles contiennent.

Pour plus d'informations sur la syntaxe utilisée dans les tables des URL gérées et des objets d'URL, voir («Zones spécifiques des attributs HTTP», à la page 1338).

URL gérées

La liste suivante contient des informations sur chaque attribut du groupe d'attributs des URL gérées :

Attribut Noeud - Cet attribut est un attribut de clé

Description
Nom du système géré de l'agent

Type
Chaîne

Noms

Nom de l'attribut
Node

Nom de la colonne
ORIGINNODE

Attribut Horodatage

Description
Date et heure locales de l'agent lors de la collecte de données

Type
Date et heure

Noms

Nom de l'attribut
Timestamp

Nom de la colonne
TIMESTAMP

Attribut URL - Cet attribut est un attribut de clé

Description
URL en cours de surveillance.

Type
Chaîne

Noms

Nom de l'attribut
URL

Nom de la colonne
HTTPURL

Attribut Temps de réponse

Description
Temps de téléchargement de la réponse en millisecondes.

Type
Entier avec valeur énumérée. La chaîne est affichée dans Tivoli Enterprise Portal, l'entrepôt de données et les requêtes renvoient le nombre. La valeur définie est `TIMEOUT (-1)`.

Noms

Nom de l'attribut
Response_Time

Nom de la colonne
HTTPURL

Attribut Taille de page

Description
Taille de la page renvoyée par la requête HTTP.

Type
Entier avec valeur énumérée. La chaîne est affichée dans Tivoli Enterprise Portal, l'entrepôt de données et les requêtes renvoient le nombre. La valeur définie est `NO_RESPONSE_RECEIVED(-1)`.

Noms

Nom de l'attribut
Page_Size

Nom de la colonne
PAGESZ

Attribut Objets de page

Description
Nombre total d'objets associés à la page surveillée.

Type
Entier avec valeur énumérée. La chaîne est affichée dans Tivoli Enterprise Portal, l'entrepôt de données et les requêtes renvoient le nombre. La valeur définie est `NOT_COLLECTED(-1)`.

Noms

Nom de l'attribut
Page_Objects

Nom de la colonne
PGOBJS

Attribut Taille totale des objets

Description
Taille de la page renvoyée par la requête HTTP.

Type
Entier avec valeur énumérée. La chaîne est affichée dans Tivoli Enterprise Portal, l'entrepôt de données et les requêtes renvoient le nombre. La valeur définie est `NOT_COLLECTED(-1)`.

Noms

Nom de l'attribut
Total_Object_Size

Nom de la colonne
TOTOSZ

Attribut Titre de page

Description
Titre de la page d'URL reçue.

Type
Chaîne

Noms

Nom de l'attribut
Page_Title

Nom de la colonne
PAGETTL

Attribut Type du serveur

Description
Type de serveur utilisé sur le site Web de l'URL cible.

Type
Chaîne

Noms

Nom de l'attribut
Server_Type

Nom de la colonne
SRVTYP

Attribut Code de réponse

Description
Code de réponse de la requête HTTP.

Type
Entier avec valeur énumérée. La chaîne est affichée dans Tivoli Enterprise Portal, l'entrepôt de données et les requêtes renvoient le nombre. La valeur définie est `NO_RESPONSE_RECEIVED(-1)`.

Noms

Nom de l'attribut
Response_Code

Nom de la colonne
CODE

Attribut Statut

Description
Statut actuel de l'URL gérée (OK ou description du statut).

Type
Chaîne

Noms

Nom de l'attribut
Status

Nom de la colonne
STATUS

Attribut Alias d'URL

Description
Alias spécifié par l'utilisateur pour l'URL.

Type
Chaîne

Noms

Nom de l'attribut
URL_Alias

Nom de la colonne
ALIAS

Attribut Données utilisateur

Description
Données utilisateur spécifiées avec l'URL.

Type
Chaîne

Noms

Nom de l'attribut
User_Data

Nom de la colonne
USER

Objets d'URL

La liste suivante contient des informations sur chaque attribut du groupe d'attributs des objets d'URL :

Attribut Noeud - Cet attribut est un attribut de clé

Description
Nom du système géré de l'agent

Type
Chaîne

Noms

Nom de l'attribut
Node

Nom de la colonne
ORIGINNODE

Attribut Horodatage

Description
Date et heure locales de l'agent lors de la collecte de données

Type
Date et heure

Noms

Nom de l'attribut
Timestamp

Nom de la colonne
TIMESTAMP

Attribut URL - Cet attribut est un attribut de clé

Description
URL en cours de surveillance.

Type
Chaîne

Noms

Nom de l'attribut
URL

Nom de la colonne
HTTPURL

Attribut Nom d'objet

Description
Nom de l'objet page dans l'URL cible.

Type
Chaîne

Noms

Nom de l'attribut
Object_Name

Nom de la colonne
ONAME

Attribut Taille d'objet

Description
Taille en octets de l'objet page dans l'URL cible.

Type
Entier avec valeurs énumérées. Les chaînes sont affichées dans Tivoli Enterprise Portal. L'entrepôt de données et les requêtes renvoient des nombres. Les valeurs définies sont `NOT_COLLECTED (-1)` et `OBJECT_NOT_FOUND (-2)`. Les autres valeurs affichent la valeur numérique.

Noms

Nom de l'attribut
Object_Size

Nom de la colonne
SIZE

Attribut Temps de réponse de l'objet

Description
Temps de téléchargement de l'objet en millisecondes.

Type
Entier avec valeurs énumérées. Les chaînes sont affichées dans Tivoli Enterprise Portal. L'entrepôt de données et les requêtes renvoient des nombres. Les valeurs définies sont `NOT_COLLECTED (-1)`, `NO_RESPONSE_RECEIVED (-2)` et `STATUS_CODE_ERROR (-3)`. Les autres valeurs affichent la valeur numérique.

Noms

Nom de l'attribut
Object_Response_Time

Nom de la colonne
ORTIME

Groupes d'attributs de reconnaissance

Groupe d'attributs qui représente l'ensemble des instances de sous-noeud définies pour un type de sous-noeud

Lors de la création d'un type de sous-noeud, un groupe d'attributs est créé ; celui-ci représente l'ensemble des instances de sous-noeud définies pour ce type de sous-noeud. Chacun de ces groupes d'attributs comprend le même ensemble d'attributs.

La liste suivante contient des informations sur chaque attribut du groupe d'attributs Reconnaissance. Le nom en gras montre comment l'attribut s'affiche dans Tivoli Enterprise Portal :

Attribut Noeud - Cet attribut est un attribut de clé

Description
Nom du système géré de l'agent

Type
Chaîne

Noms

Nom de l'attribut
Node

Nom de la colonne
ORIGINNODE

Attribut Horodatage

Description
Heure du système d'agent à laquelle la ligne de données a été générée et envoyée à Tivoli Enterprise Monitoring Server (ou stockée pour des opérations historiques). Elle représente le fuseau horaire local du système d'agent.

Type
Date et heure

Noms

Nom de l'attribut
Timestamp

Nom de la colonne
TIMESTAMP

Attribut Nom de système géré du sous-noeud

Description
Nom de système géré de l'agent de sous-noeud.

Type
Chaîne

Noms

Nom de l'attribut
Subnode_MSN

Nom de la colonne
SN_MSN

Attribut Affinité de sous-noeud

Description
Affinité de l'agent de sous-noeud.

Type
Chaîne

Noms

Nom de l'attribut
Subnode_Affinity

Nom de la colonne
SN_AFFIN

Attribut Type de sous-noeud

Description
Type de noeud de ce sous-noeud.

Type
Chaîne

Noms

Nom de l'attribut
Subnode_Type

Nom de la colonne
SN_TYPE

Attribut Nom de ressource du sous-noeud

Description
Nom de ressource de l'agent de sous-noeud.

Type
Chaîne

Noms

Nom de l'attribut
Subnode_Resource_Name

Nom de la colonne
SN_RES

Attribut Version de sous-noeud

Description
Version de l'agent du sous-noeud.

Type

Noms

Nom de l'attribut
Subnode_Version

Nom de la colonne
SN_VER

Groupe d'attributs Statut d'action

Le groupe d'attributs Statut d'action contient le statut des actions traitées par l'agent.

Ce groupe d'attributs est basé sur les événements et contient des informations sur chaque attribut du groupe d'attributs Statut d'action :

Attribut Noeud - Cet attribut est un attribut de clé

Description
Nom du système géré de l'agent.

Type
Chaîne

Noms

Nom de l'attribut
Node

Nom de la colonne
ORIGINNODE

Attribut Horodatage

Description
Heure collectée du système d'agent, à laquelle la ligne de données a été générée et envoyée de l'agent à Tivoli Enterprise Monitoring Server. ou stockée à des fins d'historique. Elle représente le fuseau horaire local du système d'agent.

Type
Date et heure

Noms

Nom de l'attribut
Timestamp

Nom de la colonne
TIMESTAMP

Attribut Nom d'action

Description
Nom de l'action qui a été exécutée.

Type
Chaîne

Noms

Nom de l'attribut
Action_Name

Nom de la colonne
TSKNAME

Attribut Statut d'action

Description
Statut de l'action.

Type
Entier avec valeurs énumérées. Les valeurs sont : OK (0), NOT_APPLICABLE (1), GENERAL_ERROR (2), WARNING (3), NOT_RUNNING (4), DEPENDENT_NOT_RUNNING (5), ALREADY_RUNNING (6), PREREQ_NOT_RUNNING (7), TIMED_OUT (8), DOESNT_EXIST (9), UNKNOWN (10), DEPENDENT_STILL_RUNNING (11), INSUFFICIENT_USER_AUTHORITY (12)

Noms

Nom de l'attribut
Action_Status

Nom de la colonne
TSKSTAT

Attribut Code retour de l'application issue de l'action

Description
Code retour de l'application démarrée par l'action.

Type
Entier

Noms

Nom de l'attribut
Action_App_Return_Code

Nom de la colonne
TSKAPRC

Attribut Message d'action

Description
Message associé au code retour de l'action.

Type
Chaîne

Noms

Nom de l'attribut
Action_Message

Nom de la colonne
TSKMSGE

Attribut Instance d'action

Description
Instance associée à la sortie produite par l'exécution de l'action. Si l'action est une commande système, l'instance correspond au numéro de ligne de la sortie de la commande.

Type
Chaîne

Noms

Nom de l'attribut
Action_Instance

Nom de la colonne
TSKINST

Attribut Résultats d'action

Description
Sortie produite par l'exécution de l'action.

Type
Chaîne

Noms

Nom de l'attribut
Action_Results

Nom de la colonne
TSKOUTP

Attribut Commande Action

Description
Commande exécutée par l'action.

Type
Chaîne

Noms

Nom de l'attribut
Action_Command

Nom de la colonne
TSKCMND

Attribut Noeud d'action

Description
Noeud sur lequel l'action a été exécutée.

Type
Chaîne

Noms

Nom de l'attribut
Action_Node

Nom de la colonne
TSKORGN

Attribut Sous-noeud d'action

Description
Sous-noeud sur lequel l'action a été exécutée.

Type
Chaîne

Noms

Nom de l'attribut
Action_Subnode

Nom de la colonne
TSKSBND

Attribut ID action

Description
ID de l'action.

Type
Entier

Noms

Nom de l'attribut
Action_ID

Nom de la colonne
TSKID

Attribut Type d'action

Description
Type de l'action.

Type
Entier avec valeurs énumérées. Les chaînes sont affichées dans Tivoli Enterprise Portal, l'entrepôt de données et les requêtes renvoient les nombres. Les valeurs définies sont : UNKNOWN (0), AUTOMATION (1).

Noms

Nom de l'attribut
Action_Type

Nom de la colonne
TSKTYPE

Attribut Propriétaire d'action

Description
Nom de la situation ou utilisateur qui a initié l'action.

Type
Chaîne

Noms

Nom de l'attribut
Action_Owner

Nom de la colonne
TSKOWNR

Groupe d'attributs de statut du fichier journal

Le groupe d'attributs de statut du fichier journal contient des informations qui reflètent le statut du fichier journal que cet agent surveille.

Le groupe d'attributs Statut du fichier journal est fourni si vous avez un groupe d'attributs de journal et si la version de l'agent est la version minimale par défaut de Tivoli Monitoring, à savoir 6.2.1 ou version ultérieure. Le groupe d'attributs d'état de fichier journal contient deux attributs définis comme nombres 64 bits pour qu'ils puissent traiter des fichiers volumineux. La prise en charge de l'attribut numérique 64 bits est fournie par Tivoli Monitoring version 6.2.1 ou ultérieure.

La liste suivante contient des informations sur chaque attribut du groupe d'attributs Statut du fichier journal :

Attribut Noeud - Cet attribut est un attribut de clé

Description
Nom du système géré de l'agent.

Type
Chaîne

Noms

Nom de l'attribut
Node

Nom de la colonne
ORIGINNODE

Attribut Horodatage

Description
La valeur est l'heure collectée du système d'agent à laquelle la ligne de données a été créée et envoyée de l'agent à Tivoli Enterprise Monitoring Server ou stockée à des fins d'historique. Elle représente le fuseau horaire local du système d'agent.

Type
Date et heure

Noms

Nom de l'attribut
Timestamp

Nom de la colonne
TIMESTAMP

Attribut de nom de table - Cet attribut est un attribut de clé

Description
Nom de la table dans laquelle ce journal est surveillé

Type
Chaîne

Noms

Nom de l'attribut
Table_Name

Nom de la colonne
TBLNAME

Attribut de nom de fichier - Cet attribut est un attribut de clé

Description
Nom du fichier à surveiller

Type
Chaîne

Noms

Nom de l'attribut
File_Name

Nom de la colonne
FILNAME

Attribut de modèle RegEx - Cet attribut est un attribut de clé

Description
Modèle d'expression régulière (le cas échéant) qui a entraîné la surveillance de ce fichier.

Type
Chaîne

Noms

Nom de l'attribut
RegEx_Pattern

Nom de la colonne
REPATRN

Attribut Type de fichier

Description
Type du fichier (fichier standard ou canal de communication)

Type
Entier avec valeurs énumérées. Les chaînes sont affichées dans Tivoli Enterprise Portal. Les valeurs définies sont UNKNOWN(0), REGULAR FILE(1) et PIPE(2)

Noms

Nom de l'attribut
File_Type

Nom de la colonne
FILTYPE

Attribut Statut de fichier

Description
Etat du fichier à surveiller

Type
Entier avec valeurs énumérées. Les chaînes sont affichées dans Tivoli Enterprise Portal. Les valeurs définies sont : OK(0), PERMISSION DENIED(1), FILE DOES NOT EXIST(2), INTERRUPTED SYSTEM CALL(4), I/O ERROR(5), NO SUCH DEVICE(6), BAD FILE NUMBER(9), OUT OF MEMORY(12), ACCESS DENIED(13), RESOURCE BUSY(16), NOT A DIRECTORY(20), IS A DIRECTORY(21), INVALID ARGUMENT(22), FILE TABLE OVERFLOW(23), TOO MANY OPEN FILES(24), TEXT FILE BUSY(26), FILE TOO LARGE(27), NO SPACE LEFT ON DEVICE(28), ILLEGAL SEEK ON PIPE(29), READ-ONLY FILE SYSTEM(30), TOO MANY LINKS(31), BROKEN PIPE(32)

Noms

Nom de l'attribut
File_Status

Nom de la colonne
FILSTAT

Attribut Nombre d'enregistrements correspondants

Description
Nombre d'enregistrements traités de ce journal qui correspondent à l'un des modèles spécifiés

Type
Entier

Noms

Nom de l'attribut
Num_Records_Matched

Nom de la colonne
RECMTCH

Attribut Nombre d'enregistrements non correspondants

Description
Nombre d'enregistrements traités envoyés au journal UnmatchLog (qui ne correspondent à aucun modèle)

Type
Entier

Noms

Nom de l'attribut
Num_Records_Not_Matched

Nom de la colonne
RECUNMT

Attribut Nombre d’enregistrements traités

Description
Nombre d'enregistrements traités de ce journal depuis le démarrage de l'agent (y compris ceux qui ne sont pas des correspondances/événements)

Type
Entier

Noms

Nom de l'attribut
Num_Records_Processed

Nom de la colonne
RECPROC

Attribut Position actuelle dans le fichier

Description
Position actuelle en octets dans le fichier surveillé. Jusqu'à ce point, les données sont traitées, au-delà de ce point, les données ne le sont pas. Non applicable aux canaux de communication.

Type
Entier

Noms

Nom de l'attribut
Current_File_Position

Nom de la colonne
OFFSET

Attribut Taille du fichier actuelle

Description
Taille actuelle du fichier surveillé. Non applicable aux canaux de communication.

Type
Entier

Noms

Nom de l'attribut
Current_File_Size

Nom de la colonne
FILESIZE

Attribut Heure de la dernière modification

Description
Heure de la dernière opération d'écriture dans le journal surveillé. Non applicable aux canaux de communication.

Type
Horodatage

Noms

Nom de l'attribut
Last_Modification_Time

Nom de la colonne
LASTMOD

Attribut Page de codes

Description
Page de codes de langue du fichier surveillé

Type
Chaîne

Noms

Nom de l'attribut
Codepage

Nom de la colonne
CODEPG

Groupe d'attributs Statistiques RegEx du fichier journal

Le groupe d'attributs Statistiques RegEx du fichier journal contient des informations qui présentent les statistiques des recherches d'expressions régulières du fichier journal.

Les expressions régulières peuvent être utilisées pour filtrer ou pour définir les enregistrements. Ce groupe d'attributs affiche des informations sur les deux types. Lorsque l'attribut Type de résultat contient `INCLUDE` ou `EXCLUDE`, le filtre est utilisé pour filtrer les enregistrements. Si l'attribut Type de résultat contient `BEGIN` or `END`, le filtre est utilisé pour définir les enregistrements. Les mesures de l'unité centrale sont approximatives et dépendent de la granularité des données exposées par le système d'exploitation. Ces mesures peuvent générer la valeur `0.00` lorsque l'évaluation d'une expression régulière prend peut de temps. Utilisez les temps UC pour déterminer le coût relatif des expressions régulières et optimiser le comportement des expressions régulières.

Le groupe d'attributs Statistiques RegEx du fichier journal est fourni si vous avez un groupe d'attributs de journal et si la version minimale de l'agent Tivoli Monitoring correspond à la 6.2.1. La version minimale Tivoli Monitoring Version est sélectionnée dans la page **Informations d'agent**. Pour plus d'informations, voir «Désignation et configuration de l'agent», à la page 1204. Le groupe d'attributs Statistiques RegEx du fichier journal contient des attributs définis en tant que nombres 64 bits, ce qui leur permet de gérer de longues durées. La prise en charge de l'attribut numérique 64 bits est fournie par Tivoli Monitoring version 6.2.1 ou ultérieure.

La liste suivante contient des informations relatives à chaque attribut du groupe d'attributs Statistiques RegEx de fichier journal :

Attribut Noeud - Cet attribut est un attribut de clé

Description
Nom du système géré de l'agent.

Type
Chaîne

Noms

Nom de l'attribut
Node

Nom de la colonne
ORIGINNODE

Attribut Horodatage

Description
L'heure locale sur l'agent à laquelle les données ont été collectées.

Type
Date et heure

Noms

Nom de l'attribut
Timestamp

Nom de la colonne
TIMESTAMP

Attribut de nom de table - Cet attribut est un attribut de clé

Description
Nom du groupe d'attributs de fichier journal.

Type
Chaîne

Noms

Nom de l'attribut
Table_Name

Nom de la colonne
TBLNAME

Attribut de nom d'attribut - Cet attribut est un attribut de clé

Description
Nom de l'attribut auquel s'applique ce filtre.

Type
Chaîne

Noms

Nom de l'attribut
Attribute_Name

Nom de la colonne
ATRNAME

Numéro de filtre

Description
Numéro de séquence, démarrant à zéro, du filtre utilisé pour l'attribut.

Type
Entier (propriété numérique)

Noms

Nom de l'attribut
Filter_Number

Nom de la colonne
FLTRNUM

Attribut Type de résultat

Description
Le type de filtre peut être INCLUDE ou EXCLUDE pour accepter ou rejeter l'attribut si le filtre correspond. Il peut être BEGIN ou END pour indiquer le début ou la fin d'un enregistrement sur plusieurs lignes.

Type
Entier avec valeurs énumérées. Les chaînes sont affichées dans Tivoli Enterprise Portal. Si le filtre est utilisé pour filtrer les enregistrements, les valeurs définies sont `INCLUDE(1)` ou `EXCLUDE(2)`. Si le filtre est utilisé pour définir les enregistrements, les valeurs définies sont `BEGIN(3)` or `END(4)` .

Noms

Nom de l'attribut
Result_Type

Nom de la colonne
RSTTYPE

Attribut Temps processeur moyen

Description
Nombre moyen de temps processeur utilisé pour exécuter le filtre pour cet attribut. Le temps de processeur moyen est le temps de processeur total en secondes divisé par le nombre de filtres.

Type
Entier (jauge)

Noms

Nom de l'attribut
Average_Processor_Time

Nom de la colonne
CPUTAVG

Attribut Temps processeur

Description
Nombre total de temps processeur utilisé pour exécuter le filtre pour cet attribut. Le temps processeur est cumulatif et tronqué (non arrondi). Similaire au fichier Linux `/proc/<pid>/task/`*`unité d'exécution`*`/stat`.

Type
Entier (compteur)

Noms

Nom de l'attribut
Processor_Time

Nom de la colonne
CPUTIME

Attribut Temps processeur maximal

Description
Quantité de temps processeur maximale utilisée pour un seul traitement de filtre. Il est possible que la valeur maximale soit zéro si le filtre n'a jamais été utilisé ou que chaque traitement de filtre dure moins d'un centième de seconde.

Type
Entier (jauge)

Noms

Nom de l'attribut
Max_Processor_Time

Nom de la colonne
CPUTMAX

Attribut Temps processeur minimal

Description
Quantité de temps processeur minimale utilisée pour un seul traitement de filtre. Il est possible que la valeur minimale soit zéro si un traitement de filtre a duré moins de 0,01 seconde.

Type
Entier (jauge)

Noms

Nom de l'attribut
Min_Processor_Time

Nom de la colonne
CPUTMIN

Attribut Nombre de filtres

Description
Nombre de fois que vous avez exécuté le filtre. Utilisé avec la durée de processeur totale pour calculer la durée moyenne de traitement.

Type
Entier (compteur)

Noms

Nom de l'attribut
Filter_Count

Nom de la colonne
COUNT

Attribut Nombre de filtres en correspondance

Description
Nombre de fois que vous avez fait appel au filtre et que l'attribut correspondait.

Type
Entier (compteur)

Noms

Nom de l'attribut
Filter_Count_Matched

Nom de la colonne
COUNTMA

Attribut Nombre de filtres sans correspondance

Description
Nombre de fois que vous avez exécuté le filtre et que l'attribut ne correspondait pas.

Type
Entier (compteur)

Noms

Nom de l'attribut
Filter_Count_Unmatched

Nom de la colonne
COUNTUN

Attribut de modèle RegEx - Cet attribut est un attribut de clé

Description
Expression régulière utilisée pour la correspondance.

Type
Chaîne

Noms

Nom de l'attribut
RegEx_Pattern

Nom de la colonne
REGXPAT

Attribut Dernière heure de mise en correspondance

Description
Dernière heure d'utilisation du filtre et de mise en correspondance du résultat.

Type
Date et heure

Noms

Nom de l'attribut
Last_Matched_Time

Nom de la colonne
LASTMAT

Attribut Dernière heure d'absence de correspondance

Description
Dernière heure d'utilisation du filtre et d'absence de correspondance du résultat.

Type
Date et heure

Noms

Nom de l'attribut
Last_Unmatched_Time

Nom de la colonne
LASTUMA

Création d'extensions de prise en charge d'application pour des agents existants

Pour l'environnement IBM Tivoli Monitoring, vous pouvez générer un package installable pour distribuer des espaces de travail, des situations, des requêtes et des commandes Action personnalisés que vous avez créés sous la forme d'une extension de prise en charge d'application pour un agent existant.

Avant de commencer

Pour plus d'informations sur la manière de créer des situations personnalisées, des espaces de travail, des commandes Action et des requêtes, voir («Création d'espaces de travail, de commandes Action et de situations», à la page 1411).

Pourquoi et quand exécuter cette tâche

Important : Cette tâche n'aborde pas la procédure d'ajout de prise en charge d'application à un agent en cours de génération. Pour ajouter la prise en charge d'application à un agent en cours de génération, voir («Importation des fichiers de prise en charge de l'application», à la page 1447).

Procédure

1. Dans Agent Builder, sélectionnez **Fichier** > **Nouveau** > **Autre**.
2. Sélectionnez **Extension de la prise en charge de l'application Agent Builder** sous **Agent Builder**.
3. Cliquez sur **Suivant** pour accéder à l'écran d'accueil de l'assistant **Extension de prise en charge d'application IBM Tivoli Monitoring**.
4. Cliquez sur **Suivant** sur la page d'accueil.
5. Entrez un nom pour le projet et cliquez sur **Terminer**.

Création d'un projet d'extension de prise en charge d'application

Créez un projet d'extension de prise en charge d'application à l'aide du générateur d'agents.

Procédure

1. Dans Agent Builder, sélectionnez **Fichier** > **Nouveau** > **Autre**.
2. Sélectionnez **Extension de la prise en charge de l'application Agent Builder** sous **Agent Builder**.
3. Cliquez sur **Suivant** pour accéder à l'écran d'accueil de l'assistant **Extension de prise en charge d'application IBM Tivoli Monitoring**.
4. Cliquez sur **Suivant** sur la page d'accueil.
5. Entrez un nom pour le projet et cliquez sur **Terminer**.

Ajout de fichiers de prise en charge dans un projet

Ajoutez vos fichiers de prise en charge à un projet d'extension de prise en charge d'application

Avant de commencer
Création d'un projet d'extension de prise en charge d'application. Pour plus d'informations, voir «Création d'un projet d'extension de prise en charge d'application», à la page 1516.

Procédure

1. Cliquez avec le bouton droit de la souris sur un projet d'extension de prise en charge d'application et sélectionnez **IBM Tivoli** > **Importer des extensions de prise en charge d'application**
2. Dans la fenêtre **Informations d'importation**, sélectionnez le nom du système hôte sur lequel réside le serveur Tivoli Enterprise Portal ou cliquez sur **Ajouter** pour en ajouter un.
3. Dans la zone **Application**, entrez le code produit de l'agent.
4. Entrez l'affinité de l'agent pour lequel vous créez une prise en charge d'application personnalisée.

   L'affinité d'agent est un identificateur interne Tivoli Monitoring qui associe des espaces de travail, des requêtes et d'autres éléments à l'agent. Elle doit être unique dans l'installation de Tivoli Monitoring. Cliquez sur **Parcourir** pour ouvrir la fenêtre **Types de noeud** et sélectionner cette information dans une liste plutôt que de la saisir.
5. Lorsque les informations d'importation entrées vous conviennent, cliquez sur **Terminer**.
6. Dans la fenêtre **Situations**, sélectionnez les situations à importer dans la liste Situations disponibles.

   Cliquez sur **<<** pour les ajouter à la liste Situations sélectionnées, puis cliquez sur **OK**. Un nouveau dossier est créé dans le projet et il contient les fichiers nécessaires pour installer les espaces de travail, les situations et les requêtes.
7. Dans la fenêtre **Requêtes**, sélectionnez les requêtes à importer dans la liste Requêtes disponibles.

   Cliquez sur **<<** pour les ajouter à la liste Requêtes sélectionnées, puis cliquez sur **OK**.
8. Dans la fenêtre **Appliquer des actions**, sélectionnez les commandes Action à importer dans la liste Commandes Action disponibles.

   Cliquez sur **<<** pour les ajouter à la liste Commandes Action sélectionnées, puis cliquez sur **OK**. Les fichiers de prise en charge de l'agent sont placés dans le projet dans le dossier approprié.

Que faire ensuite

Vous pouvez répéter cette procédure pour autant d'agents différents que vous le souhaitez. Agent Builder crée une image d'installation unique à partir de tous les fichiers de prise en charge que contient le projet d'extension de la prise en charge d'application.

Génération de l'image d'installation de l'extension de prise en charge d'application

Générez une image d'installation d'extension de prise en charge d'application.

Procédure

1. Cliquez avec le bouton droit de la souris sur le projet Extension de prise en charge d'application et sélectionnez **IBM Tivoli** > **Créer une image d'installation d'extension de prise en charge d'application**.
2. Dans la fenêtre **Informations sur l'extension de la prise en charge d'application**, indiquez le répertoire où l'image doit être placée.
3. Votre extension de prise en charge d'application doit avoir son propre code produit. Entrez le code produit enregistré de votre nouvel agent. Vous pouvez utiliser l'un des codes produit qui sont réservés pour l'utilisation avec Agent Builder. Les valeurs admises sont `K00-K99,K{0-2}{A-Z}` et `K{4-9}{A-Z}`.

   Remarque : Ces valeurs sont réservées uniquement à une utilisation interne et ne sont pas destinées aux agents à partager ou vendre. Si vous créez un agent à partager avec d'autres personnes, vous devez envoyer une note à toolkit@us.ibm.com pour réserver un code produit. La demande de code produit doit inclure une description de l'agent à générer. Un code produit est ensuite attribué et enregistré, puis il vous est renvoyé. Lorsque vous recevez le code produit de 3 lettres, vous devez permettre à Agent Builder d'utiliser le code produit attribué.
4. Entrez le nom de l'extension de prise en charge d'application.
5. Entrez une description de l'extension de prise en charge d'application.

6. Indiquez une version pour l'extension de prise en charge d'application au format VVRRMMFF, où `vv` est le numéro de la version, `rr` le numéro de l'édition, `mm` le numéro de modification (numéro de groupe de correctifs) et `ff` le numéro du correctif temporaire.
7. Cliquez sur **Terminer**.

Installation de l'extension de prise en charge d'application

Installez votre extension de prise en charge d'application

Procédure

1. Transférez votre image sur le serveur Tivoli Enterprise Monitoring Server et sur les serveurs Tivoli Enterprise Portal Server.
2. Pour installer la prise en charge de Tivoli Enterprise Monitoring Server, exécutez l'une des commandes suivantes :
   - Sous Windows : `install`*`KXX`*`TEMSSupport.bat`
   - Sous UNIX : `install`*`KXX`*`TEMSSupport.sh`

   Le format de la commande est le suivant :

   ```
   installKXXTEMSSupport[.bat | .sh] <répertoire d'installation ITM> [-s tems_host]
    [-u utilisateur_tems]  \[-p motdepasse_tems]
   ```
3. Pour installer la prise en charge de Tivoli Enterprise Portal Server, exécutez les commandes suivantes :
   - Sous Windows : `install`*`KXX`*`TEPSSupport.bat`
   - Sous UNIX : `install`*`KXX`*`TEPSSupport.sh`

   Le format de la commande est le suivant :

   ```
   installKXXTEPSSupport[.bat | .sh] répertoire installation <ITM> [-r]
   ```

   où `-r` indique que Tivoli Enterprise Portal Server doit être redémarré après l'installation.

Conversion d'un projet d'installation de solution en un projet d'extension de prise en charge d'application

Convertissez un **projet d'installation de solution** en un projet d'extension de prise en charge d'application

Pourquoi et quand exécuter cette tâche

Si vous disposez déjà d'un **projet d'installation de solution** que vous voulez convertir en projet d'extension de prise en charge d'application, procédez comme suit :

Remarque : Dans le **projet d'installation de solution**, seuls les fichiers de prise en charge sont migrés.

Procédure

1. Cliquez avec le bouton droit de la souris sur le **projet d'installation de solution**, puis sélectionnez **IBM Tivoli** > **Convertir le projet d'installation de solution.**
2. Entrez le nom d'un nouveau projet d'extension de prise en charge d'application ou sélectionnez-en un existant dans la liste.
3. Cliquez sur **Terminer**.

Génération d'un modèle de données Cognos

Agent Builder peut générer un modèle de données Cognos pour chaque agent, ce qui vous permet d'importer des informations relatives à l'agent dans Cognos Framework Manager pour créer des rapports.

Vous pouvez ouvrir et afficher ce modèle de données Cognos dans Framework Manager qui génère ensuite un package de modèles à publier dans Tivoli Common Reporting. Vous pouvez également personnaliser ou modifier le modèle de données dans Framework Manager avant sa publication.

Lorsqu'un rapport est créé, Agent Builder permet en outre d'importer un package de rapport final dans le projet Agent Builder. Cette fonctionnalité permet de générer les futurs projets d'agent à l'aide des rapports déjà inclus dans le package d'agent. Les rapports inclus dans le package de l'image d'installation de l'agent peuvent être importés dans Tivoli Common Reporting au sein de votre environnement de production.

Remarque : Dans cette documentation, les conventions suivantes sont utilisées :

- K*xx* ou k*xx* renvoie au code produit attribué à l'agent, par exemple k99.
- *dbType* renvoie à la base de données utilisée par Tivoli Data Warehouse, par exemple DB2.

Prérequis à la génération d'un modèle de données Cognos

Effectuez ces tâches avant de générer un modèle de données Cognos

Pourquoi et quand exécuter cette tâche

Remarque :

- Ces étapes doivent être effectuées une seule fois, car tous les futurs modèles de données générés avec Agent Builder utiliseront cet environnement.
- Il est conseillé de créer un environnement de développement isolé pour le test d'agents et la création de rapports.

Procédure

1. Installez et configurez («Tivoli Data Warehouse», à la page 1519).
2. Création de tables et de procédures dans Tivoli Data Warehouse.
   a) «Création de tables et de procédures dans Tivoli Data Warehouse», à la page 1519.
   b) «Remplissage de Tivoli Data Warehouse avec Tivoli Reporting and Analytics Model», à la page 1522.
3. Installez et configurez («Tivoli Common Reporting», à la page 1522).
4. Installez et configurez («Framework Manager», à la page 1523).

Tivoli Data Warehouse

A propos de Tivoli Data Warehouse.

Pour créer des rapports, un agent Tivoli Data Warehouse, un agent Warehouse Proxy et un agent Summarization and Pruning doivent être installés et configurés dans votre environnement. Pour plus d'informations, voir *IBM Tivoli Monitoring - Guide d'installation et de configuration*.

Création de tables et de procédures dans Tivoli Data Warehouse

Créez ou modifiez la table `ManagedSystem` et la procédure stockée dans Tivoli Data Warehouse.

Pourquoi et quand exécuter cette tâche

Le modèle de données généré Cognos comprend une table `ManagedSystem` qui est utilisée pour définir une dimension `ManagedSystem`. La dimension `ManagedSystem` permet de créer des rapports qui peuvent corréler des systèmes gérés. Par exemple, si l'agent est un agent de sous-noeud, la dimension permet de déterminer les sous-noeuds existants pour une instance d'agent donnée.

La table ManagedSystem n'est pas créée par Tivoli Data Warehouse. Par conséquent, lorsqu'un agent est généré dans Agent Builder, des scripts SQL sont générés pour chaque plateforme de base de données qui :

- Créez la table ManagedSystem. Utilisez ce script si la table n'existe pas dans Tivoli Data Warehouse.
- Modifiez la table ManagedSystem. Utilisez ce script si la table existe dans Tivoli Data Warehouse. Les autres produits de génération de rapports permettent de créer la table ManagedSystem, mais pas avec toutes les colonnes obligatoires.
- Créez une procédure stockée qui remplit la table ManagedSystem à partir de tables de Tivoli Data Warehouse.

N'exécutez ces scripts qu'une seule fois.

Exécution de scripts DB2 pour créer des tables et des procédures dans Tivoli Data Warehouse
Pour une base de données DB2, utilisez ces scripts pour créer des tables dans Tivoli Data Warehouse

Avant de commencer

Les scripts de DB2 se trouvent dans le répertoire suivant :

```
reports/db2/Kxx/reports/cognos_reports/itmkxx/db_scripts
```

Procédure

1. Les scripts générés (create_table.sql, alter_table.sql , et create_procedure.sql) utilisent tous *itmuser* en tant qu'ID utilisateur de Tivoli Data Warehouse. Si *itmuser* n'est pas l'ID utilisateur Tivoli Data Warehouse dans votre environnement, remplacez toutes les occurrences de *itmuser* par l'ID utilisateur correct.
2. Connectez Tivoli Data Warehouse en tant qu'utilisateur Tivoli Data Warehouse :

   ```
   db2 connect to <nom alias Tivoli Data Warehouse> user
   <id utilisateur Tivoli Data Warehouse> using <mot de passe>
   ```

3. Déterminez si la table ManagedSystem existe :

   ```
   db2 "select count(*) from sysibm.systables where name = 'MANAGEDSYSTEM'
   et creator=upper ('<ID utilisateur Tivoli Data Warehouse>')"
   ```

4. Créez ou modifiez la table.
   - Si la requête renvoie 1, la table existe. Exécutez le script alter :

     ```
     db2 -tvf alter_table.sql
     ```

   - Si la requête renvoie 0, la table n'existe pas. Exécutez le script 'create' :

     ```
     db2 -tvf create_table.sql
     ```

5. Exécutez le script de création de la procédure stockée :

   ```
   db2 -td@ -f create_procedure.sql
   ```

Exécution de scripts Oracle pour créer des tables et des procédures dans Tivoli Data Warehouse
Pour une base de données Oracle, utilisez ces scripts pour créer des tables dans Tivoli Data Warehouse

Avant de commencer

Les scripts d'Oracle se trouvent dans le répertoire suivant :

```
reports/oracle/Kxx/reports/cognos_reports/itmkxx/db_scripts
```

Procédure

1. Les scripts générés (`create_table.sql`, `alter_table.sql` , et `create_procedure.sql`) utilisent tous *itmuser* en tant qu'ID utilisateur de Tivoli Data Warehouse. Si *itmuser* n'est pas l'ID utilisateur Tivoli Data Warehouse dans votre environnement, remplacez toutes les occurrences de *itmuser* par l'ID utilisateur correct.
2. Démarrez `sqlplus` :

```
sqlplus <ID utilisateur IBM Tivoli Monitoring>/<mot de passe>@
<ID source Tivoli Data Warehouse>
```

3. Déterminez si la table ManagedSystem existe :

```
select count(*) from user_tables where table_name = 'MANAGEDSYSTEM';
```

4. Créez ou modifiez la table.
   - Si la requête renvoie `1`, la table existe. Exécutez le script alter :

     ```
     @<chemin vers alter_table.sql>;
     ```

   - Si la requête renvoie `0`, la table n'existe pas. Exécutez le script 'create' :

     ```
     @<chemin vers create_table.sql>;
     ```

5. Exécutez le script de création de la procédure stockée :

```
@<chemin vers create_procedure.sql>;
```

Exécution de scripts SQL Server 2005 et 2008 pour créer des tables et des procédures dans Tivoli Data Warehouse

Avant de commencer

Les scripts de SQL Server se trouvent dans le répertoire suivant :

```
reports/mssql/Kxx/reports/cognos_reports/itmkxx/db_scripts
```

Procédure

1. Les scripts générés (`create_table.sql`, `alter_table.sql` , et `create_procedure.sql`) utilisent tous *itmuser* en tant qu'ID utilisateur de Tivoli Data Warehouse. Si *itmuser* n'est pas l'ID utilisateur Tivoli Data Warehouse dans votre environnement, remplacez toutes les occurrences de *itmuser* par l'ID utilisateur correct.
2. Déterminez si la table `ManagedSystem` existe :

```
osql -S <Server> -U <ID utilisateur Tivoli Data Warehouse> -P <mot de passe> -d
<nom base de données Tivoli Data Warehouse> -Q "Select count(*)
from INFORMATION_SCHEMA.TABLES where table_name = 'ManagedSystem'"
```

3. Créez ou modifiez la table.
   - Si la requête renvoie `1`, la table existe. Exécutez le script alter :

     ```
     osql -S <Serveur> -U <ID utilisateur Tivoli Data Warehouse> -P <mot de passe> -d
     <nom base de données Tivoli Data Warehouse> -I -n -i <chemin vers alter_table.sql>
     ```

   - Si la requête renvoie `0`, la table n'existe pas. Exécutez le script 'create' :

     ```
     osql -S <Serveur> -U <ID utilisateur Tivoli Data Warehouse> -P <mot de passe> -d
     <nom base de données Tivoli Data Warehouse> -I -n -i <chemin vers create_table.sql>
     ```

4. Exécutez le script de création de la procédure stockée :

```
osql -S <Serveur> -U <ID utilisateur Tivoli Data Warehouse> -P
<mot de passe> -d <nom base de données Tivoli Data Warehouse>
-I -n -i <chemin vers create_procedure.sql>
```

Remplissage de Tivoli Data Warehouse avec Tivoli Reporting and Analytics Model
Utilisez des scripts de base de données pour remplir Tivoli Data Warehouse

Pourquoi et quand exécuter cette tâche

Tivoli Reporting and Analytics Model (TRAM) contient l'ensemble des connaissances communes à tous les packages de génération de rapports. TRAM est installé par un ensemble de scripts unique à chaque base de données. Les scripts nécessaires pour le remplissage de chaque base de données prise en charge sont inclus dans l'image d'installation d'agent, dans le répertoire de rapports. Procédez comme suit pour créer des dimensions communes de Tivoli Reporting and Analytics Model dans Tivoli Data Warehouse.

Procédure

1. Recherchez les scripts de base de données Tivoli Reporting and Analytics Model.
2. Extrayez le package d'agent.
   - Sous les systèmes Windows, le package d'agent correspond au fichier k*xx*.zip.
   - Sous les systèmes Linux et UNIX, le package d'agent correspond au fichier k*xx*.tgz.
3. Accédez aux scripts de la base de données appropriée.
   - Les scripts DB2 sont situés dans le package d'agent dans :
     ```
     reports/db2/K<xx>/reports/cognos_reports/itmk<xx>/db_scripts
     ```
   - Les scripts Oracle sont situés dans le package d'agent dans :
     ```
     reports/oracle/K<xx>/reports/cognos_reports/itmk<xx>/db_scripts
     ```
   - Les scripts Microsoft SQL Server sont situés dans le package d'agent dans :
     ```
     reports/mssql/K<xx>/reports/cognos_reports/itmk<xx>/db_scripts
     ```
4. Exécutez les scripts de base de données pour générer les dimensions communes dans Tivoli Data Warehouse. Chaque ensemble de scripts fournit un fichier readme contenant des instructions d'utilisation.
5. Vérifiez que les scripts ont ajouté les tables suivantes dans Tivoli Data Warehouse :
   ```
   "Computer System", WEEKDAY_LOOKUP, MONTH_LOOKUP, TIMEZONE_DIMENSION, TIME_DIMENSION
   ```

Tivoli Common Reporting
Tivoli Common Reporting contient le moteur Cognos Business Intelligence qui comprend des éléments d'aide à la création de rapports d'agent.

Tivoli Common Reporting doit être installé et configuré avec une source de données connectée à Tivoli Data Warehouse.

Installation de Tivoli Common Reporting

Vous devez installer Tivoli Common Reporting. Les versions 1.3, 2.1, 2.1.1 ou ultérieures sont prises en charge. Pour plus d'informations sur l'installation de Tivoli Common Reporting, voir Installation de Tivoli Common Reporting.

Configuration de Tivoli Common Reporting

Vous devez configurer Tivoli Common Reporting. Pour plus d'informations sur la configuration de Tivoli Common Reporting, voir Configuration d'IBM Tivoli Common Reporting.

Créez une source de données entre Tivoli Data Warehouse et Tivoli Common Reporting. Pour plus d'informations, voir Configuration du serveur proxy. Cliquez sur le type de base de données approprié. Veuillez noter le nom donné à la source de données. La valeur par défaut est **TDW**.

Remarque : Le nom de la source de données doit correspondre au nom de la zone **Source de données** de la page **Informations sur Cognos**. Pour plus d'informations sur la page **Informations sur Cognos**, voir «Informations Cognos», à la page 1222.

Framework Manager

Framework Manager est une application fournie avec l'application Tivoli Common Reporting, mais qui doit être installée et configurée séparément.

Framework Manager est utilisé pour afficher et modifier les modèles de données ainsi que publier les modèles de données vers Tivoli Common Reporting

Installation de Framework Manager

Vous devez installer Framework Manager. Les versions 8.4, 8.4.1 ou ultérieures sont prises en charge.

Framework Manager est fourni avec Tivoli Common Reporting, mais doit être installé manuellement. Tivoli Common Reporting 1.3 est fourni avec Framework Manager 8.4. Tivoli Common Reporting 2.1 et 2.1.1 sont fournis avec Framework Manager 8.4.1. Pour obtenir des informations sur l'installation de Framework Manager, voir Installation de Framework Manager dans le document *Tivoli Common Reporting - Guide d'utilisation*.

Configuration de Framework Manager

Vous devez configurer Framework Manager. Pour obtenir des informations sur la configuration de Framework Manager, voir Configuration de Framework Manager dans le document *Tivoli Common Reporting - Guide d'utilisation*.

Création de rapports

Utilisez Framework Manager pour publier le modèle de l'agent et Report Studio pour commencer à créer des rapports.

Avant de commencer

Lorsque l'agent est prêt, il doit être installé dans l'environnement Tivoli Monitoring. En outre, la collecte d'historique de l'agent doit être configurée et l'agent doit s'exécuter pendant au moins un intervalle de téléchargement de l'entrepôt de données. La synthèse doit être configurée et les choix de paramétrage de la synthèse effectués dans Tivoli Monitoring doivent être identiques à ceux effectués dans Agent Builder. L'agent de synthèse et d'élagage doit s'exécuter au moins une fois après le chargement des données de l'agent dans l'entrepôt de données.

1. Installez, configurez et démarrez votre agent.
2. Créez et distribuez sur l'agent une collecte d'historique pour chaque groupe d'attributs pour lequel vous souhaitez créer un rapport.

   Remarque : L'intervalle de téléchargement de l'entrepôt de données est quotidien par défaut. Vous pouvez toutefois réduire cet intervalle.

   Pour plus d'informations sur la configuration de la collecte d'historique, voir Gestion des données d'historique dans le document *IBM Tivoli Monitoring - Guide d'administration*.
3. Dans Tivoli Monitoring, configurez la récapitulation pour tous les groupes d'attributs pour lesquels vous avez créé des collectes d'historique à l'étape 2.

   Remarque : Une fois la collecte d'historique et la récapitulation configurées, vous devez attendre un certain temps pour que les données finissent de s'inscrire dans les tables récapitulatives.

   Remarque : Par défaut, l'agent de synthèse et d'élagage est configuré pour s'exécuter une fois par jour à 2 heures du matin. Si vous le souhaitez, vous pouvez modifier ce paramètre. Vous pouvez par

exemple le configurer pour qu'il s'exécute une fois par heure. Pour plus d'informations sur la configuration de Tivoli Data Warehouse, voir Paramétrage de l'entreposage des données dans le document *IBM Tivoli Monitoring - Guide d'installation et de configuration*.

Pourquoi et quand exécuter cette tâche

La génération d'un agent dans Agent Builder créé un projet Framework Manager complet qui comprend le modèle de données et le fichier de projet de Framework Manager. Framework Manager peut ouvrir le fichier de projet directement, ce qui a pour effet d'ouvrir le modèle de données à des fins de modification, de personnalisation ou de publication.

Procédure

Remarque : Le modèle de données généré pour l'agent contient toutes les périodicités pour chaque groupe d'attributs : horaire, quotidienne, hebdomadaire, mensuelle, trimestrielle et annuelle. Les dimensions existent uniquement dans Tivoli Data Warehouse pour l'agent si la synthèse et l'élagage sont configurés pour cet agent, et si les dimensions sont sélectionnées, et si l'agent de synthèse et d'élagage a créé et rempli les tables. Les rapports peuvent être définis et publiés dans Tivoli Common Reporting s'ils utilisent des dimensions inexistantes. Ces rapports ne fonctionnent que lorsque l'agent de synthèse et d'élagage crée les tables récapitulatives.

1. Ouverture d'Agent Data Model dans Framework Manager :
   a) Ouvrez Framework Manager.
   b) Dans la page **Bienvenue**, cliquez sur **Ouvrir un projet**.

      Conseil : Si vous êtes dans Framework Manager, cliquez sur **Ouvrir** dans le menu **Fichier**.
   c) Accédez au modèle de données de l'agent.
      - Pour DB2 :

        ```
        reports/db2/Kxx/model/
        ```

      - Pour Oracle :

        ```
        reports/oracle/Kxx/model/
        ```

      - Sous Microsoft SQL Server :

        ```
        reports/mssql/Kxx/model/
        ```

   d) Sélectionnez le fichier de projet de l'agent, K*xx*`.cpf`.

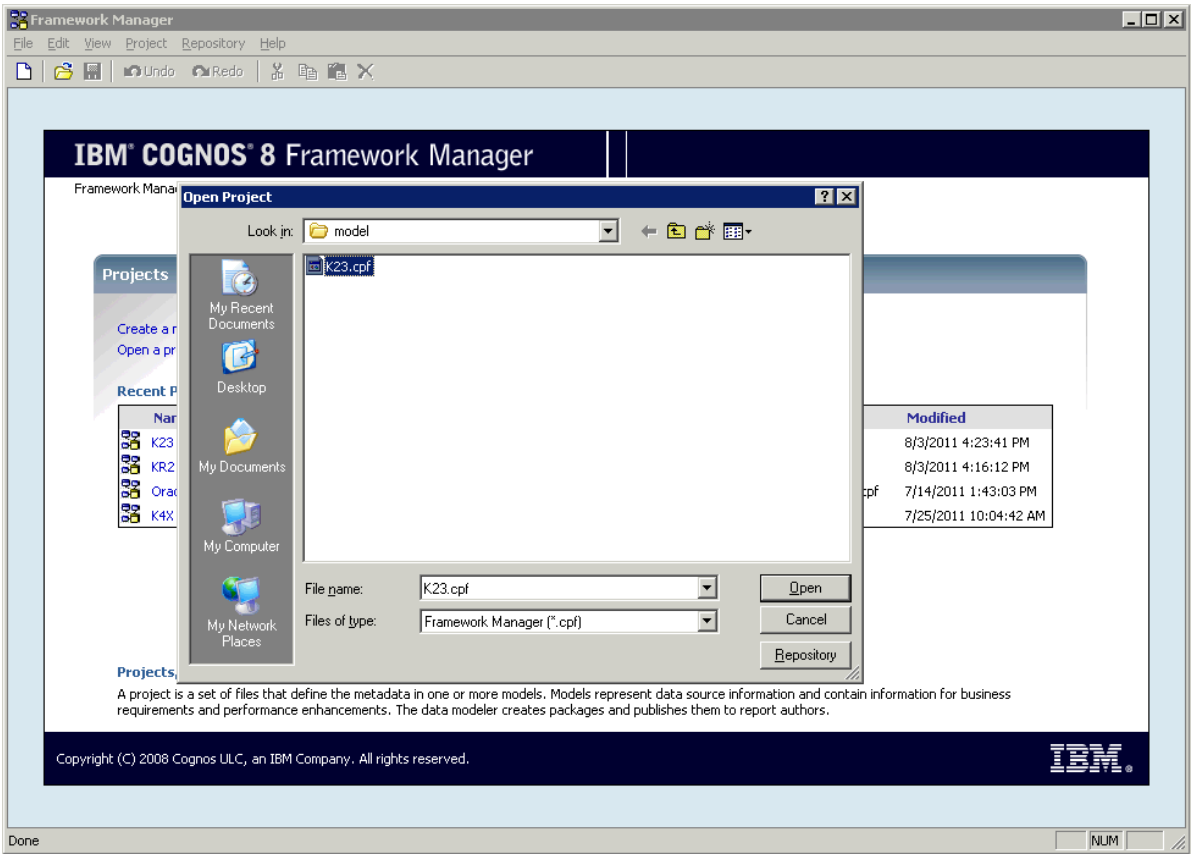


Figure 80. Sélection du fichier projet de l'agent

Remarque : Lorsqu'un projet d'agent est ouvert dans Framework Manager, le nom de l'agent est répertorié dans la liste des projets récents.

2. Remplissez la table ManagedSystem. Pour plus d'informations, voir «Remplissage de la table ManagedSystem», à la page 1529.
3. Utilisez Framework Manager pour publier le modèle de l'agent dans Tivoli Common Reporting.
   a) Ouvrez Framework Manager.
   b) Ouvrez le projet d'agent.
   c) Développez **Packages** dans l'arborescence.
   d) Cliquez avec le bouton droit sur le package d'agent et sélectionnez **Publier les packages**.

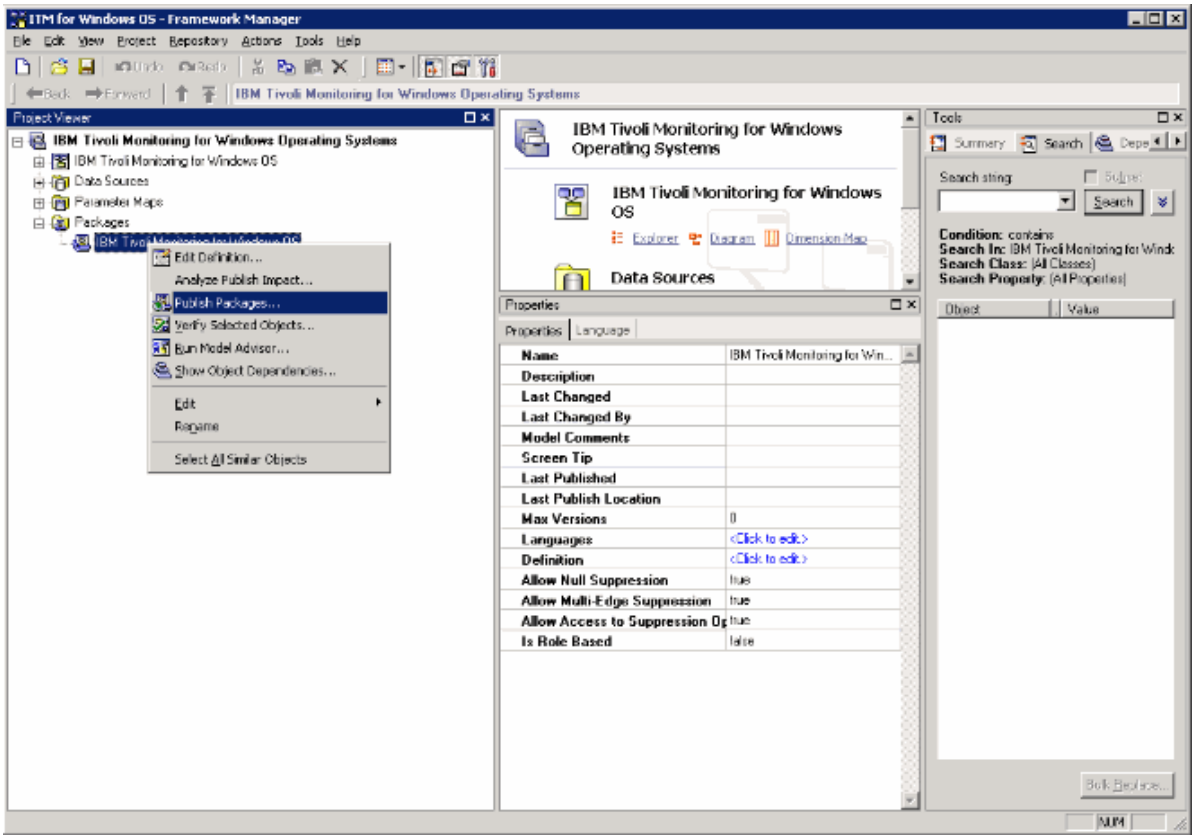


Figure 81. Sélection des packages de publication

4. Utilisez Report Studio pour créer des rapports ou des modèles.
   a) Connectez-vous à Tivoli Common Reporting.
   b) Accédez aux dossiers publics, développez **Génération de rapports** dans le panneau de navigation, puis sélectionnez **Common Reporting**.

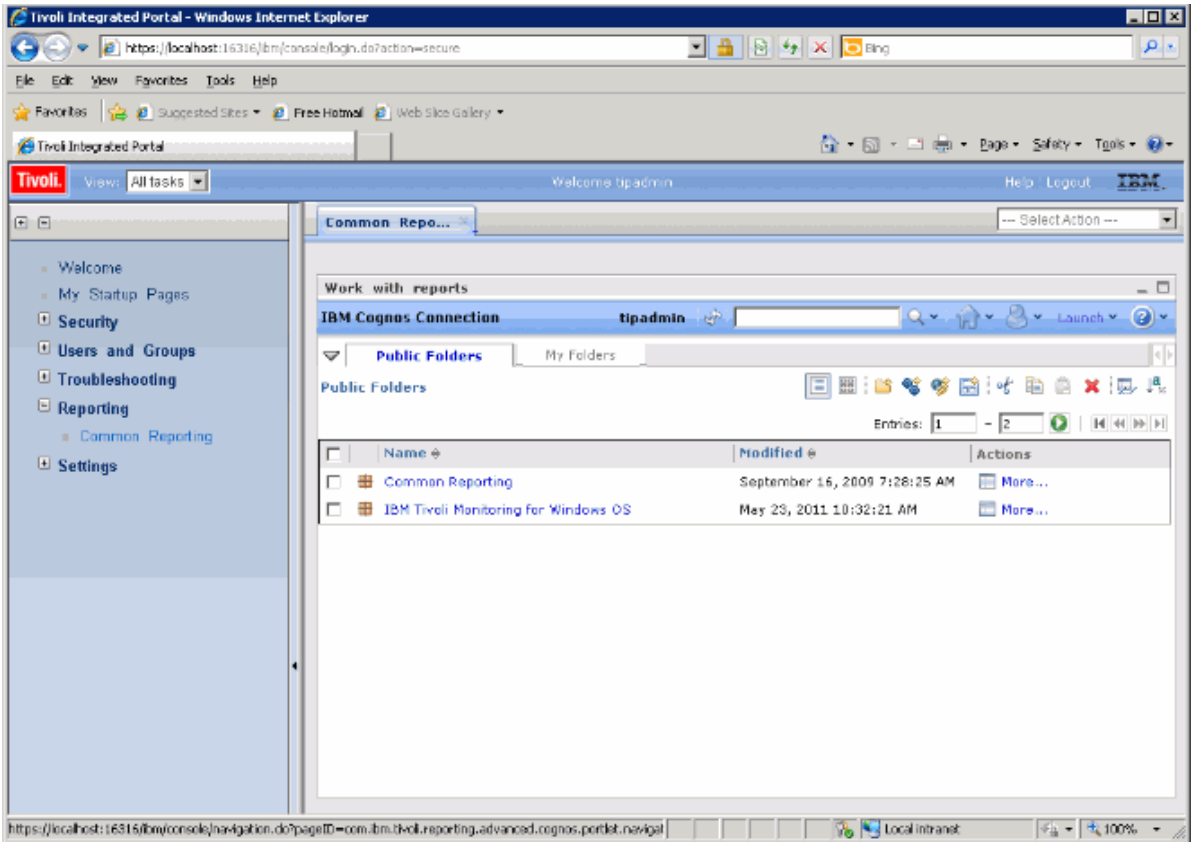


Figure 82. Sélection de Common Reporting

c) Sélectionnez votre agent Tivoli Monitoring dans la liste fournie.

d) Ouvrez l'outil de création de rapport en cliquant sur le menu Lancer et en sélectionnant **Report Studio** ou **Query Studio**.

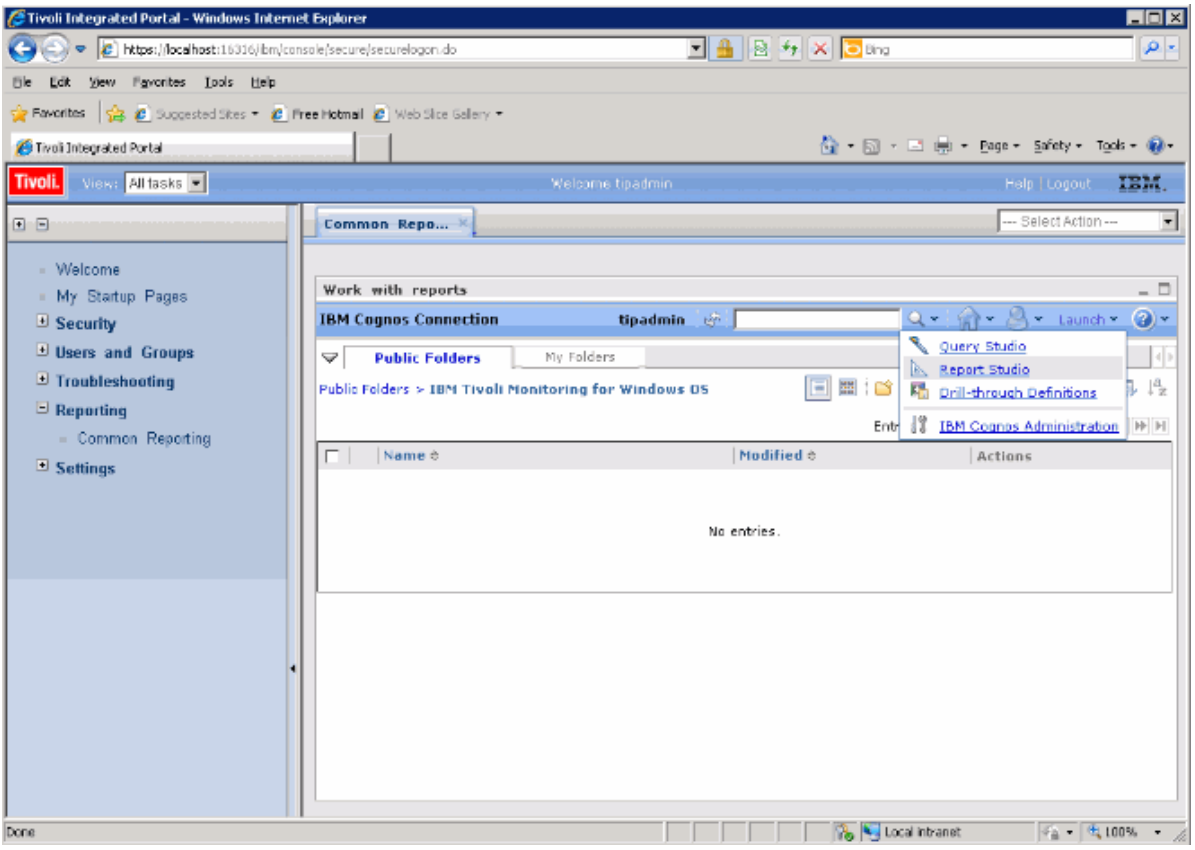


Figure 83. Sélection de Report Studio

Que faire ensuite

Vous pouvez utiliser Report Studio pour créer de nouveaux rapports ou modèles, ou modifier un rapport ou un modèle existant.

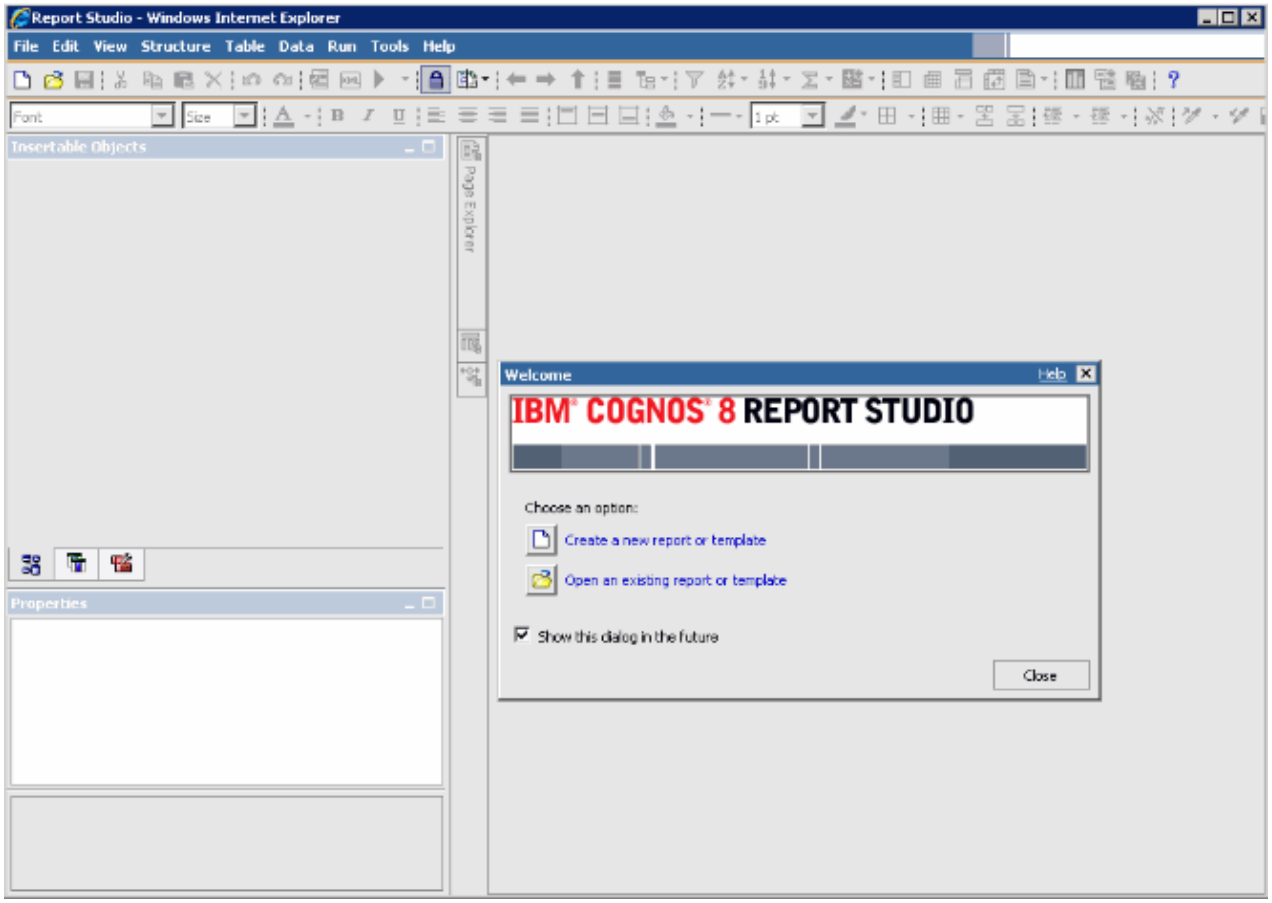


Figure 84. Report Studio

Pour plus d'informations, voir l'ensemble de rubriques relatives à Tivoli Common Reporting dans IBM Knowledge Center.

Remplissage de la table ManagedSystem

La table `ManagedSystem` doit être remplie via la procédure stockée `kqz_populate_msn`.

Pour plus d'informations, voir «Exécution de la procédure stockée DB2», à la page 1531. Cette procédure doit être exécutée périodiquement pour que la table `ManagedSystem` contienne la liste actualisée des noms de systèmes gérés.

La procédure stockée lit les tables d'historique suivantes dans Tivoli Data Warehouse si elles existent :

- La table Statut de l'objet de performances de l'agent
- La table de disponibilité de l'agent. Les agents qui surveillent les processus ou les services comportent une table de disponibilité.
- Les tables de reconnaissance de l'agent. Les agents de sous-noeud créent des tables de reconnaissance.

La collecte d'historique doit être démarrée sur un jeu particulier de groupes d'attributs. Un jeu de scripts est généré qui crée et démarre la collecte d'historique pour ces groupes d'attributs. Si vous ne souhaitez pas utiliser les scripts, la liste des groupes d'attributs apparaît dans le bloc d'en-tête de commentaires du script concerné.

Des exemples de scripts sont créés pour indiquer les tables pour lesquelles la collecte d'historique doit être activée :

- `reports/configuretdw.sh`
- `reports/configuretdw.bat`

La table suivante décrit les arguments requis :

Remarque : Vous devez indiquer - n ou - m, mais pas les deux.

Tableau 301. Arguments requis	
Argument	**Description**
-h *accueil_candle*	Chemin d'installation de Tivoli Monitoring.
-u *utilisateur_teps*	Utilisateur Tivoli Enterprise Portal Server pour se connecter comme lors de la création de collectes d'historique.
-n *nom_tems*	Serveur Tivoli Enterprise Monitoring Server sur lequel les collectes doivent être démarrées. Plusieurs serveurs Tivoli Enterprise Monitoring Server peuvent être indiqués à l'aide d'une liste séparée d'un espace. Si vous indiquez plusieurs serveurs Tivoli Enterprise Monitoring Server, mettez la liste entre guillemets. Par exemple, -n "tems1 tems2"
-m *groupe_systèmes_gérés_ou_système_géré*	Nom du groupe de systèmes gérés ou du système géré sur lequel la collecte doit être démarrée. Plusieurs systèmes gérés ou groupes de systèmes gérés peuvent être spécifiés sur une liste dans laquelle les éléments sont séparés par des espaces. Si vous en indiquez plusieurs, placez la liste entre guillemets. Par exemple, -m "msg1 msg2"

La table suivante décrit les arguments facultatifs :

Tableau 302. Arguments facultatifs	
Argument	**Description**
-s *hôte_teps*	Nom d'hôte ou adresse IP du serveur Tivoli Enterprise Portal Server. S'il n'est pas spécifié, la valeur par défaut est localhost.
-p *mot_de_passe_teps*	Mot de passe de l'utilisateur Tivoli Enterprise Portal Server spécifié avec l'option -u. Si ce mot de passe n'est pas indiqué, le script le demande
-c *intervalle_collecte_historique*	Intervalle de collecte d'historique à utiliser lors du démarrage des collectes d'historique. Si cette option est omise, la valeur par défaut est 1h (1 heure). Les valeurs valides sont : 15m, 30m, 1h, 12h ou 1d, où m correspond aux minutes, h aux heures et d aux jours.
-r *intervalle_élagage*	Fréquence d'élagage à utiliser pour les données d'historique. Les données historiques doivent être supprimées pour que les tables cessent de s'agrandir. Si cet élément n'est pas indiqué, la valeur par défaut est 2d (2 jours). Utilisez d pour les jours, m pour les mois et y pour les années.

Une fois la collecte d'historique démarrée, la procédure stockée kqz_populate_msn doit être exécutée régulièrement. La procédure stockée est exécutée périodiquement afin que la table ManagedSystem contienne la liste actualisée des systèmes gérés dans l'environnement Tivoli Monitoring.

Exécution de la procédure stockée DB2
Exécutez une procédure stockée sur DB2.

Pourquoi et quand exécuter cette tâche

Pour exécuter la procédure stockée sur DB2, procédez comme suit :

Procédure

1. Connectez la base de données Tivoli Data Warehouse en tant qu'utilisateur de l'entrepôt :

```
connect to <alias_base_de_données_Tivoli_Data_Warehouse> user
<id_utilisateur_Tivoli_Data_Warehouse> using <mot_de_passe>
```

2. Exécutez la procédure stockée :

```
db2 "call <schéma_Tivoli_Data_Warehouse>.kqz_populate_msn
('<code produit à trois lettres pour l'agent>')"
```

Exécution de la procédure stockée Oracle
Exécutez une procédure stockée sur Oracle.

Pourquoi et quand exécuter cette tâche

Pour exécuter la procédure stockée sur Oracle, procédez comme suit :

Procédure

1. Démarrez `sqlplus` :

```
sqlplus <id_utilisateur_Tivoli_Data_Warehouse>/<mot_de_passe>@
<ID de sécurité Oracle>
```

2. Exécutez la procédure stockée :

```
execute kqz_populate_msn('<code produit à trois lettres pour l'agent>');
```

Exécution de la procédure stockée sur SQL Server 2005 et 2008
Exécutez une procédure stockée sur SQL Server.

Pourquoi et quand exécuter cette tâche

Pour exécuter la procédure stockée sur SQL Server 2005 et 2008, procédez comme suit :

Procédure

Exécutez la procédure stockée :

```
osql -S <server> -U <id_Tivoli_Data_Warehouse> -P
<mot_de_passe_Tivoli_Data_Warehouse> -d
<nom_base_de_données_Tivoli_Data_Warehouse> -Q "EXEC
[<schéma_Tivoli_Data_Warehouse>].[kqz_populate_msn]
@pv_productcode = N'<code produit à trois lettres>'"
```

Exportation de rapports et de modèles de données depuis Tivoli Common Reporting
Exportez des rapports et des modèles de données à partir de Tivoli Common Reporting.

Procédure

1. Connectez-vous à Tivoli Common Reporting.
2. Accédez aux dossiers publics puis, sous **Génération de rapports** dans le panneau de navigation, sélectionnez **Common Reporting**.

3. Dans la section Travail avec les rapports, cliquez sur le menu **Launch** et sélectionnez **IBM Cognos Administration**.
4. Cliquez sur l'onglet **Configuration**.
5. Cliquez sur **Administration de contenu**.

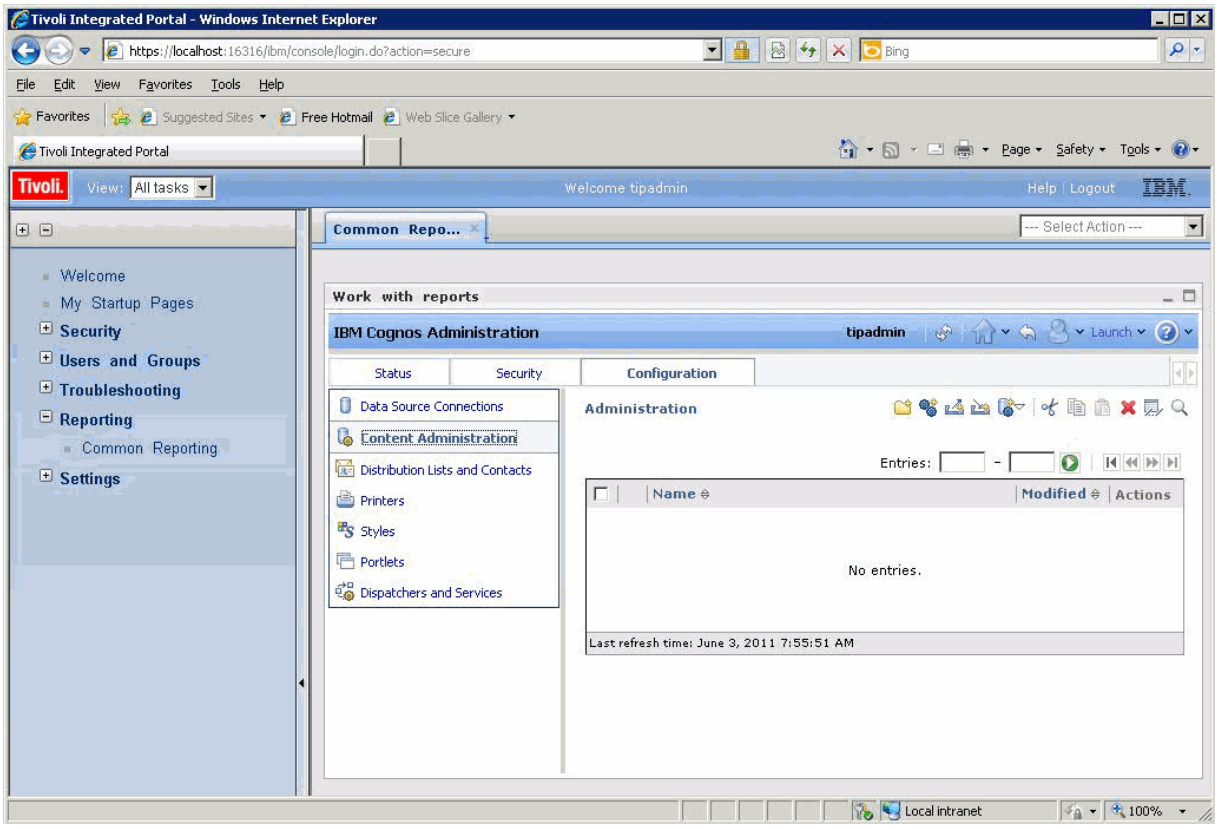


Figure 85. Onglet Administration de contenu

6. Cliquez sur l'icône **Nouvelle exportation** pour exporter un nouveau package.
7. Nommez le package. Vous pouvez éventuellement ajouter une infobulle et une description.
8. Sélectionnez **Sélectionnez les dossiers publics et le contenu d'annuaire**.
9. Dans la boîte de dialogue Dossiers publics, cliquez sur le lien **Ajouter**.
10. Déplacez votre package d'agent vers **Entrées sélectionnées**.
11. Sur la dernière page de l'assistant, sélectionnez **Sauvegarder uniquement**. Une fois l'assistant terminé, le package de rapports est indiqué sous l'onglet Administration de contenu.
12. Sous l'onglet Administration de contenu, cliquez sur Exécuter (flèche verte) pour créer le fichier compressé `.zip`.

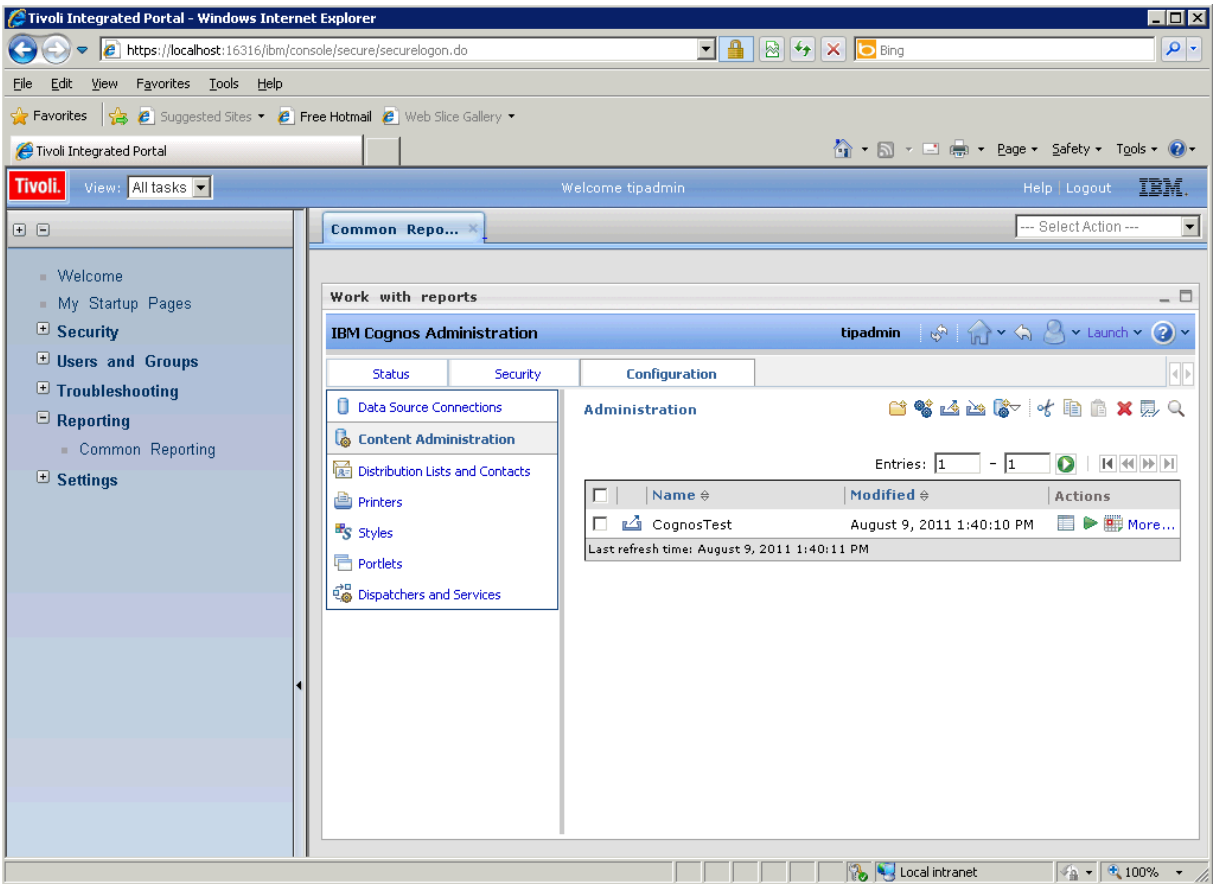


Figure 86. Onglet Administration de contenu avec le package d'agent indiqué

Résultats

Le fichier `.zip` créé par l'exportation est placé dans le répertoire de déploiement.

- Le chemin du répertoire pour Tivoli Common Reporting version 1.3 est :

```
C:\IBM\tivoli\tip\products\tcr\Cognos\c8\deployment
```

- Le chemin du répertoire pour Tivoli Common Reporting version 2.1 ou version supérieure est :

```
C:\IBM\tivoli\tipv2Components\TCRComponent\cognos\deployment
```

Que faire ensuite

Pour plus d'informations sur l'exportation de rapports, voir Exportation des packages de rapports Cognos dans le manuel *Tivoli Common Reporting - Guide d'utilisation*.

Importation de rapports dans Agent Builder

Lorsque le package de rapports est exporté depuis Tivoli Common Reporting, il peut être importé dans le projet Agent Builder. Le package de rapports peut être ensuite inclus dans l'image d'installation de l'agent.

Procédure

1. Cliquez avec le bouton droit sur le projet d'agent dans Agent Builder.
2. Sélectionnez **IBM** > **Importation de packages de rapports**.
3. Dans la fenêtre **Importation de packages de rapports**, sélectionnez le **type de base de données** sur lequel le package de rapports a été créé.
4. Entrez le chemin complet du package de rapports, ou cliquez sur **Parcourir** pour le sélectionner.

5. Cliquez sur **OK**.
6. Le package de rapports apparaît désormais dans le projet d'agent sous le répertoire `reports/dbtype`.

   Remarque : Si vous créez des packages de rapports propres à une base de données, vous devez importer chaque package dans Agent Builder.

Installation de rapports depuis un package d'agent dans Tivoli Common Reporting
Importez un package de rapports depuis votre agent dans Tivoli Common Reporting

Procédure

1. Suivez les étapes de l'assistant pour importer un nouveau package à partir de votre image d'agent.

   Dans l'image d'agent, les rapports se trouvent dans `reports/dbType/Kxx/reports/cognos_reports/itmkxx/packages`
2. Copiez le fichier `zip` des rapports compressé dans le répertoire de déploiement Tivoli Common Reporting.
   - Le chemin du répertoire pour Tivoli Common Reporting version 1.3 est : `C:\IBM\tivoli\tip\products\tcr\Cognos\c8\deployment`
   - Le chemin du répertoire pour Tivoli Common Reporting version 2.1 ou supérieure est : `C:\IBM\tivoli\tipv2Components\TCRComponent\cognos\deployment`
3. Connectez-vous à Tivoli Common Reporting.
4. Accédez aux dossiers publics puis, sous **Génération de rapports** dans le panneau de navigation, sélectionnez **Common Reporting**.
5. Dans la section Travail avec les rapports, cliquez sur le menu **Lancement** et sélectionnez **IBM Cognos Administration**.
6. Allez dans l'onglet **Configuration** et ouvrez la section **Content Administration**.
7. Cliquez sur **Nouvelle importation** pour créer une importation de package.
8. Sélectionnez le package de rapports de l'agent.
9. Sélectionnez les dossiers publics que vous souhaitez importer.
10. Sélectionnez sauvegarder.
11. Cliquez sur Exécuter (flèche verte) pour effectuer l'importation.

Résultats

Pour plus d'informations, voir Connexion à l'interface de génération de rapports dans le manuel *Tivoli Common Reporting - Guide d'utilisation*.

Expressions régulières ICU

Description des caractéristiques de l'implémentation d'expressions régulières ICU.

Le contenu de référence est extraite du *guide d'utilisation d'ICU*. Il décrit les caractéristiques de l'implémentation d'expressions régulières ICU. Ces informations sont essentielles si vous utilisez la fonction d'expression régulière d'Agent Builder car des langages de programmation différents implémentent des expressions régulières selon des méthodes légèrement différentes.

Tableau 303. Métacaractères génériques

Caractère	Description
\a	Correspond à un caractère d'alerte (BELL) \u0007
\A	Correspond au début de la saisie. Diffère de ^ en ce que \A ne permet pas de correspondance après une nouvelle ligne à l'intérieur de l'entrée.

Tableau 303. Métacaractères génériques (suite)

Caractère	Description
\b, à l'extérieur d'un [ensemble]	Correspond si la position en cours est une limite de mot. Les limites ont lieu lors des transitions entre les caractères représentant un mot (\w) et les caractères ne représentant pas un mot (\W), les marques de combinaison étant ignorées. Pour plus d'informations sur les limites de mot, voir ICU Boundary Analysis.
\b, à l'intérieur d'un [ensemble]	Correspondance avec un caractère RETOUR ARRIERE, \u0008.
\B	Correspond si la position en cours n'est pas une limite de mot.
\cX	Correspond à un caractère Ctrl-X.
\d	Correspond à tout caractère dont la catégorie générale Unicode est Nd (nombre, chiffre décimal).
\D	Correspond à tout caractère qui n'est pas un chiffre décimal.
\e	Correspond à un caractère ÉCHAPPEMENT \u001B.
\E	Marque la fin d'une séquence de citation \Q ... \E.
\f	Correspondance avec un caractère ALIMENTATION PAPIER, \u000C.
\G	Correspond si la position en cours est à la fin de l'occurrence précédente.
\n	Correspondance avec un caractère SAUT DE LIGNE, \u000A.
\N{NOM DE CARACTERE UNICODE}	Correspond au caractère nommé.
\p{NOM DE PROPRIETE UNICODE}	Correspond à tout caractère comportant la propriété Unicode indiquée.
\P{NOM DE PROPRIETE UNICODE}	Correspond à tout caractère ne comportant pas la propriété Unicode indiquée.
\Q	Placez entre apostrophes tous les caractères suivants jusqu'à \E.
\r	Correspondance avec un caractère RETOUR CHARIOT, \u000D.
\s	Correspond à un espace blanc. L'espace blanc est défini comme [\t\n\f\r\p{Z}].
\S	Correspond à tout caractère d'espace non blanc.
\t	Correspondance avec un caractère TABULATION HORIZONTALE, \u0009.
\uhhhh	Correspondance avec le caractère dont la valeur hexadécimale est hhhh.

Tableau 303. Métacaractères génériques (suite)	
Caractère	**Description**
\Uhhhhhhhh	Correspondance avec le caractère dont la valeur hexadécimale est hhhhhhhh. Exactement huit chiffres hexadécimaux doivent être fournis, même si le point de code Unicode le plus élevé est \U0010ffff.
\w	Correspond à tout caractère représentant un mot. Les caractères de mot sont [\p{Ll}\p{Lu} \p{Lt}\p{Lo}\p{Nd}].
\W	Correspond à tout caractère ne représentant pas un mot.
\x{hhhh}	Correspondance avec le caractère dont la valeur hexadécimale est hhhh. Entre un et 6 chiffres hexadécimaux peuvent être fournis.
\xhh	Correspondance avec le caractère dont la valeur hexadécimale à deux chiffres est hh.
\X	Correspond à un grappe de graphèmes.
\Z\	Correspond si la position en cours est à la fin de la précédente occurrence, mais avant le dernier caractère de fin de ligne, s'il y a lieu.
\z	Correspond si la position en cours est à la fin de la saisie.
\n	Référence arrière. Correspondance avec tout ce qui correspondait au n-ième groupe de capture. n doit être un nombre > 1 et < nombre total de groupes de capture dans le modèle. **Remarque :** Les échappements octaux, tels que \012, ne sont pas pris en charge dans les caractères génériques ICU.
[modèle]	Correspond à n'importe quel caractère de l'ensemble. Voir UnicodeSet pour obtenir une description complète des éléments susceptibles d'apparaître dans le modèle.
.	Correspond à n'importe quel caractère.
^	Correspond au début d'une ligne.
$	Correspond à la fin d'une ligne.
\	Place le caractère suivant entre des guillemets. Les caractères devant être placés entre des guillemets à traiter sous forme de littéraux sont * ? + [( ) { } ^ $ | \ . /

Tableau 304. Opérateurs génériques	
Opérateur	**Description**
|	Alternative. A | B correspond à A ou B.

Tableau 304. Opérateurs génériques (suite)

Opérateur	Description
*	Correspond à 0 ou plusieurs fois. Correspond à autant de fois que possible.
+	Correspond à 1 ou plusieurs fois. Correspond à autant de fois que possible.
?	Correspond à zéro ou une fois. De préférence une fois.
{n}	Correspond exactement à n fois
{n,}	Correspond à au moins n fois. Correspond à autant de fois que possible.
{n,m}	Correspond à au moins n et au plus m fois. Correspond à autant de fois que possible, mais au maximum à m fois.
*?	Correspond à 0 ou plusieurs fois. Correspond à un minimum de fois que possible.
+?	Correspond à 1 ou plusieurs fois. Correspond à un minimum de fois que possible.
??	Correspond à zéro ou une fois. De préférence zéro fois.
{n}?	Correspond exactement à n fois
{n,}?	Correspond à au moins n fois mais au plus au nombre de fois requis pour une concordance globale.
{n,m}?	Correspond à au moins n et au plus m fois. Correspond à un minimum de fois que possible, mais au minimum à n fois.
*+	Correspond à 0 ou plusieurs fois. Correspond à autant de fois que possible lorsqu'il est détecté pour la première fois ; ne faites pas de nouvelle tentative avec un nombre inférieur, même si la correspondance globale échoue (correspondance possessive)
++	Correspond à 1 ou plusieurs fois. Correspondance possessive.
?+	Correspond à zéro ou une fois. Correspondance possessive.
{n}+	Correspond exactement à n fois
{n,}+	Correspond à au moins n fois. Correspondance possessive.
{n,m}+	Correspond à au moins n et au plus m fois. Correspondance possessive.

Tableau 304. Opérateurs génériques (suite)	
Opérateur	**Description**
`( ... )`	Parenthèses capturantes. La plage des entrées correspondant à la sous-expression placée entre parenthèses est disponible après la correspondance.
`(?: ... )`	Parenthèses non capturantes. Regroupent le modèle inclus, mais ne fournissent pas la capture du texte correspondant. Plus efficaces que les parenthèses capturantes.
`(?> ... )`	Parenthèses à correspondance atomique. La première correspondance de la sous-expression placée entre parenthèses est la seule tentée. Si elle ne conduit pas à une correspondance de modèle global, retournez la recherche de correspondance à une position précédant le `"(?>"`.
`(?# ... )`	Commentaire au format libre `(?# commentaire )`.
`(?= ... )`	Assertion avant. Vrai si le modèle entre parenthèses correspond à la position de saisie en cours mais ne dépasse pas la position de saisie.
`(?! ... )`	Assertion avant négative. Vrai si le modèle entre parenthèses ne correspond pas à la position de saisie en cours. Ne dépasse pas la position de saisie.
`(?<= ... )`	Assertion arrière. Vrai si le modèle entre parenthèses correspond au texte qui précède la position de saisie en cours. Le dernier caractère de la correspondance étant le caractère de saisie précédant directement la position en cours. Ne modifie pas la position de saisie. La longueur des éventuelles chaînes possible appariée par le modèle d'assertion arrière ne doit pas être illimitée (pas d'opérateurs * ou +).
`(?<!...)`	Assertion arrière négative. Vrai si le modèle entre parenthèses ne correspond pas au texte qui précède la position de saisie en cours. Le dernier caractère de la correspondance étant le caractère de saisie précédant directement la position en cours. Ne modifie pas la position de saisie. La longueur des éventuelles chaînes possible appariée par le modèle d'assertion arrière ne doit pas être illimitée (pas d'opérateurs * ou +).
`(?ismx-ismx: ... )`	Paramètres des indicateurs. Evalue l'expression entre parenthèses à l'aide des indicateurs indiqués activés ou désactivés.

Tableau 304. Opérateurs génériques (suite)	
Opérateur	**Description**
`(?ismx-ismx)`	Paramètres des indicateurs. Modifie les paramètres des indicateurs. Les modifications s'appliquent à la partie du modèle qui suit le paramètre. Par exemple, `(?i)` est remplacé par une occurrence non sensible à la casse.

Texte de remplacement

Le texte de remplacement pour les opérations de recherche et de remplacement peut contenir des références au texte de groupe de capture à partir de la recherche. Les références sont au format $n, où n représente le numéro du groupe de capture.

Tableau 305. Caractères de texte de remplacement	
Caractère	**Description**
$n	Le texte du groupe de captures n positionnel est remplacé par `$n`. n doit être `>= 0`, et ne pas être supérieur au nombre de groupes de captures. Un $ non suivi d'un chiffre n'a pas de signification particulière ; il s'affiche tel quel ($.) dans le texte de substitution.
\	Traitez ce caractère comme un littéral, éliminant toute signification particulière. L'échappement à l'aide d'une barre oblique inversée dans le texte de substitution n'est requis que pour `'$'` et `'\'`, mais peut être utilisé sur tout autre caractère sans effets secondaires.
$@n	Le texte du groupe de capture n est substitué à l'expression régulière correspondant au groupe de capture n. n doit être `>= 0`, et ne doit pas être supérieur au nombre de groupes de capture. Un `$@` non suivi d'un chiffre n'a pas de signification particulière ; il s'affiche tel quel ($@) dans le texte de substitution.
$♯n	Le texte du groupe de captures n correspondant est remplacé par $♯n. n doit être `>= 0` et ne doit pas être supérieur au nombre de groupes de captures correspondants. Un $♯ non suivi d'un chiffre n'a pas de signification particulière ; il s'affiche tel quel ($♯) dans le texte de substitution.

Options d'indicateur

Les indicateurs ci-dessous contrôlent les divers aspects de la correspondance d'expression régulière. Les valeurs d'indicateur peuvent être indiquées lors de la compilation d'une expression dans un objet RegexPattern. Sinon, elles peuvent être spécifiées dans le modèle proprement dit à l'aide des options de modèle `(?ismx-ismx)`.

Tableau 306. Options d'indicateur		
Indicateur (modèle)	**Indicateur (constante d'API)**	**Description**
`i`	`UREGEX_CASE_INSENSITIVE`	Si cet indicateur est défini, la correspondance a lieu d'une manière non sensible à la casse.
`x`	`UREGEX_COMMENTS`	Si cet indicateur est défini, l'utilisation d'espace blanc et de `#comments` est autorisée au sein des modèles.
`s`	`UREGEX_DOTALL`	Si cet indicateur est défini, un `"."` dans un modèle correspond à un caractère de fin de ligne dans le texte de saisie. Par défaut, il ne correspond pas. Il est à noter qu'une paire de caractères retour chariot/saut de ligne dans le texte agit comme un caractère de fin de ligne unique et correspond à un `"."` unique dans un modèle d'expression régulière.
`m`	`UREGEX_MULTILINE`	Contrôle le comportement de `"^"` et `"$"` dans un modèle. Par défaut, ceux-ci correspondent uniquement au début et à la fin, respectivement, du texte de saisie. Si cet indicateur est défini, `"^"` et `"$"` permettent aussi une correspondance au début et à la fin de chaque ligne à l'intérieur du texte d'entrée.

Création d'ensembles de fichiers sans agent

Vous pouvez créer des ensembles de fichiers placés dans le dépôt Tivoli Monitoring. Ces regroupements peuvent ensuite être déployés sur des systèmes cible de votre environnement.

Pourquoi et quand exécuter cette tâche

Cette fonction vous permet de configurer à distance des produits pour lesquels il n'existe pas d'option de configuration à distance. Pour utiliser cette fonction, vous devez placer les fichiers de configuration pré-remplis dans le dépôt et les envoyer ensuite aux systèmes concernés.

Procédure

1. Dans Agent Builder, sélectionnez **Fichier** > **Nouveau** > **Autre**.
2. Sous **Agent Builder**, sélectionnez **Regroupement de déploiement à distance sans agent**.
3. Cliquez sur **Suivant**.
4. Dans la zone **Nom de projet**, entrez un nom pour votre projet.
5. Cliquez sur **Suivant**.
6. Complétez les informations de la fenêtre **Informations de regroupement de déploiement à distance** :

a) Dans la zone **Identificateur du regroupement**, entrez un identificateur sous forme de chaîne alphanumérique unique de 3 à 31 caractères. Cette chaîne peut contenir un trait d'union, sauf en première position. Elle doit débuter par une lettre, à l'exclusion de la lettre K.

b) Dans la zone **Description du regroupement**, entrez une description du regroupement.

c) Dans la zone **Version**, entrez la version du regroupement au format VVRRMMFFF. Où `vv`= numéro de la version ; `rr`= numéro de l'édition ; `mm`= numéro de modification (numéro du groupe de correctifs) et `fff` = numéro du correctif temporaire.

7. Dans la zone **Systèmes d'exploitation**, sélectionnez les systèmes d'exploitation sur lesquels le regroupement peut être déployé.
8. Cliquez sur **Terminer** pour créer un projet dans l'espace de travail et ouvrir l'**éditeur de regroupement de déploiement à distance**.

Editeur de regroupement de déploiement à distance

L'éditeur de regroupement de déploiement à distance est utilisé pour générer des commandes aidant au déploiement de votre regroupement de fichiers.

L'éditeur de regroupement de déploiement à distance fournit des informations sur le regroupement de fichiers associés à un projet.

La section **Informations d'identification du regroupement** contient les informations suivantes :

Identificateur du regroupement
ID unique du regroupement

Description du regroupement
Description du regroupement

Version du regroupement
Version du regroupement

Compilation
Identificateur de compilation du regroupement. Entrez un numéro de compilation dans cette zone. Si aucun numéro de compilation n'est indiqué, une valeur numérique est générée à partir de la date et de l'heure auxquelles le regroupement a été créé.

Option Créer des commandes de copie pour les fichiers du regroupement
Cochez cette case pour générer un ensemble de commandes de copie par défaut qui s'exécuteront lors du déploiement du regroupement. Les fichiers seront copiés à l'emplacement spécifié dans la zone de texte **Emplacement de copie**. L'emplacement par défaut est *INSTALLDIR*. Indiquez cette variable de déploiement à distance à partir du déploiement par ligne de commande en définissant KDY.*INSTALLDIR*=...

La section **Systèmes d'exploitation** affiche les systèmes d'exploitation sur lesquels le regroupement peut être déployé.

La section **Commandes** affiche les commandes à exécuter lors du déploiement du regroupement.

La section **Regroupements prérequis** affiche les regroupements qui doivent être présents pour que ce regroupement puisse fonctionner.

Utilisez l'éditeur de regroupement de déploiement à distance pour choisir un ensemble de commandes de copie par défaut chargées de copier le contenu de votre regroupement à un emplacement déterminé. Si cette option est sélectionnée, une commande de copie est alors générée pour chaque fichier de votre projet. L'emplacement de copie par défaut est *INSTALLDIR*. Il s'agit d'une variable spécifique de déploiement à distance qui, si elle n'est pas définie sur la ligne de commande de déploiement, prend la valeur par défaut de *CANDLEHOME*. Pour modifier l'emplacement déterminé par *INSTALLDIR*, spécifiez la propriété **KDY.INSTALLDIR** lors de l'exécution de la commande **addSystem**.

La structure de répertoire spécifiée dans votre projet de regroupement est répliquée dans *INSTALLDIR*. Par exemple, s'il y a un dossier nommé `config` avec un fichier `myprod.config` dans votre projet, la commande de copie générée copiera le fichier dans *INSTALLDIR*`/config/myprod.config` lorsque le regroupement sera déployé.

Ajout de commandes au regroupement

Vous pouvez spécifier des commandes supplémentaires à exécuter lors du déploiement.

Pourquoi et quand exécuter cette tâche

Vous pouvez spécifier des commandes supplémentaires à exécuter lors du déploiement à l'aide de l'**Editeur de regroupement de déploiement à distance**.

Procédure

1. Pour spécifier des commandes supplémentaires à exécuter lors du déploiement, cliquez sur **Ajouter** dans la section **Commandes** de l'**éditeur de regroupement de déploiement à distance**.
2. Dans la fenêtre **Commande**, sélectionnez le type de commande **Préinstallation**, **Installation**, **Post-installation** ou **Désinstallation** puis entrez la commande à exécuter.

   Vous devez indiquer le chemin qualifié complet de la commande à exécuter. Pour des raisons de praticité, la fonction de déploiement à distance fournit un ensemble de variables prédéfinies. Pour utiliser ces variables dans une commande, faites figurer la variable entre des barres verticales, par exemple `|DEPLOYDIR|`. Pour plus d'informations sur les variables prédéfinies utilisables dans les commandes, voir (Tableau 307, à la page 1542).

   Tableau 307. Variables prédéfinies pour les commandes

Variable	Description
DEPLOYDIR	Répertoire temporaire du noeud final dans lequel le regroupement est stocké au cours du déploiement. Par exemple, pour exécuter le script `myscript.sh` inclus dans votre regroupement, entrez la commande suivante : `|DEPLOYDIR|/myscript.sh`
INSTALLDIR	Correspond soit à *CANDLEHOME*, soit à la valeur de *KDY.INSTALLDIR*, si elle est spécifiée dans la commande **addSystem**.
CANDLEHOME	Répertoire d'installation de Tivoli Monitoring.

3. Pour finir, sélectionnez les **Systèmes d'exploitation** sur lesquels la commande doit être exécutée.

Ajout de prérequis à un regroupement

L'**Editeur de regroupement de déploiement à distance** vous permet de spécifier une configuration minimale pour le regroupement.

Procédure

1. Pour ajouter un prérequis, cliquez sur **Ajouter** dans la section **Regroupements prérequis** de l'**éditeur de regroupement de déploiement à distance**, sur la page **Informations de regroupement**.
2. Dans la fenêtre **Nouveau prérequis**, entrez l'identificateur de regroupement dont dépend ce regroupement, ainsi que la version minimale requise.
3. Sélectionnez les systèmes d'exploitation pour lesquels ce prérequis est obligatoire.
4. Cliquez sur **OK** pour terminer et quitter.

Ajout de fichiers à un regroupement

Ajoutez des fichiers à un regroupement de fichiers à l'aide de l'**Editeur de regroupement de déploiement à distance**.

Procédure

1. Pour ajouter des fichiers à un regroupement destiné au déploiement à distance, suivez l'une des procédures ci-après :
   - Dans l'éditeur de regroupement de déploiement à distance, cliquez sur **Ajouter des fichiers au regroupement**.
   - Cliquez avec le bouton droit de la souris sur le projet dans l'arborescence du navigateur, puis cliquez sur **Déploiement à distance IBM Tivoli Monitoring** > **Ajouter des fichiers au regroupement**

   Ces deux actions entraînent l'affichage de la fenêtre **Importer les fichiers de regroupement** :
2. Indiquez des fichiers ou répertoires individuels qui contiennent des fichiers dans la zone **Informations sur les fichiers**.
3. Cliquez sur **Terminer**.

   Les fichiers ou les répertoires spécifiés sont copiés dans le répertoire du projet. La structure de répertoire du projet est conservée lorsque vous générez le regroupement de déploiement à distance. Si vous souhaitez qu'Agent Builder génère les commandes de copie par défaut, assurez-vous que les fichiers figurent dans la structure de répertoire où ils devront être au moment du déploiement.

Génération d'un regroupement

Utilisez Agent Builder pour générer un regroupement pour le déploiement à distance d'un agent.

Procédure

1. Pour générer le regroupement de déploiement à distance, suivez l'une des procédures ci-après pour afficher la fenêtre **Générer le regroupement de déploiement à distance définitif** :
   - Dans l'**éditeur de regroupement de déploiement à distance**, cliquez sur **Générer le regroupement de déploiement à distance définitif**.
   - Cliquez avec le bouton droit de la souris sur le projet dans l'arborescence du navigateur, puis cliquez sur **Déploiement à distance IBM Tivoli Monitoring** > **Générer le regroupement de déploiement à distance.**
2. Vous pouvez désormais générer le regroupement de deux manières :
   - S'il y a un serveur Tivoli Enterprise Monitoring Server sur le système où vous exécutez Agent Builder, cliquez sur **Installer le regroupement de déploiement à distance dans un dépôt TEMS local**.

     Agent Builder tente alors de déterminer l'emplacement d'installation de Tivoli Monitoring et l'entre dans la zone **Répertoire**. Si *CANDLE_HOME* n'est pas défini, l'emplacement par défaut de `C:\IBM\ITM` ou `/opt/IBM/ITM` est utilisé. Vérifiez que l'emplacement d'installation est correct avant de poursuivre.

     Vous devez fournir les informations de connexion à Tivoli Enterprise Monitoring Server pour pouvoir installer le regroupement.
   - Pour générer le regroupement dans un répertoire du système, cliquez sur **Générer le regroupement de déploiement à distance dans répertoire local.**

     Une fois le processus terminé, vous devez transférer ce répertoire sur un système Tivoli Enterprise Monitoring Server et utiliser la commande `tacmd addbundles` pour ajouter le regroupement au dépôt.

Que faire ensuite

Lorsque vous déployez le regroupement, vous devez utiliser la commande `tacmd addSystem`. Par exemple :

```
tacmd addsystem -t MONITORINGCOLLECTION -n Primary:ITMAGT:NT
```

, où `-t` (type) est le code produit retourné par la commande `tacmd viewDepot` :

```
>tacmd viewDepot
Product Code : MONITORINGCOLLECTION
Version : 010000003
Description : MonitoringCollectionScripts
Host Type : WINNT
Host Version : WINNT
Prerequisites:
```

Remarque : Il n'est pas possible d'effectuer un déploiement à distance à partir du bureau ou du navigateur Tivoli Enterprise Portal. Si vous effectuez malgré tout un déploiement à distance depuis le bureau ou le navigateur Tivoli Enterprise Portal, le message KFWITM219E s'affiche.

Pour plus d'informations, voir la documentation Tivoli Monitoring.

Création de regroupements déployables pour les sondes Tivoli Netcool/OMNIbus

Vous pouvez utiliser Agent Builder pour créer des packages et des regroupements de configuration qui peuvent être utilisés pour déployer des sondes Tivoli Netcool/OMNIbus sur des ordinateurs distants.

Pourquoi et quand exécuter cette tâche

Pour assurer le déploiement à distance des sondes, vous pouvez également créer des regroupements de fichiers Tivoli Netcool/OMNIbus qui peuvent être déployés sur des ordinateurs distants avant que vous ne déployiez les sondes.

Procédure

1. Dans Agent Builder, sélectionnez **Fichier** > **Nouveau** > **Autre**.
2. Sous **Assistants IBM Tivoli OMNIbus**, sélectionnez **Offre groupée**.
3. Cliquez sur **Suivant**.

Que faire ensuite

Vous pouvez alors utiliser l'assistant **OMNIbus Install Bundle** pour créer les regroupements. Pour plus d'informations sur l'utilisation de cet assistant, voir la documentation de Tivoli Netcool/OMNIbus.

Prise en charge des noms de fichier dynamiques

Utiliser la prise en charge de nom de fichier dynamique pour spécifier un modèle de nom de fichier au lieu d'un nom de fichier réel.

Certains programmes d'application créent un nom de fichier de sortie qui est sujet à modification. Les modifications se font en fonction de critères particuliers tels que les jour, mois, année en cours ou bien créent un nom de fichier comportant un numéro d'ordre régulièrement incrémenté. Dans ce cas, vous pouvez indiquer un modèle de nom de fichier au lieu du nom de fichier réel Il existe deux formats reconnus pour spécifier un modèle de nom de fichier :

- Expressions régulières (préférées)
- Syntaxe de nom de fichier dynamique IBM Tivoli Universal Agent (obsolète).

Modèles de nom de fichier d'expression régulière

Pour spécifier des modèles de noms de fichiers, vous pouvez utiliser des expressions régulières conformément à la syntaxe ICU (International Components for Unicode) qui est documentée dans l'(«Expressions régulières ICU», à la page 1534). Pour utiliser cette fonction, vous devez cocher la case **Les noms de fichier correspondent à l'expression régulière** dans la page **Informations avancées sur le groupe d'attributs du fichier journal**. Lorsque vous spécifiez des modèles utilisant des expressions régulières, vous devez également sélectionner une option dans la liste déroulante **Lorsque plusieurs fichiers correspondent** dans la page **Informations avancées sur le groupe d'attributs du fichier journal** pour indiquer les instructions pour sélectionner le fichier correspondant le plus récent.

Remarque : Les expressions régulières constituent la méthode recommandée pour spécifier des modèles de noms de fichiers.

Pour plus d'informations sur la manière de configurer les propriétés avancées du groupe d'attributs de fichier journal, voir («Surveillance d'un fichier journal», à la page 1299), étape («6», à la page 1300). Supposons que vous avez spécifié le modèle de nom de fichier suivant :

```
d:\program files\logs\tivoli.*
```

Ce modèle permet de rechercher des fichiers dont le nom commence par `tivoli` dans le répertoire `d:\program files\logs`. Les expressions régulières peuvent être spécifiées uniquement dans la partie indiquant le nom du fichier et non dans le nom du chemin d'accès.

Syntaxe de nom de fichier dynamique

La syntaxe de nom de fichier dynamique ne permet de surveiller qu'un seul fichier à la fois. Le fournisseur de données de fichier inspecte tous les fichiers de l'emplacement désigné, à la recherche de fichiers correspondant au modèle défini. Le fournisseur de données de fichier surveille toujours le fichier correspondant le plus récent, en se basant sur le nom ayant le plus grand numéro ou la valeur date/heure la plus élevée. Le fichier approprié à surveiller est déterminé par le nom du fichier et non par la date de création de celui-ci ou d'autres critères.

Des modèles peuvent être définis pour des noms de fichier constitués d'un nombre quelconque de parties. Par exemple, `Log{###}` correspond à des noms de fichiers comportant une seule partie, tels que `Log010` ou `Log456`. Dans les noms de fichier en plusieurs parties, vous pouvez spécifier des caractères de modèle dans une ou plusieurs parties du nom de fichier. Par exemple, `aaa.bbb{???}.ccc` est un modèle valide, mais `aaa.bbb{???}.ccc{###}` également.

Remarque : Les expressions régulières constituent la méthode recommandée, à la place de la syntaxe de nom de fichier dynamique, pour spécifier des modèles de noms de fichiers. Pour plus d'informations sur les expressions régulières, voir «Modèles de nom de fichier d'expression régulière», à la page 1545.

Les exemples suivants montrent la spécification de modèle de nom de fichier :

`{#########}.abc`
: Etablit une correspondance avec les noms de fichier numériques de 8 chiffres ayant l'extension *`.abc`*, tels que `10252006.abc` et `10262006.abc`. Le fichier `10262006.abc` est surveillé, car `10262006` est supérieur à `10252006`.

`{#########}.*`
: Correspond à des noms de fichier numériques à 8 chiffres dont l'extension est ignorée. Par exemple, `20061025.log`, `20061101.log` et `10252006.abc`. Le fichier `20061101.log` est surveillé, car `20061101` est le nombre le plus grand.

`{#######??}.abc`
: Etablit une correspondances avec les noms de fichier numériques de 8 caractères ayant l'extension `.abc` et ignore les deux derniers caractères du nom. Par exemple, `02110199.abc`, `02110200.abc` et `021101AZ.abc`. Le fichier `02110200.abc` est surveillé, car `021102` est le nombre le plus grand.

Console.{######}
Etablir une correspondance avec les noms de fichiers qui contiennent *Console* dans le nom et un nombre de 6 chiffres dans l'extension. Par exemple, Console.000133, Console.000201 et Console.000134. Le fichier Console.000201 est surveillé.

IN{######}.log
Etablit une correspondance avec les noms de fichiers qui commencent par IN suivi de six chiffres et de l'extension .log. Par exemple, IN021001.log, IN021002.log et IN021004.log. Le fichier IN021004.log est surveillé.

PS{###}FTP.txt
Etablit une correspondance avec les noms de fichier qui commencent par PS suivi de trois chiffres suivis de FTP et de l'extension .txt. Par exemple, PS001FTP.txt, PS005FTP.txt et PS010FTP.txt. Le fichier PS010FTP.txt est surveillé.

Suivez les instructions ci-dessous pour définir des modèles de nom de fichier :

- Utilisez des accolades {} pour insérer des caractères de modèle dans un nom de fichier. La présence de caractères de modèle entre des accolades indique qu'un modèle de nom de fichier est utilisé.
- Utilisez l'astérisque (*) comme caractère générique pour ignorer les extensions de fichier ou les caractères finaux dans le nom de fichier. Par exemple, Myapp{###}.log* indique qu'un nom de fichier commençant par Myapp suivi de trois chiffres suivis de .log est une correspondance, indépendamment de ce qui suit.

  L'astérisque doit être indiqué après les accolades ({ }) et ne peut pas être utilisé au début d'un nom de fichier. Dans une extension de nom de fichier, l'astérisque doit être utilisé seul.

  Exemples de caractères génériques corrects (*) :

  err{??}.*

  error{$}.*

  Exemples de caractères génériques incorrects (*) :

  error.20*
  Aucune accolade ne précède l'astérisque (*).

  error*.{###}
  L'astérisque n'est pas utilisé à la fin du nom de fichier.

  error.*
  Aucune accolade ne précède l'astérisque (*).
- Si une extension de fichier spécifique est définie, seuls les fichiers comportant cette extension sont pris en considération.
- Utilisez le signe dièse pour indiquer chaque élément numérique d'un nom de fichier.
- Utilisez un point d'interrogation pour exclure chaque élément de la convention d'attribution de nom qui ne servira pas de critère de recherche dans la détermination du nom de fichier approprié.
- Utilisez le signe dollar ($) pour représenter soit un caractère ou l'absence de caractère. Par exemple, si vous voulez établir une correspondances avec les fichiers Log et LogA, spécifiez Log{$}. Plusieurs restrictions syntaxiques régissent l'utilisation du symbole du dollar. Lorsque vous utilisez un ou plusieurs caractères dollar pour le préfixe d'un nom de fichier, comme dans {$$$$$$}_abc.log, le nombre de signes dollar doit correspondre exactement au nombre de caractères dans cette position dans le nom de fichier. En outre, vous ne pouvez spécifier ces caractères dans plusieurs endroits dans un modèle de nom de fichier, par exemple, {$$$}b{$$$}.log ne correspond pas à abc.log. En raison de ces restrictions relatives au caractère dollar, utilisez des modèles de noms de fichiers dans des expressions régulières si le nombre de caractères constituant les noms de fichier recherchés est indéterminé.
- Le nombre total de signes dièse et de points d'interrogation entre les accolades est significatif. Il doit correspondre exactement à la partie Nom du nom de fichier. Par exemple, le modèle AA{####} demande au fournisseur de données de fichier de rechercher des fichiers tels que AA0001. Les noms de fichier tels que AA001 ou AA00001 sont ignorés.

- Le modèle de nom de fichier exact, la constante et les parties numériques doivent correspondre exactement au nom de fichier. Par exemple, le modèle AA{###} indique au fournisseur de données de fichier de vérifier le fichier AA101. Les noms de fichiers, tels que XAA101, AA222X et AA55555, sont ignorés.
- Utilisez la chaîne de modèle réservée {TIVOLILOGTIME} pour remplacer l'horodatage hexadécimal et le numéro d'ordre du fichier dans un fichier journal de serveur ou d'agent Tivoli Monitoring. Cette chaîne de modèle est utile lorsque vous effectuez une auto-surveillance de composants Tivoli Monitoring. Par exemple, si vous voulez surveiller le dernier journal du . dans le répertoire /opt/IBM/ITM/logs, vous pouvez indiquer un modèle de nom de fichier :

  ```
  /opt/IBM/ITM/logs/Host1_ms_{TIVOLILOGTIME}.log
  ```

  Si Host1_ms_452053c0-01.log, Host1_ms_451f11f4-01.log, Host1_ms_45205946-01.log et Host1_ms_451f11f4-02.log sont présents dans le répertoire /logs, le fichier Host1_ms_45205946-01.log est sélectionné pour la surveillance.

Pour indiquer précisément un nom de fichier constitué d'éléments de date (année, mois et jour), utilisez les lettres majuscules A, M et J. Ces lettres doivent être indiquées entre accolades pour qu'elles ne soient pas traitées comme des lettres dans le nom du fichier.

Voir les exemples suivants :

{AAAAMMJJ}.log
Indique des noms de fichier tels que 20060930.log et 20061015.log.

{MMJJAA}.log
Indique des noms de fichier tels que 101106.log et 110106.log.

{JJMMAAAA}.log
Indique des noms de fichier tels que 01092006.log et 15082006.log.

{JJMMMAA}.log
Indique des noms de fichier tels que 24Jan07 et 13Sep06.

{MM-JJ-AA}.log
Définit des noms de fichier tels que 11-02-06.log ou 04-29-07.log. Le caractère de séparation (-) est ignoré dans la zone de date et il ne nécessite pas le point d'interrogation pour être ignoré.

MY{AAJJJ}.log
Définit des noms de fichier tels que MY06202.log, MY06010.log et MY04350.log.

Dans des cas plus complexes où une zone de date est intégrée dans un nom de fichier assez long et où les modèles de date indiqués dans les exemples précédents ne sont pas suffisants, vous pouvez créer des modèles qui combinent les dièses et les points d'interrogation tout en effectuant des comparaisons numériques pour sélectionner le fichier le plus récent pour la surveillance. Par exemple, le modèle ABC{?####?##?##?##?##?##?}XYZ.TXT peut être utilisé pour des noms de fichier tels que ABC 2006-04-20 11_22_33 XYZ.TXT. Dans cet exemple, vous êtes intéressé uniquement par les chiffres indiqués par un #- et les points d'interrogation servant de marques de réservation qui ignorent les autres caractères du nom de fichier.

Le fournisseur de données de fichier vérifie régulièrement à l'emplacement cible s'il n'y a pas de nouveaux fichiers correspondant au modèle de fichier défini. Lorsqu'un fichier plus récent correspondant à ce modèle est détecté, le fournisseur de données de fichier oriente automatiquement la surveillance d'application vers ce nouveau fichier. Le fournisseur de données de fichier recherche le fichier le plus approprié lorsque :

- Le fournisseur de données de fichier démarre.
- le fichier actuellement surveillé n'existe plus parce qu'il a vraisemblablement été renommé ou supprimé.
- Le contenu du fichier existant a été modifié, probablement pour réécriture.
- l'intervalle de vérification a expiré. L'intervalle par défaut est de 10 minutes. Vous pouvez remplacer cet intervalle par une valeur inférieure ou supérieure en renseignant la variable d'environnement

```
KUMP_DP_FILE_SWITCH_CHECK_INTERVAL=nombre-de-secondes
```

Configuration des alertes SNMP

Description du fichier de configuration utilisé par le protocole SNMP Fournisseur de données pour afficher les informations des alertes sous une forme plus lisible. Le fichier est également utilisé pour attribuer des catégories, des niveaux de gravité, un statut et des ID source aux alertes.

Contient également des instructions pour modifier le fichier par défaut ou le remplacer par votre propre fichier de configuration.

Fichier de configuration des alertes SNMP, `trapcnfg`

Au démarrage, le Fournisseur de données SNMP lit un fichier de configuration nommé `trapcnfg`. L'une des finalités de ce fichier est de traduire les informations des alertes SNMP pour les rendre plus lisibles. Une autre est d'attribuer des catégories, des niveaux de gravité, un statut et des ID source à des alertes spécifiques, car ces catégories ne sont pas définies par SNMP.

Vous pouvez modifier le fichier `trapcnfg` pour répondre aux besoins spécifiques de votre site en ajoutant de nouvelles définitions d'alerte ou d'entreprise, ou en modifiant celles qui existent déjà. Vous pouvez également utiliser votre propre fichier de configuration.

Utilisation du fichier `trapd.conf` de HP OpenView

Le fichier `trapcnfg` est de format similaire, mais pas identique au fichier de configuration d'alerte de HP OpenView Network Node Manager `trapd.conf`. Vous pouvez copier le fichier OpenView et réutiliser de nombreuses instructions de définition si nécessaire.

Types d'enregistrements

`trapcnfg` contient trois types d'enregistrements ou blocs d'enregistrements :

commentaires
Les enregistrements de commentaires commencent par un dièse (#).

définitions d'entreprise
Les définitions d'entreprise sont constituées de deux jetons délimités par des espaces, où le premier jeton est un nom et le second un ID objet (OID) entouré d'accolades ({ }).

définitions d'alerte
Les définitions d'alerte sont constituées de huit jetons séparés par des espaces. Les définitions d'alerte sont des enregistrements de blocs, car chaque définition peut être composée de plusieurs enregistrements.

Le premier type n'exige aucune explication. La (Figure 87, à la page 1549) présente des exemples des types 2 et 3.

Le premier exemple cité à la Figure 87, à la page 1549 présente un enregistrement de définition d'entreprise qui définit l'ID objet entreprise 1.3.6.1.4.1.311.1.1.3.1.1 comme étant Microsoft Windows NT.

LE deuxième exemple représente un enregistrement de définition d'alerte qui définit `trapName` `MSNTCOLD` comme étant associé à l'ID objet entreprise `1.3.6.1.4.1.311.1.1.3.1.1`, numéro d'alerte générique 0 et numéro d'alerte spécifique 0. Notez que la gravité est sous forme décimale tandis que la catégorie est sous forme textuelle. La gravité est traduite sous forme textuelle avant d'être affichée. L'enregistrement suivant du bloc de type n°3 correspond à la brève description qu'Agent Builder n'utilise pas. Agent Builder utilise une description longue incluse dans les délimiteurs SDESC et EDESC.

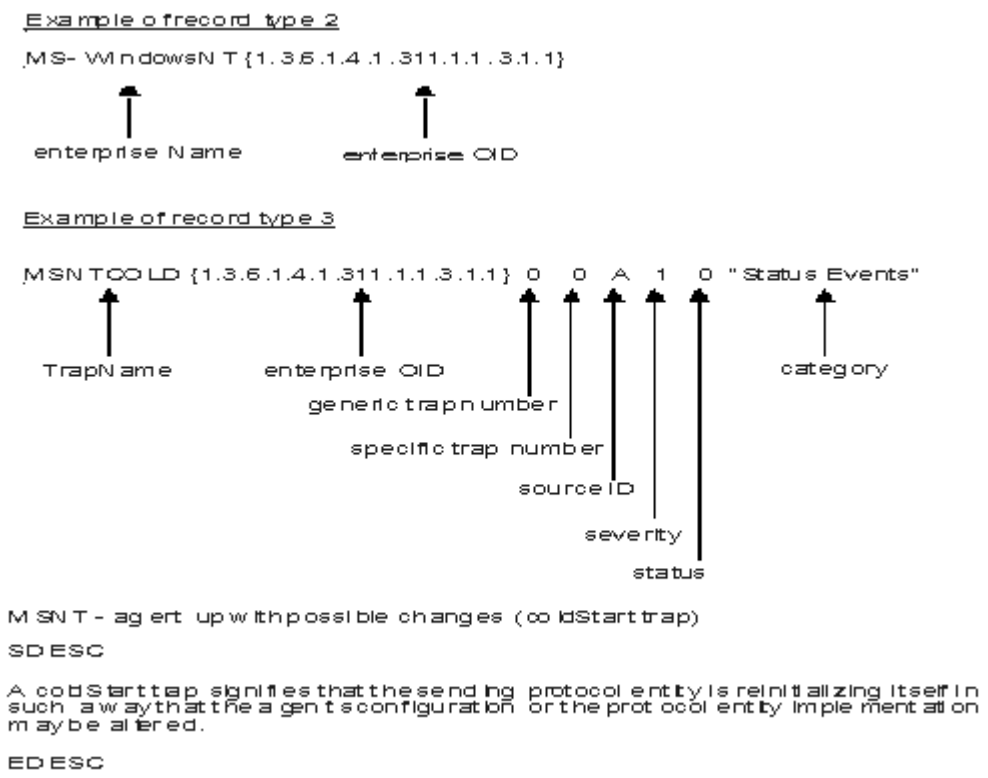


Figure 87. Exemples de types 2 et 3 d'enregistrement de configuration

Valeurs par défaut du fichier `trapcnfg`

Tableaux qui répertorient les valeurs par défaut prises en charge par le protocole SNMP Fournisseur de données.

Catégories prises en charge

Le (Tableau 308, à la page 1549) présente les catégories prises en charge par Agent Builder.

Tableau 308. Catégories prises en charge par le Fournisseur de données SNMP

Catégorie	Représentation textuelle
0	Evénements seuils
1	Evénements de topologie de réseau
2	Evénements erronés
3	Evénements de situation
4	Evénements de configuration de noeud
5	Evénements d'alerte application
6	Evénements de toutes catégories
7	Evénements de journal
8	Evénements de mappe
9	Ignorer les événements

Le (Tableau 309, à la page 1550) répertorie les niveaux de gravité pris en charge par Agent Builder.

Tableau 309. Niveaux de gravité pris en charge par le Fournisseur de données SNMP	
Gravité	**Représentation textuelle**
0	Effacer
1	Indéterminé
2	Avertiss.
3	Erreur mineure
4	Critique
5	Erreur majeure

Statuts pris en charge

Le (Tableau 310, à la page 1550) présente les statuts définis dans le fichier de configuration d'Agent Builder.

Tableau 310. Statuts pris en charge par le Fournisseur de données SNMP	
Statut	**Représentation textuelle**
0	Inchangé
1	Inconnu
2	Haut
3	Marginal
4	Bas
5	Non géré
6	Accepter
7	Utilisateur1
8	Utilisateur2

ID source pris en charge

Le (Tableau 311, à la page 1550) répertorie les ID source pris en charge par `trapcnfg`.

Tableau 311. ID source pris en charge par le Fournisseur de données SNMP	
ID source	**Description**
a	Application
A	Agent
S	Xnmcollect
d	Démo
D	Collecteur de données
E	Nvevents
I	Ipmap
L	LoadMIB
m	Shpmon

Tableau 311. ID source pris en charge par le Fournisseur de données SNMP (suite)	
ID source	**Description**
M	Topologie IP
n	Lié à netmon
N	Alertes générées par netmon
O	OSI SA
P	Alertes non IP
r	Tralertd
s	Spappld
S	Agent de sécurité
t	Xnmtrap
T	Trapd
V	Lié au fournisseur
?	Inconnu

Guide de référence des commandes Action

Présentation des commandes Action, références aux commandes Action et descriptions des commandes Action spéciales.

Commandes Action

Les commandes Action peuvent être inclues dans un agent de surveillance Agent Builder. Les commandes Action peuvent être exécutées à partir du client du portail ou incluses dans une situation ou une règle. Si une commande fait partie intégrante d'une situation, elle s'exécute lorsque cette situation est vérifiée. Une commande Action d'une situation est également appelée une automatisation réflexe. Lorsque vous activez une commande Action dans une situation, vous automatisez une réponse à des conditions du système. Par exemple, vous pouvez utiliser une commande Action pour envoyer une commande en vue de redémarrer un processus sur le système géré. Vous pouvez également utiliser une commande Action pour envoyer un message texte sur un téléphone mobile.

L'automatisation avancée utilise des règles pour exécuter des actions, planifier un travail et automatiser des tâches manuelles. Une règle comprend une série d'étapes automatisées appelées activités, reliées entre elles pour créer un flux de travaux. Une fois une activité terminée, Tivoli Enterprise Portal reçoit un code de renvoi et la logique de l'automatisation avancée répond par des activités sous-jacentes prescrites par ce code de renvoi.

Une commande Action de base affiche le code retour de l'opération dans une boîte de message ou un fichier journal qui s'affiche après l'exécution de l'action. Une fois cette fenêtre fermée, aucune autre information n'est disponible pour cette action.

Plus d'informations sur les commandes Action

Pour plus d'informations sur l'utilisation des commandes Action, voir *Tivoli Enterprise Portal - Guide d'utilisation*.

Pour obtenir la liste et la description des commandes Action pour cet agent de surveillance, voir «Commandes Action spéciales», à la page 1552. Voir aussi les informations qu'elle contient pour chaque commande individuelle.

Commandes Action spéciales

Un agent de surveillance Agent Builder peut reconnaître et exécuter un traitement spécial pour un ensemble de commandes Action spécifiques :

- SSHEXEC

Pour plus d'informations sur la création de ces commandes et leur inclusion dans un projet de l'agent de surveillance Agent Builder, voir «Création d'espaces de travail, de commandes Action et de situations», à la page 1411.

Action SSHEXEC

Avant de commencer

Pour plus d'informations sur les commandes Action, voir («Guide de référence des commandes Action», à la page 1551).

Pourquoi et quand exécuter cette tâche

L'action SSHEXEC est reconnue pour une application surveillée qui possède au moins un groupe d'attributs Script SSH. Elle indique que la commande qui suit le mot clé SSHEXEC est lancée à distance sur le système cible SSH. La commande est lancée avec les données d'identification et les droits de l'utilisateur configuré pour surveiller le système cible SSH. La commande est exécutée sur le système distant représenté par le Nom du système géré.

Procédure

Si vous souhaitez inclure la commande Action dans une règle de situation ou de flux de travaux, utilisez la syntaxe suivante pour la commande système :

```
SSHEXEC [Commande]
```

Par exemple :

```
SSHEXEC [ls &chemin]
```

Remarque : Vous pouvez personnaliser tout ou partie de la commande pendant l'appel de la commande Action en utilisant l'option des arguments Action avec la *Commande*.

Remarque : Si la *Commande* comprend plusieurs arguments, envisagez d'inclure des crochets pour permettre l'appel de la commande Action avec l'interface de ligne de commande **tacmd**.

Fonctions d'accessibilité

Les fonctions d'accessibilité aident les utilisateurs souffrant d'un handicap (mobilité réduite ou vision limitée) à se servir des contenus des technologies de l'information.

Fonctions d'accessibilité

L'interface basée sur le Web d'IBM Cloud Application Performance Management est la console Cloud APM. Cette console comprend les principales fonctions d'accessibilité suivantes :

- Elle permet aux utilisateurs d'utiliser les technologies d'assistance, tels que le logiciel de lecture d'écran et le synthétiseur de parole numérique, pour entendre ce qui est affiché à l'écran. Consultez la documentation de la technologie d'assistance pour obtenir des détails sur son utilisation avec ce produit.
- Elle permet aux utilisateurs d'utiliser des fonctions spécifiques ou équivalentes en utilisant uniquement le clavier.
- Elle communique toutes les informations indépendamment de la couleur.[1]

La console Cloud APM utilise la dernière norme W3C, WAI-ARIA 1.0 (http://www.w3.org/TR/wai-aria/), pour assurer la conformité à US Section 508 (http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) et aux Règles pour l'accessibilité des contenus Web (WCAG) 2.0 . Pour tirer parti des fonctions d'accessibilité, utilisez la dernière version de votre lecteur d'écran de pair avec le navigateur Web le plus récent pris en charge par ce produit.

La documentation en ligne de la console console Cloud APM prend en charge les fonctions d'accessibilité dans l'IBM Knowledge Center. Les fonctions d'accessibilité de l'IBM Knowledge Center sont décrites à l'adresse : IBM Knowledge Center release notes .

Navigation au clavier

Ce produit utilise les touches de navigation standard.

Informations sur l'interface

L'interface utilisateur Web de la console Cloud APM n'utilise pas de feuilles de style en cascade pour un rendu correct du contenu et fournit une expérience utilisateur satisfaisante. C'est cependant le cas de la documentation du produit. L'IBM Knowledge Center fournit un moyen équivalent pour les utilisateurs malvoyants afin d'utiliser leurs paramètres d'affichage personnalisé, y compris le mode de contraste élevé. Il est possible de contrôler la taille de police dans les paramètres du périphérique ou du navigateur.

L'interface utilisateur Web de la console Cloud APM inclut des repères de navigation WAI-ARIA dont vous pouvez vous servir pour naviguer rapidement jusqu'aux zones fonctionnelles de l'application.

L'interface utilisateur de la console Cloud APM ne dispose pas de contenu qui clignote 2 à 55 fois par seconde.

Informations sur l'accessibilité associées

En plus de l'aide IBM standard et des sites Web de support, IBM a mis en place un support téléphonique par téléscripteur destiné aux utilisateurs sourds ou malentendants pour leur permettre d'accéder aux services de ventes et d'assistance :

TTY service 800-IBM-3383 (800-426-3383) (en Amérique du Nord)

[1] Les exceptions incluent des pages **Configuration d'agent** de la console Performance Management.

IBM et l'accessibilité

Pour plus d'informations sur l'engagement d'IBM en matière d'accessibilité, consultez le site IBM Accessibility (www.ibm.com/able).

Remarques

Ces informations ont été développées pour des produits et services disponibles aux Etats-Unis. Pour vous procurer ces documents en d'autres langues, veuillez en faire la demande à IBM. Toutefois, vous devrez peut-être prouver que vous êtes propriétaire d'une copie de ce produit ou de cette version du produit dans cette langue pour prétendre à ces documents.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Une référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japon

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119

Armonk, NY 10504-1785
US

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'IBM Customer Agreement, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance décrites dans le présent document ont été calculées en conditions de fonctionnement et d'environnement spécifiques. Les résultats peuvent donc varier.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Les instructions relatives aux intentions d'IBM pour ses opérations à venir sont susceptibles d'être modifiées ou annulées sans préavis, et doivent être considérées uniquement comme des objectifs.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes ou de sociétés serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Ces exemples de programmes sont fournis "en l'état", sans garantie d'aucune sorte. IBM n'est en aucun cas responsable des dommages liés à l'utilisation de ces exemples de programmes.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright,
libellée comme suit :
© (nom de votre société) (année).
Des segments de code sont dérivés des Programmes exemples
d'IBM Corp.
© Copyright IBM Corp. 2014, 2015.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines dans de nombreux pays. Les autres noms de produit et de service peuvent appartenir à IBM ou à des tiers. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse www.ibm.com/legal/copytrade.shtml.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Dispositions relatives à la documentation du produit

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

Applicabilité

Ces dispositions s'ajoutent aux conditions d'utilisation du site Web d'IBM.

Usage personnel

Vous pouvez reproduire ces publications pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez distribuer ou publier tout ou partie de ces publications ou en faire des oeuvres dérivées sans le consentement exprès d'IBM.

Usage commercial

Vous pouvez reproduire, distribuer et afficher ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez reproduire, distribuer, afficher ou publier tout ou partie de ces publications en dehors de votre entreprise, ou en faire des oeuvres dérivées, sans le consentement exprès d'IBM.

Droits

Excepté les droits d'utilisation expressément accordés dans ce document, aucun autre droit, licence ou autorisation, implicite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LES PUBLICATIONS SONT LIVREES EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Déclaration IBM de confidentialité sur Internet

Les logiciels IBM, y compris les Logiciels sous forme de services, ("Offres Logiciels") peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Dans la plupart des cas, aucune information identifiant la personne n'est collectée par les Offres logicielles. Certaines de nos offres logicielles peuvent vous permettre de collecter des informations identifiant la personne. Si cette offre logicielle utilise des cookies pour collecter des informations identifiant la personne, des

informations spécifiques sur l'utilisation de cookies par cette offre sont énoncées dans les paragraphes ci-dessous.

En fonction des configurations déployées, cette offre logicielle peut utiliser des cookies de session qui collectent le nom d'utilisateur de chaque utilisateur à des fins de gestion des sessions, d'authentification et de configuration de la connexion unique. Ces cookies peuvent être désactivés, mais, en les désactivant, cela va aussi très probablement supprimer les fonctions qu'ils rendent possibles.

Si les configurations déployées de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation des différentes technologies, y compris les cookies, à ces fins, voir IBM's Privacy Policy à l'adresse http://www.ibm.com/privacy et IBM's Online Privacy Statement à l'adresse http://www.ibm.com/privacy/details, ainsi que les sections "Cookies, Web Beacons and Other Technologies" et "IBM Software Products and Software-as-a-Service Privacy Statement" à l'adresse http://www.ibm.com/software/info/product-privacy.