Tivoli Application Dependency Discovery Manager
Version 7.3

Guide d'administration

Tivoli Application Dependency Discovery Manager
Version 7.3

Guide d'administration

Remarque

Avant d'utiliser la présente documentation et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 287.

Notice d'édition

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.ibm.com/ca/fr (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

La présente édition s'applique à la version 7.3 d'IBM Tivoli Application Dependency Discovery Manager (numéro de produit 5724-N55) et à toutes les éditions et modifications ultérieures jusqu'à indication contraire dans les nouvelles éditions.

Table des matières

Tableaux

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	**IBM Canada**
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

A propos de la présente documentation

Ce document PDF est la version imprimable des informations fournies par le centre de documentation.

Conventions utilisées dans ce centre de documentation

Certaines conventions sont utilisées dans la documentation d'IBM® Tivoli Application Dependency Discovery Manager (TADDM). Elles permettent de se référer à des variables et des chemins d'accès dépendants du système d'exploitation, au répertoire `COLLATION_HOME` et à l'emplacement du fichier `collation.properties` dont il fait référence tout au long de la documentation de TADDM, y compris dans les messages.

Variables et chemins dépendant du système d'exploitation

Dans ce centre de documentation, les conventions UNIX sont utilisées pour spécifier des variables d'environnement et pour la notation des répertoires.

Si vous utilisez une ligne de commande Windows, remplacez $*variable* par %*variable*% pour les variables d'environnement, et remplacez toutes les barres obliques (/) par des barres obliques inverses (\) dans les chemins d'accès des répertoires.

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

Répertoire `COLLATION_HOME`

Le répertoire racine de TADDM est également nommé répertoire `COLLATION_HOME`.

Sur les systèmes d'exploitation tels que AIX ou Linux, l'emplacement par défaut pour l'installation de TADDM est le répertoire `/opt/IBM/taddm`. Par conséquent, l'emplacement du répertoire `$COLLATION_HOME` est `/opt/IBM/taddm/dist`.

Sur les systèmes d'exploitation Windows, l'emplacement d'installation par défaut de TADDM est le répertoire `c:\IBM\taddm`. Dans ce cas, l'emplacement du répertoire `%COLLATION_HOME%` est `c:\IBM\taddm\dist`.

Emplacement du fichier `collation.properties`

Le fichier `collation.properties` renferme les propriétés du serveur TADDM et inclut des commentaires sur chacune d'elles. Il se trouve dans le répertoire `$COLLATION_HOME/etc`.

Termes et définitions

Reportez-vous à la liste des termes et définitions pour vous informer sur des concepts importants dans IBM Tivoli Application Dependency Discovery Manager (TADDM).

application métier
Une collection de composants qui fournit une fonctionnalité métier que vous pouvez utiliser au niveau interne, externe ou avec d'autres applications métier.

base de données TADDM
Dans TADDM, la base de données dans laquelle les données de configuration, les dépendances et l'historique des changements sont enregistrés.

Chaque serveur TADDM, à l'exception des serveurs de reconnaissance et des serveurs de stockage secondaires, possède sa propre base de données. Les serveurs de reconnaissance ne comportent aucune base de données. Les serveurs de stockage partagent la base de données du serveur de stockage principal.

collection
Dans TADDM, groupe d'éléments de configuration.

collection d'accès
Une collection utilisée pour contrôler l'accès aux éléments de configuration et les droits de modification des éléments de configuration. Vous ne pouvez créer des collections d'accès que si la sécurité du niveau de données est activée.

Console de gestion de reconnaissance
L'interface utilisateur client TADDM permettant de gérer les reconnaissances. Cette console est également appelée console produit. Elle s'applique au déploiement d'un serveur de domaine et au déploiement de serveurs de reconnaissance dans un déploiement de serveurs de diffusion en continu. La fonction de la console est la même dans ces deux déploiements.

console produit
Voir *console de gestion de reconnaissance*.

déploiement de serveur de domaine
Un déploiement TADDM possédant un serveur de domaine. Un déploiement de serveur de domaine peut faire partie d'un déploiement de serveur de synchronisation.

Dans un déploiement de serveur de domaine, la propriété suivante du serveur TADDM doit être définie sur la valeur suivante :

```
com.collation.cmdbmode=domain
```

déploiement de serveur de synchronisation
Un déploiement TADDM avec un serveur de synchronisation et deux ou plusieurs déploiements de serveur de domaine comportant chacun sa propre base de données locale.

Dans ce type de déploiement, le serveur de synchronisation copie les données de reconnaissance de plusieurs serveurs de domaine, un domaine à la fois, au cours d'un processus de synchronisation par lots.

Dans un déploiement de serveur de synchronisation, la propriété suivante du serveur TADDM doit être définie sur l'une des valeurs suivantes :

```
com.collation.cmdbmode=enterprise
```

Ce type de déploiement est obsolète. Par conséquent, dans un nouveau déploiement TADDM, dans lequel plusieurs serveurs sont requis, utilisez le déploiement de serveurs de diffusion en continu. Vous pouvez convertir

un serveur de synchronisation en serveur de stockage principal d'un déploiement de serveurs de diffusion en continu.

déploiement de serveurs de diffusion en continu
Un déploiement TADDM avec un serveur de stockage principal et au moins un serveur de reconnaissance. Ce type de déploiement peut également inclure un ou plusieurs serveurs de stockage secondaires en option. Le serveur de stockage principal et les serveurs de stockage secondaires partagent une même base de données. Les serveurs de reconnaissance ne comportent aucune base de données.

Dans ce type de déploiement, les données de reconnaissance affluent en parallèle de plusieurs serveurs de reconnaissance pour converger vers la base de données TADDM.

Dans un déploiement de serveurs de diffusion en continu, la propriété du serveur TADDM doit être définie sur l'une des valeurs suivantes :

- `com.collation.taddm.mode=DiscoveryServer`
- `com.collation.taddm.mode=StorageServer`

Pour tous les serveurs, à l'exception du serveur de stockage principal, les propriétés suivantes (pour le nom d'hôte et le numéro de port du serveur de stockage principal) doivent également être définies :

- `com.collation.PrimaryStorageServer.host`
- `com.collation.PrimaryStorageServer.port`

Si la propriété com.collation.taddm.mode est définie, la propriété com.collation.cmdbmode ne doit pas être définie ou elle doit être placée en commentaire.

domaine
Dans TADDM, un sous-ensemble logique de l'infrastructure d'une société ou d'une autre organisation. Les domaines peuvent représenter des limites organisationnelles, fonctionnelles ou géographiques.

EC Voir *élément de configuration*.

élément de configuration (EC)
Un composant de l'infrastructure informatique sous le contrôle de la gestion des configurations et donc soumis à un contrôle formel des modifications. Chaque EC dans la base de données TADDM possède un objet persistant et un historique des changements qui lui sont associés. Exemples d'EC : système d'exploitation, interface L2, taille du pool de mémoire tampon de base de données.

équivalent serveur (ES)
Une unité représentative de l'infrastructure informatique, définie comme un système informatique (avec des configurations standard, des systèmes d'exploitation, des interfaces réseau et des interfaces de stockage) avec un logiciel serveur installé (base de données, serveur Web ou serveur d'applications, par exemple). Le concept d'équivalent serveur inclut aussi le réseau, l'archivage et les autres sous-systèmes fournissant des services pour le fonctionnement optimal du serveur. Un serveur équivalent dépend du système d'exploitation :

Système d'exploitation	Nombre approximatif d'EC
Windows	500
AIX	1000

Système d'exploitation	Nombre approximatif d'EC
Linux	1000
HP-UX	500
Périphériques réseau	1000

ES Voir *équivalent serveur*.

lancement en contexte
Concept consistant à passer de façon homogène d'une interface utilisateur de produit Tivoli à une autre interface utilisateur de produit Tivoli (soit sur une console différente, soit sur la même console ou interface de portail) avec une identification unique et avec l'interface utilisateur cible en position sur l'emplacement correct pour que les utilisateurs poursuivent leur tâche.

location multiple
Dans TADDM, l'utilisation par un fournisseur de services ou un vendeur informatique d'une installation TADDM pour découvrir plusieurs environnements clients. De plus, le fournisseur de services ou le vendeur informatique peut voir les données provenant de tous les environnements clients, mais au sein de chaque environnement client, seules les données spécifiques à un client peuvent être affichées dans l'interface utilisateur ou consultées dans les rapports inhérents à cet environnement client.

Portail de gestion de données
L'interface utilisateur Web de TADDM permettant d'afficher et de manipuler les données d'une base de données TADDM. Elle s'applique à un déploiement de serveur de domaine, à un déploiement de serveur de synchronisation et à chaque serveur de stockage dans un déploiement de serveur de diffusion en continu. L'interface utilisateur est très similaire dans tous les déploiements bien qu'elle comporte quelques fonctions supplémentaires permettant d'ajouter et de synchroniser des domaines dans le déploiement de serveur de synchronisation.

reconnaissance asynchrone
Dans TADDM, l'exécution d'un script de reconnaissance sur un système cible permettant de reconnaître des systèmes auxquels le serveur TADDM n'a pas directement accès. Cette reconnaissance s'effectuant manuellement et indépendamment d'une reconnaissance authentifiée, elle est dite «asynchrone».

reconnaissance authentifiée
L'analyse du détecteur TADDM permettant de reconnaître des informations détaillées sur les éléments suivants :

- Chaque système d'exploitation dans l'environnement d'exécution. Cette analyse est également appelée reconnaissance de niveau 2 et requiert les droits d'accès au système d'exploitation.
- L'infrastructure d'application, les composants logiciels déployés, les serveurs physiques, les périphériques réseau, les systèmes virtuels et les données hôtes utilisés dans un environnement d'exécution. Cette analyse est également appelée reconnaissance de niveau 3 et requiert les droits d'accès au système d'exploitation et à l'application.

reconnaissance basée sur un script
Dans TADDM, l'utilisation dans une reconnaissance authentifiée de scripts de détecteur identiques à ceux fournis par les détecteurs dans le support de reconnaissance asynchrone.

reconnaissance de niveau 1
L'analyse du détecteur TADDM permet de reconnaître des informations de base sur les systèmes informatiques actifs dans l'environnement d'exécution. Cette analyse est également appelée reconnaissance sans autorisation d'accès car elle ne requiert aucune autorisation d'accès. Elle utilise le détecteur Stack Scan et le détecteur de portée IBM Tivoli Monitoring. La reconnaissance de niveau 1 est très superficielle. Elle collecte uniquement le nom hôte, le nom du système d'exploitation, l'adresse IP, le nom de domaine complet et l'adresse MAC (Media Access Control) de chaque interface reconnue. De plus, la reconnaissance des adresses MAC se limite aux systèmes Linux on System z et Windows. La reconnaissance de niveau 1 ne permet pas de reconnaître les sous-réseaux. Pour chaque interface IP reconnue qui n'appartient pas à un sous-réseau existant reconnu lors d'une reconnaissance de niveau 2 ou 3, de nouveaux sous-réseaux sont créés en fonction de la valeur de la propriété `com.collation.IpNetworkAssignmentAgent.defaultNetmask` du fichier `collation.properties`.

reconnaissance de niveau 2
L'analyse du détecteur TADDM permet de reconnaître des informations détaillées sur chaque système d'exploitation de l'environnement d'exécution. Cette analyse est également appelée reconnaissance avec autorisation d'accès car elle requiert les autorisations d'accès au système d'exploitation. La reconnaissance de niveau 2 collecte les noms des applications, les noms des systèmes d'exploitation et les numéros de port associés à chaque application en cours d'exécution. Si une application a établi une connexion TCP/IP avec une autre application, ces informations sont capturées en tant que dépendance.

reconnaissance de niveau 3
L'analyse du détecteur TADDM reconnaît des informations détaillées sur l'infrastructure de l'application, les composants logiciels déployés, les serveurs physiques, les unités réseau, les systèmes virtuels et les données hôte utilisées dans l'environnement d'exécution. Cette analyse est également appelée reconnaissance avec autorisations d'accès, car elle requiert les autorisations d'accès au système d'exploitation et à l'application.

reconnaissance d'utilisation
L'analyse du détecteur TADDM reconnaît les informations d'utilisation du système hôte. La reconnaissance d'utilisation requiert les autorisations d'accès au système d'exploitation.

reconnaissance non authentifiée
L'analyse du détecteur TADDM permet de reconnaître des informations de base sur les systèmes informatiques actifs dans l'environnement d'exécution. Cette analyse est également appelée reconnaissance de niveau 1 et ne requiert aucun droit d'accès.

serveur de domaine
Un serveur TADDM exécutant des détecteurs dans un déploiement de serveur de domaine et possédant sa propre base de données.

serveur de reconnaissance
Un serveur TADDM qui exécute des détecteurs dans un déploiement de serveurs de diffusion en continu mais qui ne possède pas sa propre base de données.

serveur de stockage
Un serveur TADDM qui traite les données reçues des serveurs de reconnaissance et les enregistre dans la base de données TADDM. Le serveur de stockage principal coordonne les serveurs de reconnaissance ainsi que tous les autres serveurs de stockage et fait office de serveur de stockage. Tous les serveurs de stockage qui ne sont pas des serveurs principaux sont appelés serveurs de stockage secondaires.

serveur de synchronisation
Un serveur TADDM qui synchronise les données de reconnaissance à partir de tous les serveurs de domaine de l'entreprise et qui comporte sa propre base de données. Ce serveur ne reconnaît pas directement les données.

serveur TADDM
Une dénomination générique pouvant représenter l'une des dénominations suivantes :

- Serveur de domaine dans un déploiement de serveur de domaine
- Serveur de synchronisation dans un déploiement de serveur de synchronisation
- Serveur de reconnaissance dans un déploiement de serveur de reconnaissance
- Serveur de stockage (y compris le serveur de stockage principal) dans un déploiement de serveurs de diffusion en continu

système cible
Dans le processus de reconnaissance TADDM, le système devant être reconnu.

unité d'exécution de tâche de reconnaissance
Dans TADDM, unité d'exécution qui exécute des détecteurs.

Administration

Présentation de TADDM

IBM Tivoli Application Dependency Discovery Manager (TADDM) est un outil de gestion de la configuration permettant d'aider les équipes dédiées aux opérations informatiques de garantir et d'améliorer la disponibilité des applications dans des environnements d'application. TADDM fournit des détails sur les éléments de configuration à l'aide de sa fonction de reconnaissance sans agent automatisée des actifs et de leurs dépendances. Il propose également une technologie de bibliothèques de reconnaissance permettant d'optimiser les données provenant d'autres sources.

TADDM offre aux équipes chargées des opérations une vue descendante des applications. Elles peuvent ainsi comprendre rapidement la structure, le statut, la configuration et l'historique des modifications des applications essentielles à leur entreprise. Lorsque des problèmes liés aux performances et à la disponibilité surviennent, cette vue permet au personnel de les isoler immédiatement et de planifier plus efficacement les modifications à apporter à l'application sans générer d'interruption. La base de données TADDM, une base de données de gestion de la configuration, est créée et gérée sans modélisation de l'infrastructure personnalisée. TADDM fournit également des mappes de dépendance sur plusieurs niveaux, des vues topologiques, une fonction de suivi des modifications et de propagation des événements, ainsi que rapports et analyses détaillés.

TADDM dépend de la reconnaissance des informations, effectuée à l'aide de détecteurs déployés dans le cadre du produit TADDM. Les données résultant du processus de reconnaissance sont utilisées pour créer des mappes de dépendance sur plusieurs niveaux liant les topologies physiques et logiques. Ce répertoire hiérarchique représente la totalité de votre environnement d'exécution.

Les points suivants récapitulent les actions exécutées par TADDM :

1. Les détecteurs identifient et collectent l'identité, les attributs et les paramètres de chaque application, système et composant du réseau.
2. Les données de configuration, les dépendances et l'historique des modifications sont stockés dans la base de données TADDM et les topologies sont stockées sur le serveur TADDM. Lorsque des éléments sont reconnus, ils sont stockés dans la base de données TADDM à partir des sources suivantes :
   - Détecteurs
   - Manuels de bibliothèque de reconnaissance, également appelés manuels IdML (Identity Markup Language), qui sont générés par des systèmes logiciels de gestion externes
   - API
3. Les données de reconnaissance sont affichées sous forme de topologies d'applications d'exécution sur plusieurs niveaux dans l'interface TADDM. Les reconnaissances suivantes mettent les topologies à jour. De plus, TADDM conserve l'historique des modifications apportées à la configuration et aux dépendances de l'infrastructure.
4. TADDM génère des rapports et des vues topologiques supplémentaires des informations stockées dans la base de données TADDM.

Entités reconnues par TADDM

Le tableau 1 répertorie et décrit les entités reconnues par TADDM dans votre environnement.

Tableau 1. Entités reconnues et leur description

Entité	Description
Niveau réseau	Les périphériques suivants sont reconnus avec les valeurs de paramètre MIB2 (RFC 1213) pour chaque périphérique : • Routeurs • Commutateurs • Equilibreurs de charge • Pare-feux • Périphériques IP génériques
Niveau système	Les périphériques suivants sont reconnus au niveau du système : • Hôtes et disques du serveur • Interfaces IP hôte • Serveurs de base de données • Equilibreurs de charge ou clusters
Niveau application	Les composants suivants sont reconnus au niveau de l'application. Pour chaque composant (à l'exception des processus génériques), les informations de version, les fichiers et les propriétés de configuration, les informations sur l'hôte et les extensions provenant d'autres fournisseurs sont également reconnues. • Serveurs personnalisés, en fonction des modèles personnalisés que vous concevez • Serveurs d'applications Java EE et leur configuration • Composants et modules Java EE et Java SE • Composants des serveurs Web • Modules Web, fichiers de configuration et répertoires d'installation • Processus JVM génériques • Bases de données
Services d'infrastructure	Les services d'infrastructure du système prenant en charge l'environnement d'application sont reconnus, ainsi que la structure de dépendance entre les composants de ces services et les composants des applications. Les composants suivants se trouvent dans le service d'infrastructure : • Services DNS et NFS • LDAP
Structure des relations	Outre la reconnaissance des composants, la connectivité physique et logique au niveau du réseau, du système et des applications est reconnue au niveau de prise en charge suivant dans chaque niveau : • Connectivité IP de couche 3 • Connectivité IP de couche 2 • Dépendances d'exécution des composants d'application • Dépendances des services d'infrastructure

Les configurations et les interdépendances des entités suivantes sont également reconnues :

- Composants des applications tels que les serveurs Web, les serveurs d'applications et les bases de données
- Composants du système tels que les hôtes, les systèmes d'exploitation, les équilibreurs de charge et les serveurs de base de données
- Composants réseau tels que les routeurs, les commutateurs et les pare-feux
- Services d'infrastructure tels que les services DNS et LDAP

Remarque : L'utilisation d'adresses IP virtuelles ou de plusieurs contrôleurs d'interface réseau peut entraîner un signalement de résultats incorrects par TADDM. Lorsque vous planifiez une reconnaissance, tenez compte de l'infrastructure réseau.

Présentation de la procédure de reconnaissance

La reconnaissance est un processus multiniveau qui collecte des informations de configuration sur l'ensemble de l'infrastructure informatique en identifiant les composants logiciels déployés, les serveurs physiques, les périphériques réseau, les réseaux locaux virtuels et les données d'hôte employées dans l'environnement d'exécution. Une reconnaissance s'effectue à l'aide de détecteurs faisant partie intégrante du produit TADDM.

Le détecteur est chargé de reconnaître les éléments de configuration, de créer les objets de modèle et de conserver ces objets dans la base de données TADDM. Les détecteurs utilisent des protocoles qui sont spécifiques aux ressources qu'ils sont destinés à reconnaître. Les protocoles suivants sont des exemples:

- CDP (Cisco Discovery Protocol)
- JMX (Java™ Management Extensions)
- Secure Shell (SSH)
- SNMP (Simple Network Management Protocol)
- SQL (Structured Query Language)

Une connexion sécurisée est utilisée dans la mesure du possible entre le serveur TADDM et les systèmes cible.

TADDM n'exécute pas de reconnaissances sur des réseaux IPv6, mais les attributs IPv6 sont reconnus par des reconnaissances sur des réseaux IPv4.

Détecteurs

TADDM propose plusieurs détecteurs spécialisés permettant de reconnaître la plupart des composants se trouvant dans les différents niveaux de logiciels d'application, d'hôtes et de réseaux d'un centre de données classique. Vous pouvez également développer des détecteurs personnalisés pour des composants uniques. Les détecteurs résident sur le serveur TADDM et collectent les attributs de configuration et les dépendances.

Les détecteurs ne sont pas intrusifs, ce qui signifie qu'ils s'exécutent sur le serveur TADDM et non sur le poste de travail client. Grâce à TADDM, vous pouvez donc collecter des informations liées à la reconnaissance sans supporter les coûts d'installation locale et la maintenance d'un agent sur chaque poste de travail client que vous souhaitez reconnaître.

Les détecteurs se servant de connexions réseau sécurisées, d'autorisations d'accès chiffrées et d'utilitaires natifs hôte, ils sont sécurisés et ils fournissent le même niveau d'acquisition de données que celui proposé par le logiciel qui se trouve sur le poste de travail client.

Les détecteurs se caractérisent par les trois aspects configurables suivants :

Portée La portée de la reconnaissance est généralement une plage d'adresses IP valide, un sous-réseau ou une adresse spécifique. Elle définit les limites de la reconnaissance.

Liste d'accès
La liste d'accès est l'ensemble des autorisations d'accès tels que les noms d'utilisateur, les mots de passe, les noms de communauté SNMP (Simple Network Management Protocol) que le détecteur utilise lorsqu'il accède aux éléments de configuration de l'infrastructure d'application. Vous devez configurer la liste d'accès pour les éléments de configuration que vous souhaitez reconnaître.

Calendrier
La reconnaissance peut être exécutée à la demande ou déclenchée par des événements extérieurs. Le calendrier identifie si les détecteurs sont exécutés à la demande ou en fonction d'un calendrier.

Reconnaissance des éléments de configuration par un détecteur :

Les étapes suivantes décrivent comment un détecteur reconnaît les éléments de configuration de votre environnement.

1. Pour identifier les périphériques IP actifs dans la portée spécifiée, le détecteur tente d'établir une connexion TCP sur différents ports (par exemple les ports 22, 23 et 135) afin de détecter une réponse. Une réponse suffit à informer le détecteur que le périphérique existe.
2. Le détecteur tente de se connecter au périphérique IP sur plusieurs ports (par exemple les ports 22 et 135) afin de déterminer la technologie à utiliser pour reconnaître l'hôte.
3. Si un port utilisant le protocole SSH (Secure Shell) est ouvert, le détecteur tente d'établir une connexion SSH à l'aide des autorisations d'accès de la liste d'accès. Le détecteur tente alors d'accéder en séquence aux entrées de la liste de type **système informatique** ou **système informatique Windows** jusqu'à ce qu'une entrée fonctionne ou que le détecteur atteigne la fin de la liste d'accès sans succès.
4. Si un port WMI (Windows Management Instrumentation) est ouvert, une connexion SSH à un système informatique de passerelle (s'il en existe un pour le système cible) est établie. Le détecteur tente alors d'accéder en séquence aux entrées de la liste de type **système informatique** jusqu'à ce qu'une entrée fonctionne ou que le détecteur atteigne la fin de la liste d'accès sans succès.
5. S'il est impossible d'établir une session, un détecteur SNMP est exécuté. Si la session est établie, un détecteur de système informatique est exécuté.
6. Un détecteur de système informatique tente de déterminer le type du système d'exploitation installé.
7. TADDM exécute un détecteur propre au système d'exploitation afin de reconnaître le système d'exploitation plus en profondeur.
8. Lors de la reconnaissance en profondeur du système d'exploitation, qui se fonde sur certains critères donnés (par exemple le numéro de port et le nom de processus), TADDM exécute les détecteurs propres aux logiciels afin de reconnaître les détails relatifs aux applications.

Démarrage du détecteur d'une application :

Les informations suivantes décrivent comment démarrer le détecteur d'une application.

GenericServerSensor exécute les commandes suivantes :

Sur les systèmes d'exploitation Linux, Solaris, AIX et Linux on System z

- **lsof -nP -i** permet d'obtenir des informations sur les ports
- **ps axww** permet d'obtenir des informations de ligne de commande

Sur les systèmes d'exploitation Windows

- **netstat.exe -nao** permet d'obtenir des informations sur les ports
- **wmic process list** permet d'obtenir des informations de ligne de commande

L'ID processus (PID) permet de fusionner les sorties. Le système de recherche de modèles s'exécute alors sur les données fusionnées. Lorsque le niveau de journalisation est défini sur DEBUG dans le fichier `collation.properties`, la sortie de ces commandes est consignée dans les journaux suivants :

- `GenericServerSensor.log`
- `DiscoverManager.log`

Les données fusionnées doivent correspondre aux critères définis dans le modèle de détecteur. Les critères permettant de démarrer un détecteur sont présentés dans l'exemple de définition de modèle pour le détecteur DB2 ci-dessous :

Exécutez la commande suivante (vous pouvez la rediriger dans un fichier) en remplaçant `<nom_utilisateur>` et `<mot_de_passe>` par un nom d'utilisateur valide et le mot de passe associé (par exemple `...dist/sdk/bin/api.sh -u administrator -p collation find --depth=5 AppServerTemplate`) :

```
...dist/sdk/bin/api.sh -u <username> -p <password> find --depth=5 AppServerTemplate
```

Cette commande produit une sortie au format XML qui est la définition de modèle. Dans cette définition, si la valeur associée à l'élément `<order>` est inférieure à 0, le modèle concerne un détecteur. Si la valeur de l'élément `<order>` est supérieure à 0, le modèle concerne un serveur personnalisé. La correspondance commence par la valeur la plus basse de l'élément `<order>`, c'est pourquoi les détecteurs obtiennent une priorité de correspondance supérieure à celle des serveurs personnalisés.

L'exemple de définition de modèle suivant concerne le détecteur DB2. Notez les deux éléments `<operand>`, l'un associé à la valeur `db2tcpcm` et l'autre à la valeur `db2agent`. La valeur de l'élément `<boolExp>>` indique si une ou deux valeurs `<operand1>` doivent être présentes. La valeur 1 associée à l'élément `<boolExp>` indique que l'opérateur logique OR est utilisé, ce qui signifie qu'une seule des deux valeurs `<operand1>` doit être présente. La valeur `0` associée à l'élément `<boolExp>` indique que l'opérateur logique AND est utilisé, ce qui signifie que les deux valeurs `<operand1>` doivent être présentes.

```
<Template array="18" guid="C1A992327AFF33409C41D5C71046DBB9"
lastModified="1177555771479"
xsi:type="coll:com.collation.platform.model.discovery.template.AppServerTemplate">
   <displayName>DB2</displayName>
   <name>DB2</name>
   <type>DatabaseServer</type>
   <internal>true</internal>
   <filterSet guid="B599AED918F436C99FDA0E8EDA578F02"
```

```
   lastModified="1177555771475"
   parent="C1A992327AFF33409C41D5C71046DBB9"
   xsi:type="coll:com.collation.platform.model.discovery.template.FilterSet">
      <displayName>DB2</displayName>
      <filterList array="1"
      guid="BBE4D351653B37E38BFFD2DEBD532EE8"
      lastModified="1177555771476"
      parent="B599AED918F436C99FDA0E8EDA578F02"
      xsi:type="coll:com.collation.platform.model.discovery.template.Filter">
         <displayName>unknown</displayName>
         <operand1>db2tcpcm</operand1>
         <operator>contains</operator>
         <part>Program Name</part>
      </filterList>
      <filterList array="2"
      guid="63816C902B0A317F8C3B24C7A1EEBC17"
      lastModified="1177555771471"
      parent="B599AED918F436C99FDA0E8EDA578F02"
      xsi:type="coll:com.collation.platform.model.discovery.template.Filter">
         <displayName>unknown</displayName>
         <operand1>db2agent</operand1>
         <operator>contains</operator>
         <part>Program Name</part>
      </filterList>
      <boolExp>1</boolExp>
   </filterSet>
   <index>0</index>
   <order>-10</order>
   <enabled>true</enabled>
   <action>1</action>
   <source>0</source>
   <seedClass>com.collation.discover.seed.app.db.db2.Db2Seed</seedClass>
</Template>
```

Niveaux de reconnaissance

TADDM propose quatre niveaux de reconnaissance : la reconnaissance de niveau 1, la reconnaissance de niveau 2, la reconnaissance de niveau 3 et la reconnaissance d'utilisation.

reconnaissance de niveau 1

Analyse du détecteur TADDM permettant de découvrir des informations basiques relatives aux systèmes informatiques actifs dans l'environnement d'exécution. Cette analyse est également intitulée reconnaissance *sans autorisation d'accès* car elle ne requiert aucune autorisation d'accès. Elle utilise le détecteur Stack Scan et le détecteur de portée IBM Tivoli Monitoring.

La reconnaissance de niveau 1 est très superficielle. Elle collecte uniquement le nom hôte, le nom du système d'exploitation, l'adresse IP, le nom de domaine complet et l'adresse MAC (Media Access Control) de chaque interface reconnue. La reconnaissance des adresses MAC se limite aux systèmes Linux on System z et Windows.

La reconnaissance de niveau 1 ne permet pas de reconnaître les sous-réseaux. Pour chaque interface IP reconnue qui n'appartient pas à un sous-réseau existant reconnu lors d'une reconnaissance de niveau 2 ou 3, de nouveaux sous-réseaux sont créés en fonction de la valeur de la propriété com.collation.IpNetworkAssignmentAgent.defaultNetmask du fichier `collation.properties`.

reconnaissance de niveau 2

L'analyse du détecteur TADDM permet de reconnaître des informations détaillées sur chaque système d'exploitation de l'environnement

d'exécution. Cette analyse est également intitulée reconnaissance *avec autorisations d'accès* car elle requiert les autorisations d'accès au système d'exploitation.

La reconnaissance de niveau 2 collecte les noms des applications, les noms des systèmes d'exploitation et les numéros de port associés à chaque application en cours d'exécution. Si une application a établi une connexion TCP/IP avec une autre application, ces informations sont capturées en tant que dépendance.

reconnaissance de niveau 3
L'analyse du détecteur TADDM reconnaît des informations détaillées sur l'infrastructure de l'application, les composants logiciels déployés, les serveurs physiques, les unités réseau, les systèmes virtuels et les données hôte utilisées dans l'environnement d'exécution. Cette analyse est également connue en tant que reconnaissance *avec autorisations d'accès* car elle requiert les autorisations d'accès au système d'exploitation et à l'application.

reconnaissance d'utilisation
L'analyse du détecteur TADDM reconnaît les informations d'utilisation du système hôte. La reconnaissance d'utilisation requiert les autorisations d'accès au système d'exploitation.

Les reconnaissances de niveau 2 et 3 capturent des informations plus détaillées que celles de niveau 1. Si les objets créés lors d'une reconnaissance de niveau 2 ou 3 correspondent aux objets créés par une reconnaissance de niveau 1, ceux-ci sont remplacés par les objets nouvellement créés et les GUID correspondants sont également modifiés. Les données de niveau 1 ne doivent en général donc pas être utilisées pour l'intégration à d'autres produits.

Profils de reconnaissance

Pour exécuter une reconnaissance, vous devez spécifier un profil de reconnaissance qui définit un ensemble d'options pour la reconnaissance. A l'aide de ce profil, vous pouvez configurer des détecteurs distincts, gérer plusieurs configurations du même détecteur, choisir la configuration appropriée en fonction d'une série de critères et gérer des ensembles de configurations de différents détecteurs à appliquer à la même exécution d'une reconnaissance.

En sélectionnant le profil de reconnaissance approprié, vous pouvez contrôler la profondeur ou le niveau de la reconnaissance.

TADDM fournit par défaut quatre profils de reconnaissance. Trois correspondent aux trois niveaux de reconnaissance que vous pouvez sélectionner (niveau 1, 2 ou 3) selon que vous souhaitez exécuter une reconnaissance avec autorisations d'accès ou sans. Le profil restant est destiné aux reconnaissances d'utilisation.

Si aucun profil n'est spécifié, le profil de reconnaissance de niveau 3 est utilisé par défaut, mais vous pouvez le modifier dans la console de gestion de reconnaissance.

Pour plus d'informations sur les profils de reconnaissance, voir *A Flexible Approach to Discovery* dans le wiki TADDM à l'adresse https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Application%20Dependency%20Discovery%20Manager/page/A%20Flexible%20Approach%20to%20Discovery.

Activation et désactivation des détecteurs

Vous pouvez désactiver globalement un détecteur, même si celui-ci a été activé par un profil. Vous pouvez aussi activer de façon globale un détecteur et autoriser le fonctionnement du paramètre dans le profil.

Par exemple, si un détecteur est globalement activé et que le profil active le détecteur, le détecteur s'exécute. Si le détecteur est globalement activé mais désactivé dans le profil, le détecteur n'est pas exécuté lorsque ce profil est sélectionné dans le cadre de la reconnaissance.

Pour que l'activation et la désactivation globales des détecteurs dotés d'un répertoire `osgi` (`$COLLATION_HOME/osgi/plugins`) soient opérationnelles, vous devez modifier la commande **`AgentConfigurations`** dans le répertoire `osgi`.

Par exemple, dans le cas de Db2Sensor, recherchez ces répertoires :

- `$COLLATION_HOME/osgi/plugins/com.ibm.cdb.discover.sensor.app.db.db2_x.x.x/Db2Sensor.xml`
- `$COLLATION_HOME/osgi/plugins/com.ibm.cdb.discover.sensor.app.db.db2windows_x.x.x/Db2WindowsSensor.xml`

où *x.x.x* est la version du plug-in de détecteur, par exemple `7.3`.

Lors de l'édition des fichiers XML, définissez enabled sur `true` pour activer le détecteur. Pour désactiver le détecteur, définissez enabled sur `false`.

En ce qui concerne les détecteurs qui n'utilisent pas le répertoire `osgi/plugins`, les informations de configuration sont stockées dans le fichier XML de configuration du détecteur situé dans le répertoire `etc/discover-sensors`.

Reconnaissance asynchrone et reconnaissance basée sur un script

Dans une reconnaissance asynchrone et basée sur un script, au lieu d'exécuter des commandes individuelles, des détecteurs fournissent un script de reconnaissance, qu'ils exécutent sur le système cible.

Tous les détecteurs ne prennent pas en charge la reconnaissance asynchrone et la reconnaissance basée sur un script. Seuls les détecteurs fournissant un script de reconnaissance prennent en charge ces deux types de reconnaissance.

Pour plus d'informations sur les détecteurs qui prennent en charge la reconnaissance asynchrone et basée sur un script, voir la rubrique *Détecteurs prenant en charge une reconnaissance asynchrone et basée sur un script* dans le *Guide de référence des détecteurs* de TADDM.

Différences par rapport à une reconnaissance non basée sur un script

Il existe plusieurs différences importantes entre la reconnaissance asynchrone et la reconnaissance basée sur un script d'une part, et la reconnaissance non basée sur un script d'autre part :

- Les résultats d'une reconnaissance asynchrone ou d'une reconnaissance basée sur un script risquent de ne pas être aussi complets que les résultats d'une reconnaissance non basée sur un script de niveau 2 ou 3. La plupart des détecteurs reconnaissent un plus grand nombre d'objets de modèle, d'attributs et de relations lors d'une reconnaissance non basée sur un script que lors d'une reconnaissance asynchrone ou basée sur un script.

- Dans le cas d'une reconnaissance asynchrone ou basée sur un script, les détecteurs de l'application démarrent une seule fois pour un système cible donné. Cependant, si l'application est en mode écoute sur plusieurs ports, chaque instance d'application est reconnue.
  Lors d'une reconnaissance non basée sur un script, un détecteur d'application est démarré pour chaque instance d'application.

Reconnaissance asynchrone :

Vous pouvez exécuter une reconnaissance asynchrone pour découvrir des systèmes auxquels le serveur TADDM ne peut pas accéder directement. Il s'agit des systèmes localisés dans des emplacements sécurisés (par exemple, des systèmes qui ne sont pas accessibles par le réseau), des systèmes qui n'exécutent pas SSH (Secure Shell) et des systèmes contenant des informations sensibles et pour lesquels il est impossible d'obtenir les autorisations d'accès.

Dans la reconnaissance asynchrone, les utilisateurs exécutent un script de reconnaissance sur le système cible. Le script de reconnaissance contient un script principal et plusieurs scripts de détection. Chaque script de détection propose une fonction de reconnaissance similaire à la fonction qu'exécute le détecteur dans une reconnaissance standard.

La sortie du script de reconnaissance est un fichier archive contenant les résultats de la reconnaissance. Vous devez copier ce fichier sur le serveur TADDM. Lors de la reconnaissance TADDM, les détecteurs TADDM traitent les résultats de la reconnaissance à partir de ce fichier archive (au lieu d'exécuter des commandes.

Cette reconnaissance s'effectuant manuellement et indépendamment d'une reconnaissance nécessitant une authentification, elle est dite «asynchrone».

Pour effectuer une reconnaissance asynchrone, le détecteur de reconnaissance asynchrone est requis. Pour plus d'informations, voir le *Guide de référence des détecteurs* de TADDM.

Pour plus d'informations sur la configuration de détecteurs pour effectuer une reconnaissance asynchrone, voir «Configuration de la reconnaissance asynchrone», à la page 109.

Reconnaissance basée sur un script :

Dans une reconnaissance basée sur un script, vous pouvez utiliser un script de reconnaissance dans une reconnaissance classique où des données d'identification sont requises. Dans ce type de reconnaissance, les scripts de détecteur utilisés sont les mêmes que ceux de la reconnaissance asynchrone.

Dans une reconnaissance basée sur un script, un détecteur n'exécute pas des commandes individuelles. Le script du détecteur est à la place exécuté sur le système cible. Les autorisations d'accès propres aux applications ne sont donc pas forcément nécessaires.

Par exemple, pour reconnaître l'application IBM WebSphere lors d'une reconnaissance classique, vous devez créer une entrée de liste d'accès avec des données d'identification pour l'application WebSphere si la sécurité est activée. Cependant, si vous utilisez la reconnaissance basée sur un script, l'entrée de la liste d'accès WebSphere n'est pas nécessaire. Ce type de reconnaissance vous permet également de renoncer à utiliser des protocoles spécifiques aux applications, tels

que JMX (Java Management Extensions), qui permettent d'étendre la reconnaissance d'applications via IBM Tivoli Monitoring.

Pour plus d'informations sur la configuration de détecteurs pour effectuer une reconnaissance basée sur un script, voir «Configuration de la reconnaissance basée sur un script», à la page 113.

Reconnaissance simultanée

Vous pouvez exécuter plusieurs reconnaissances simultanément. Ce processus est connu sous le nom de *reconnaissance simultanée*. Une reconnaissance de grande amplitude pouvant durer plusieurs heures, vous pouvez souhaiter démarrer les reconnaissances de moindre amplitude avant d'exécuter une reconnaissance de grande amplitude. Avant de pouvoir exécuter des reconnaissances simultanées, vous devez les configurer correctement.

Vous pouvez exécuter une reconnaissance simultanée à l'aide d'un autre profil de reconnaissance que celui utilisé pour lancer la première reconnaissance.

Pour gérer les reconnaissances simultanées, utilisez la Console de gestion de reconnaissance ou le script `api.sh`. Pour plus d'informations sur l'utilisation du script `api.sh`, voir la rubrique *API d'interface de ligne de commande* dans le manuel *Guide du développeur SDK* de TADDM.

Il est possible d'exécuter des reconnaissances simultanées sur le même système cible. Si plusieurs reconnaissances surveillent certaines adresses IP communes, chaque reconnaissance fonctionne de façon distincte.

Si un changement de mot de passe se produit lors de l'exécution d'une reconnaissance, les détecteurs dans cette reconnaissance simultanée utilisent immédiatement les nouvelles données d'identification, à condition que ces détecteurs n'aient pas démarré avant le changement de mot de passe.

TADDM ne prend pas en charge la reconnaissance simultanée avec une liste d'accès basée sur un profil.

Si des modifications sont apportées au modèle de serveur personnalisé alors qu'une reconnaissance est en cours d'exécution, toutes les reconnaissances simultanées ayant démarré continuent à utiliser la version existante du modèle de serveur personnalisé. La nouvelle reconnaissance distincte non simultanée suivante ayant démarré utilise la nouvelle version du modèle de serveur personnalisé.

Détermination du nom de domaine complet affiché

Vous pouvez configurer une méthode de préférence pour identifier le nom de domaine complet pour chaque système reconnu.

Pour une reconnaissance de niveau 1, le nom de domaine complet est le résultat d'une recherche inversée de l'adresse IP. Cette recherche utilise la bibliothèque du programme de résolution fournie par le système d'exploitation. Elle utilise également l'une des configurations fournies ici. Si, par exemple, le fichier hôte est préféré au serveur DNS au niveau du système d'exploitation, les informations contenues dans le fichier hôte sont prises en compte en priorité.

Dans le cas d'une reconnaissance de niveau 2, TADDM exécute une recherche inversée de toutes les adresses IP reconnues à l'aide de la bibliothèque du programme de résolution fournie par le système d'exploitation. De nouveau, la configuration du système d'exploitation détermine l'endroit où la recherche

inversée obtient des informations. Si le serveur DNS n'est pas configuré ou s'il renvoie des noms de domaine complet, vous pouvez utiliser les fichiers hôte pour le remplacer.

Une fois que les adresses IP reconnues ont été recherchées, le système tente d'établir une correspondance entre un nom de domaine complet et le système informatique. Il existe différentes méthodes d'obtention d'un nom de domaine complet et toutes ces méthodes sont utilisées dans un ordre prédéfini jusqu'à ce qu'un nom de domaine complet soit identifié. Vous pouvez modifier cet ordre de sorte que votre méthode préférée soit associée à une priorité plus élevée. Les méthodes suivantes sont disponibles :

Méthode 1

TADDM sélectionne le nom de domaine complet d'une interface IP dans lequel la portion hôte de ce nom correspond au nom d'hôte du système reconnu. En cas de correspondances multiples, le nom de domaine complet dépend de la priorité du nom de domaine, tel qu'il est défini dans la propriété suivante :`com.collation.platform.os.FqdnPriorities`. Cette propriété répertorie les noms de domaine dans l'ordre de priorité. Pour définir des priorités pour les domaines, entrez le nom des domaines sous la forme d'une liste de noms séparés par des virgules, sur une seule ligne :

```
com.collation.platform.os.FqdnPriorities=domain1.company.com,
domain2.company.com,domain3.company.com
```

Le nom de domaine complet ayant la priorité la plus élevée pour son domaine est renvoyé en tant que nom de domaine complet. Cette méthode utilise les informations détectées concernant les noms de domaine complets des interfaces et des noms de système informatique.

Si les priorités ne sont pas définies, TADDM parcourt toutes les interfaces IP. TADDM vérifie si le nom de domaine complet associé à une interface IP donnée est identique au nom du système informatique ou si la partie nom d'hôte de ce nom de domaine complet est identique au nom du système informatique. Le premier nom de domaine complet correspondant aux critères est renvoyé en tant que nom de domaine complet.

Par exemple, un système informatique intitulé «myname» est équipé de deux interfaces comportant les noms de domaine complets suivants :

- interface #1 myname.domain1.com
- interface #2 myname.domain2.com

Si la propriété `com.collation.platform.os.FqdnPriorities` n'est pas définie, la première occurrence est renvoyée en tant que nom de domaine complet. La partie hôte du nom de domaine complet des deux noms correspond au nom d'hôte du système reconnu, mais le nom de domaine complet renvoyé est «myname.domain1.com». Pour déterminer le nom sélectionné en fonction de sa priorité, utilisez la propriété `com.collation.platform.os.FqdnPriorities`. Par exemple, si l'entrée `com.collation.platform.os.FqdnPriorities` contient les informations suivantes :

```
com.collation.platform.os.FqdnPriorities=domain2.com,domain1.com
```

le nom de domaine complet est «myname.domain2.com» car ce nom a une priorité plus élevée.

Méthode 2

La propriété `com.collation.platform.os.command.fqdn` définit une commande externe sur le serveur TADDM utilisé pour exécuter la

recherche inversée. Les exemples suivants montrent comment utiliser cette propriété et entrer la propriété sur une seule ligne :

```
com.collation.platform.os.command.fqdn=nslookup $1
| grep Name | awk '{print $2}'
com.collation.platform.os.command.fqdn.AIX=nslookup $1
| grep Name | awk '{print $2}'
com.collation.platform.os.command.fqdn.Linux=nslookup $1
| grep Name | awk '{print $2}'
com.collation.platform.os.command.fqdn.SunOS=nslookup $1
| grep Name | awk '{print $2}'
com.collation.platform.os.command.fqdn.Windows=nslookup $1
```

Méthode 3

La propriété `com.collation.platform.os.command.hostOfHostname` définit une commande externe sur le système cible utilisé pour fournir le nom de domaine complet. L'exemple suivant montre comment utiliser cette propriété sur un système UNIX et entrer la propriété sur une seule ligne :

```
com.collation.platform.os.command.hostOfHostname=host `hostname`
| awk {'print $1'}
```

Méthode 4

Le nom de domaine complet de l'interface principale est utilisé. L'interface IP principale est spécifiée en tant que valeur la plus faible, où les valeurs IP sont triées dans l'ordre ascendant.

Méthode 5

L'adresse IP de l'interface principale est utilisée.

Méthode 6

Le nom du système informatique est utilisé.

Méthode 7

Définissez l'IP de contexte de session.

Méthode 8

Définissez FQDN pour CS comme FQDN pour l'IP de session.

Vous pouvez définir l'ordre dans lequel ces méthodes sont utilisées en définissant la propriété `com.collation.platform.os.fqdnSearchOrder`. La valeur de cette propriété est une liste séparée par des virgules contenant les numéros des méthodes. La valeur par défaut est 1,2,3,4,5,6,7,8. Dans ce cas, TADDM tente d'abord d'utiliser la méthode 1. Si aucun nom de domaine complet n'est renvoyé, TADDM utilise la méthode 2, et ainsi de suite, jusqu'à obtention d'un nom complet valide. Un nom de domaine complet valide est conforme aux règles spécifiées dans le document RFC 1035.

Cette solution s'applique également aux systèmes informatiques reconnus par des détecteurs SNMP. Vous pouvez définir les solutions ayant une priorité plus élevée et permettant donc d'identifier plus rapidement un nom de domaine complet.

Dans tous les cas, un serveur DNS correctement configuré constitue la meilleure méthode de définition des noms d'hôte. Si cette méthode ne peut pas être utilisée, utilisez le fichier d'hôtes. Ces deux méthodes sont les méthodes standard de résolution de nom des adresses IP. TADDM propose d'autres méthodes pouvant s'y substituer, mais ces méthodes étant propres à TADDM, elles risquent de générer des noms incohérents avec les noms issus des autres systèmes de gestion.

Traçage d'une reconnaissance

Vous pouvez faire le suivi des phases d'une reconnaissance, de son démarrage à la mise à jour de l'historique des changements et de la génération des dépendances de la topologie. Chaque phase d'une reconnaissance est enregistrée dans un fichier journal associé.

Phase d'exécution d'une reconnaissance et fichier journal

Après son démarrage, chaque reconnaissance reçoit un identificateur unique (ID exécution). Un horodatage *AAAA-MM-JJ-hh:mm:ss:SSS* identifie l'exécution de la reconnaissance ; par exemple, `20110517225225948`. La partie *AAAA-MM-JJ* correspond à l'année, au mois et au jour. La partie *hh:mm:ss.sss* indique l'heure du jour sur une horloge au format 24 heures, avec une précision des millièmes de seconde. Dans l'exemple précédent, la date est 2011/05/17 et l'heure 22:52:25.948. Cet identificateur permet de distinguer les fichiers journaux de chaque détecteur dans le répertoire `$COLLATION_HOME/log/sensors`. L'horodatage est utilisé dans les fichiers journaux.

Lors d'une reconnaissance, le gestionnaire de flux de processus surveille l'état de la reconnaissance et des événements du détecteur. Le gestionnaire de flux de processus gère aussi le passage d'un service à un autre. L'activité du flux de processus est stocké dans le fichier `$COLLATION_HOME/log/services/ProcessFlowManager.log` sur le serveur de reconnaissance ou de domaine.

Les exemples suivants montrent diverses activités surveillées par le gestionnaire de flux de processus et comment ces informations sont stockées dans le fichier journal.

Démarrage de la reconnaissance :

```
– 2011-05-17 22:53:01,643 ProcessFlowManager [RMI TCP Connection(42)-127.0.0.1] INFO
processflowmgr.ProcessFlowManagerImpl - [ProcessFlowManagerImpl.I.0] startDiscovery()
started discovery with run id 2,011,051,722,525,948
– 2011-05-17 22:53:01,643 ProcessFlowManager [RMI TCP Connection(42)-127.0.0.1] INFO
processflowmgr.ProcessFlowManagerImpl - [ProcessFlowManagerImpl.I.22] startDiscovery()
 setting the discoveryRun's run id to 2,011,051,722,525,948
– 2011-05-17 22:53:01,973 ProcessFlowManager [RMI TCP Connection(42)-127.0.0.1] INFO
processflowmgr.ProcessFlowManagerImpl -
Discovery run, 2011051722525948 started with profile Level 2 Discovery
```

Reconnaissance terminée :

```
– 2011-05-17 22:56:11,689 ProcessFlowManager [RMI TCP Connection(45)-127.0.0.1] INFO
processflowmgr.ProcessFlowManagerImpl - [ProcessFlowManagerImpl.I.36]
discoveryDone(2,011,051,722,525,948) called by Discovery Manager
```

Evénement de reconnaissance :

```
– 2011-05-17 22:53:49,901 ProcessFlowManager [RMI TCP Connection(45)-127.0.0.1] INFO
processflowmgr.ProcessFlowManagerImpl - [ProcessFlowManagerImpl.I.32]
discoveryProgress(2,011,051,722,525,948, Discovered - The CustomAppServerSensor
(JavaServer 9.156.47.175:36750) sensor discovered the following: CustomAppServerResult,
 JavaServer,9.156.47.175:36750.) called by Discovery Manager
```

Phase de génération de la topologie et fichier journal

Le générateur de topologie génère les relations et les dépendances entre les éléments de reconnaissance. Le générateur de topologie exécute une liste d'agents répertoriés dans le fichier `$COLLATION_HOME/etc/TopologyBuilderConfigurationDefault.xml`. Les agents de la topologie s'exécutent à des intervalles spécifiés. Toutefois, les événements se produisent lors d'une reconnaissance et quand une reconnaissance est terminée peuvent aussi déclencher le générateur de topologie. Chaque agent exécute une tâche spécifique : par exemple, consolider, identifier des dépendances, générer des graphiques de dépendances et supprimer d'anciennes informations. Les fichiers journaux du générateur de topologie sont stockés dans les fichiers `$COLLATION_HOME/log/`

services/TopologyBuilder.log et $COLLATION_HOME/log/agents/*.log sur le serveur de domaine, le serveur de synchronisation et le serveur de stockage principal.

Les exemples suivants montrent les différentes étapes au moment d'établir des relations et illustrent comment ces informations sont stockées dans le fichier journal.

Démarrage de l'exécution du générateur :

```
– 2011-05-17 22:56:11,717 TopologyBuilder [RMI TCP Connection(158)-127.0.0.1]
INFO cdb.TivoliStdMsgLogger
- CTJOT0400I Topology builder is starting.
```

Générateur de topologie terminé :

```
– 2011-05-17 23:16:39,429 TopologyBuilder [TopologyBuilderEngineThread$Dependency@0.5]
 INFO engine.TopologyBuilderEngine - Topology agent completed :
 all normally in seconds 30.367
```

Passage à l'agent de topologie suivant :

```
– 2011-05-17 23:16:29,774 TopologyBuilder [TopologyBuilderEngineThread$Dependency@0.5]
INFO cdb.TivoliStdMsgLogger - CTJOT0403I Topology builder agent class
com.ibm.cdb.topomgr.topobuilder.agents.ComputerSystemConsolidationAgent is stopping.
– 2011-05-17 23:16:30,078 TopologyBuilder [TopologyBuilderEngineThread$Dependency@0.5]
INFO cdb.TivoliStdMsgLogger - CTJOT0402I Topology builder agent class
com.ibm.cdb.topomgr.topobuilder.agents.ComputerSystemTypeAgent is starting.
```

En cas de problème (par exemple, le générateur de topologie se bloque), consultez le dernier agent de topologie démarré dans le fichier journal pour l'identifier. Si le fichier TopologyBuilder.log ne contient aucune entrée, consultez les entrées du fichier TopologyManager.log après l'horodatage du dernier agent démarré. Si vous savez quels agents sont à l'origine du problème, vous pouvez également consulter le fichier $COLLATION_HOME/log/agents/agentName.log pour les repérer.

Autres services et fichiers journaux

Le gestionnaire des changements traite les événements et met à jour les enregistrements de l'historique des changements. Ce traitement est indépendant de la phase de reconnaissance ; il reçoit des événements d'autres services (par exemple, le processus du générateur de topologie et le programme de chargement en bloc). Quand vous ouvrez une vue de topologie, le gestionnaire de vue génère les structures requis pour l'interface graphique afin de rendre la topologie de façon efficace. Les journaux de services sont stockés dans le répertoire $COLLATION_HOME/log/services. Chaque journal de service porte le même nom que le service : par exemple, le fichier services/ChangeManager.log.

Les exemples suivants montrent comment ces informations sont stockées dans les fichiers journaux de service.

Gestionnaire des changements :

```
2011-05-19 13:22:42,342 ChangeManager [ChgWork-1] INFO changemgr.
ChangeManagerPersisterImpl -
[ChangeManagerPersister.I.3] Got a create or delete event
```

Gestionnaire de vues :

```
2011-05-19 16:37:22,428 ViewManager [RMI TCP Connection(174)-127.0.0.1]
INFO viewmgr.ViewMetaLoader - [ViewMetaLoader.I.31] getViewMeta()
found view meta definition for view Business Application Topology
```

Mise en cache des dernières données d'identification ayant fonctionné

TADDM peut placer en cache les dernières données d'identification d'accès ayant fonctionné. Elles peuvent être réutilisées lors de la prochaine reconnaissance (niveau 2 ou basées sur un script).

Lors de la reconnaissance initiale d'une cible, le serveur TADDM procède à une itération dans la liste d'accès et valide chaque élément par rapport à la cible de la reconnaissance. Lorsque les données d'identification valides sont détectées, elles sont stockées dans un cache et réutilisées lors des reconnaissances suivantes de la même cible de reconnaissance.

Un cache peut stocker les deux valeurs suivantes :

données d'identification
: Cette valeur est stockée dans un cache si les données d'identification valides d'une cible de reconnaissance sont détectées lors de la reconnaissance. Lors de la reconnaissance suivante, elles sont lues à partir du cache et le système vérifie si elles sont toujours valides. Si elles le sont, elles sont utilisées pour la reconnaissance. Si elles ne les sont plus et que la rétromigration est désactivée, les informations indiquant que la dernière tentative a échoué sont stockées sur le serveur et la reconnaissance est arrêtée. Si la rétromigration est activée, le serveur effectue la rétromigration via la liste d'accès et tente de rechercher de nouvelles données d'identification valides. Pour activer la rétromigration, définissez la propriété `com.ibm.cdb.security.auth.cache.fallback.failed` sur `true`.

informations indiquant que la dernière tentative a échoué (avec la dernière erreur)
: Cette valeur est stockée dans un cache si les données d'identification valides d'une cible de reconnaissance sont introuvables lors de la reconnaissance. Si la rétromigration est désactivée, les informations indiquant que la dernière tentative a échoué sont affichées et la reconnaissance est arrêtée. Si la rétromigration est activée, le serveur effectue la rétromigration via la liste d'accès et tente de rechercher de nouvelles données d'identification valides. Pour activer la rétromigration, définissez la propriété `com.ibm.cdb.security.auth.cache.fallback.invalid` sur `true`.

Par défaut, la rétromigration est activée dans les deux cas. Vous pouvez personnaliser le comportement de rétromigration et la mise en cache des données d'identification en définissant de manière appropriée les propriétés de mise en cache des données d'identification d'accès.

Remarque : Les données d'identification sont mises en cache par adresse IP, balise d'emplacement, type de données d'identification et protocole utilisés lors de la connexion. Lorsqu'une entrée d'accès est supprimée, toutes les entrées de cache associées le sont également. Le cache des données d'identification peut être géré par le nouvel utilitaire cachemgr.

Limitations

- La mise en cache des données d'identification n'est pas utilisée dans la reconnaissance de niveau 3. Elle n'est utilisée que dans la reconnaissance de système informatique de niveau 2 et les détecteurs basés sur un script.
- Un cache ne suit pas les modifications relatives aux restrictions d'accès de portée. Par exemple, si une cible de reconnaissance se trouve dans la restriction

d'accès de la portée et qu'elle est reconnue et mise en cache, puis déplacée hors de la restriction sectorisée, la valeur en cache est toujours utilisée.

- La valeur en cache est prioritaire par rapport à la liste d'accès profilée. Par exemple, si vous exécutez la reconnaissance à l'aide de la liste d'accès principale et que les données d'identification valides sont stockées, la valeur du cache est toujours utilisée, même si vous spécifiez d'autres données d'identification dans un profil.

Vous pouvez supprimer une valeur en cache à l'aide de l'utilitaire cachemgr. Si vous utilisez souvent des profils différents avec des entrées d'accès différentes sur la même cible ou portée de reconnaissance, vous pouvez en désactiver la mise en cache. Sinon des données d'identification incorrectes risquent d'être utilisées dans la reconnaissance.

Présentation du processus de génération de topologie

TADDM exécute le processus de génération de la topologie de façon régulière. Une fois ce processus terminé à la suite d'une reconnaissance ou d'une opération de chargement en bloc, la base de données TADDM risque de contenir des objets non synchronisés et les relations de topologie risquent d'être incomplètes.

Quel que soit le type de déploiement TADDM choisi, le processus est identique.

La génération de topologie se compose des opérations suivantes :

Nettoyage de la base de données TADDM
Ce processus supprime les anciennes entités, les dépendances autres que les sources ou les cibles, ainsi que d'autres éléments qui sont remplacés.

Etablissement de dépendances entre les éléments de configuration
Ce processus crée des dépendances entre des processus qui communiquent, par exemple entre une application et la base de données sous-jacente ou entre l'envoi et la réception de files d'attente WebSphere MQ. Il établit également des dépendances entre différentes parties d'un cluster d'applications ou, plus simplement, entre deux systèmes informatiques.

Création et augmentation des éléments de configuration
Ce processus utilise les informations des éléments de configuration existants et les connexions pour synthétiser de nouveaux éléments de configuration. TADDM peut par exemple créer un élément de configuration appelé «ApplicationServerClusters» à partir des informations dérivées des reconnaissances antérieures et des opérations de chargement en bloc.

Création d'informations pour les vues des topologies
Ce processus génère et stocke les informations pouvant être utilisées par le portail de gestion de données pour afficher plus rapidement les vues des topologies.

Exportation des données
Le processus interroge la base de données TADDM pour exporter les informations d'élément de configuration vers des systèmes externes. Par exemple, l'intégration aux services de registre est implémentée comme agent de topologie.

Fichiers journaux et journalisation

Le *Guide de résolution des problèmes* de TADDM et ses rubriques décrivent les fichiers journaux de TADDM ainsi que la configuration de la journalisation pour l'identification et la résolution des problèmes.

Sécurisation de l'environnement

Dans les environnement sécurisés, TADDM impose l'authentification qui permet la protection des informations confidentielles.

Vous pouvez utiliser le portail de gestion de données pour configurer les comptes utilisateur. Chaque utilisateur doit disposer d'un compte utilisateur valide pour utiliser le portail de gestion de données afin d'accéder aux informations reconnues relatives aux composants du réseau et de l'infrastructure.

Lorsque vous vous connectez à la console de gestion de reconnaissance et que vous sélectionnez l'option **Etablir une session (SSL)**, toutes les données sont chiffrées (y compris les noms d'utilisateurs et les mots de passe) avant d'être envoyées via le réseau.

Lors du processus de reconnaissance, le serveur TADDM utilise le protocole SSH (Secure Shell) pour communiquer de façon sécurisée avec tous les ordinateurs hôte et avec les autres unités prenant en charge SSH.

Le serveur prend en charge l'authentification SSH par clé et l'authentification SSH par connexion et par mot de passe. Lorsque l'authentification SSH par connexion et par mot de passe est utilisée, les noms d'utilisateur et les mots de passe définis dans les listes d'accès sont utilisés lors de la connexion aux ordinateurs hôte en vue de la reconnaissance.

Voir aussi «Propriétés de sécurité», à la page 97.

Contrôle de l'accès utilisateur aux éléments de configuration

TADDM contrôle l'accès utilisateur aux éléments de configuration via l'utilisation de collections d'accès, de rôles et d'autorisations.

Le contrôle d'accès aux éléments de configuration est établi par le processus suivant :

1. Les éléments de configuration sont ajoutés aux collections d'accès.
2. Les rôles sont définis pour regrouper des ensembles de droits.
3. Les utilisateurs ou les groupes d'utilisateurs sont définis et des rôles sont affectés à chacun d'eux pour lui accorder des droits spécifiques (pour des collections d'accès particulières).

Dans le contexte de sécurité de TADDM, un utilisateur est une personne ayant accès aux éléments de configuration, alors qu'un groupe d'utilisateurs rassemble plusieurs utilisateurs dotés des mêmes rôles ou autorisations.

Vous pouvez créer des utilisateurs et des groupes d'utilisateurs dans le portail de gestion de données. L'accès des utilisateurs et des groupes d'utilisateurs aux éléments de configuration est défini par les rôles et les collections d'accès attribués à chaque utilisateur ou groupe d'utilisateurs. Vous pouvez modifier ces attributions à tout moment.

Autorisations

Une autorisation permet à l'utilisateur d'exécuter une action ou d'accéder à un élément de configuration spécifique. Les droits sont ajoutés aux rôles et par conséquent accordés aux utilisateurs en fonctions des rôles qui leur ont été attribués.

TADDM fournit quatre autorisations, chacune classée comme une autorisation au niveau des données ou au niveau de la méthode.

Autorisations au niveau des données

Les droits de lecture et de mise à jour sont des autorisations au niveau des données.

Lecture
L'utilisateur peut afficher des informations sur un élément de configuration.

Mise à jour
L'utiliser peut modifier des informations relatives à un élément de configuration.

Autorisations au niveau de la méthode

Les droits de reconnaissance et d'administration sont des autorisations au niveau de la méthode.

Reconnaissance
L'utilisateur peut lancer une reconnaissance, créer et mettre à jour des objets de la portée de reconnaissance, ou encore créer des objets à partir du le menu d'édition de la console de gestion de reconnaissance, par exemple.

Un utilisateur sans droit de reconnaissance ne peut pas se connecter à la console de gestion de reconnaissance ou afficher l'onglet Reconnaissance dans le portail de gestion de données.

Administration
L'utilisateur peut créer ou mettre à jour des utilisateurs, des rôles et des droits. Il peut aussi configurer des règles d'autorisation avec le gestionnaire d'autorisation.

Activation de la sécurité au niveau des données

Vous pouvez activer la sécurité au niveau des données pour les systèmes d'exploitation AIX, Linux, Linux on System z et Windows en éditant le fichier `collation.properties`.

Pour ce faire, vous pouvez octroyer de façon sélective des droits de lecture et de mise à jour en procédant comme suit.

1. Dans le fichier `collation.properties`, recherchez la ligne suivante et remplacez la valeur de la propriété par `true` :
   ```
   com.collation.security.enabledatalevelsecurity=false
   ```
2. Sauvegardez le fichier.
3. Arrêtez le serveur TADDM.
4. Redémarrez le serveur TADDM.

Remarque : Dans un déploiement de serveur de diffusion en continu, vous devez mettre à jour le fichier`collation.properties` sur chaque serveur de stockage et redémarrez ces derniers.

Vous pouvez définir des droits granulaires en créant des collections d'accès. Si la sécurité au niveau des données est activée, les principales ressources de TADDM peuvent être sécurisées à l'aide de collections d'accès. Si la sécurité au niveau des données est activée, les utilisateurs peuvent uniquement modifier les EC figurant dans les collections d'accès pour lesquelles ils disposent du droit de mise à jour.

Les ressources auxiliaires telles que les ressources géographiques physiques et les attributs `SiteInfo` ne s'affichent pas lors de la création d'une collection d'accès.

Rôles

Un rôle est un ensemble de droits qui peuvent être accordés à un utilisateur. L'attribution d'un rôle confère des capacités d'accès spécifiques.

Lorsque vous affectez un rôle à un utilisateur, vous devez spécifier une ou plusieurs collections d'accès pour ce rôle. Vous pouvez ainsi limiter la portée du rôle aux seules collections d'accès adaptées à cet utilisateur.

Par exemple, Sarah est responsable des serveurs et des postes de travail NT de votre entreprise, et vous lui attribuez le rôle de superviseur pour une collection d'accès contenant ces systèmes. Gérard est responsable des systèmes Linux, et vous lui affectez le rôle Superviseur pour une collection d'accès contenant ces systèmes. Même si Sarah et Gérard possèdent le même rôle (car ils exécutent les mêmes opérations), ils ont accès à des ressources distinctes.

Remarque : Si vous utilisez un serveur de synchronisation, vous devez créer le rôle pour chaque domaine TADDM et synchroniser les serveurs de domaine avec le serveur de synchronisation.

Rôles prédéfinis

TADDM fournit les rôles prédéfinis suivants :

opérateur
Ce rôle possède des droits de lecture.

superviseur
Ce rôle possède des droits de lecture, de mise à jour et de reconnaissance.

administrateur
Ce rôle possède des droits de lecture, de mise à jour, de reconnaissance et d'administrateur.

Autres rôles que vous pouvez créer

Vous pouvez créer d'autres rôles pour affecter d'autres combinaisons de droits. Les combinaisons suivantes peuvent s'avérer très utiles :

Lecture + Mise à jour
Droit de lire et de mettre à jour des objets dans des collections d'accès affectées.

Lecture + Mise à jour + Admin
Droit de lire et de mettre à jour des objets dans les collections d'accès attribuées et de créer des utilisateurs, des rôles et des autorisations.

Collections d'accès

TADDM ne gère pas l'accès aux éléments de configuration sur une base individuelle. Les éléments de configuration sont par contre ajoutés dans des ensembles appelés collections d'accès. Une collection d'accès est un ensemble d'éléments de configuration qui est géré collectivement pour des raisons de sécurité.

La sécurité de chaque collection d'accès est gérée en créant des rôles et en attribuant les rôles aux utilisateurs. Le rôle s'applique uniquement à l'accès aux collections que vous avez spécifiées lors de l'affectation du rôle à un utilisateur. Les collections d'accès servent alors à limiter la portée du rôle.

Quand vous installez TADDM, la collection d'accès nommée `DefaultAccessCollection` est créée et contient tous les éléments de configuration. Tous les utilisateurs possèdent par défaut des droits de lecture et de mise à jour pour cette collection d'accès, sauf si la sécurité au niveau des données est activée.

Remarque : Les utilisateurs ne disposent pas des droits permettant de lire et de mettre à jour des collections d'accès, ils peuvent uniquement lire et mettre à jour des éléments de configuration individuels. Toutefois, des utilisateurs disposent des droits de lecture et de mise à jour pour ces collections d'accès qui appartiennent aux collections d'accès qui leur sont affectées.

Réinitialisation des règles de sécurité

Pour réinitialiser les règles de sécurité (droits, rôles et collections d'accès) à leur état par défaut, remplacez deux fichiers. La réinitialisation des règles de sécurité demande toutefois la suppression et la nouvelle création de tous les utilisateurs.

Pourquoi et quand exécuter cette tâche

Les règles de sécurité sont stockées dans les deux fichiers suivants dans le répertoire `$COLLATION_HOME/var/policy`, qui servent à les initialiser :

- `AuthorizationPolicy.xml`
- `AuthorizationRoles.xml`

Une fois les règles de sécurité initialisées, ces fichiers sont renommés et stockés dans le même répertoire. Par exemple, les fichiers suivants ont été renommés :

- `AuthorizationPolicy.backup.xml`
- `AuthorizationRoles.backup.xml`

Les versions par défaut des fichiers, qui contiennent les règles de sécurité fournies, se trouvent dans le même répertoire. Les fichiers suivants sont les versions par défaut :

- `DefaultPolicy.xml`
- `DefaultRoles.xml`

Procédure

Pour restaurer les règles de sécurité par défaut, procédez comme suit :

1. Pour sauvegarder les fichiers de règles en cours, renommez-les ou déplacez-les vers un autre répertoire.
2. Supprimez tous les utilisateurs créés.
3. Supprimez le répertoire `$COLLATION_HOME/var/ibmsecauthz`.

4. Créez une copie du fichier `DefaultPolicy.xml` et nommez-la `AuthorizationPolicy.xml`.
5. Créez une copie du fichier `DefaultRoles.xml` et nommez-la `AuthorizationRoles.xml`.
6. Redémarrez le serveur.
7. Le cas échéant, créez des utilisateurs.

Verrouillages

Vous pouvez utiliser des verrouillages pour bloquer l'accès à TADDM à un seul utilisateur ou à tous les utilisateurs, en cas de dépassement du nombre de tentatives de connexion autorisé. La fonction de verrouillage offre un meilleur contrôle de l'authentification et prévient le cassage de mot de passe par force brute.

Un verrouillage local se déclenche si un utilisateur dépasse le nombre de tentatives de connexion autorisé. L'utilisateur ne peut plus se connecter à TADDM pendant un laps de temps défini.

Lorsqu'un verrouillage général se déclenche, aucun utilisateur ne peut se connecter à TADDM pendant un laps de temps défini. Les verrouillages généraux se déclenchent dans l'une des deux situations suivantes :

- Le nombre de verrouillages actifs des différents utilisateurs dépasse le nombre maximal de verrouillages généraux autorisé.
- Le nombre de tentatives de connexion pour les noms d'utilisateurs uniques dépasse la limite autorisée.

Le déclenchement des verrouillages n'affecte pas les sessions existantes.

Vous pouvez spécifier le nombre de tentatives de connexion autorisé et la durée d'activation d'un verrouillage en configurant les propriétés du fichier `collation.properties`. Pour plus d'informations sur ces propriétés, voir «Propriétés de verrouillage», à la page 93.

Lorsqu'un verrouillage général expire, les verrouillages locaux actifs sont automatiquement annulés.

Dans un déploiement de serveur de synchronisation, le serveur de synchronisation contrôle la sécurité de tous les domaines TADDM. Les verrouillages actifs sur le serveur de domaine avant sa connexion au serveur de synchronisation sont annulés à l'activation de la synchronisation entre le serveur de domaine et le serveur de synchronisation.

Les tentatives de connexion comptant dans le nombre autorisé de tentatives de connexion peuvent être de tous types, par exemple, de type API CLI, API Java, outils (scripts), SOAP, REST, console de gestion de reconnaissance ou portail de gestion de données. La fonction de verrouillage est compatible avec les intégrations qui utilisent l'API TADDM, mais n'est pas compatible avec les connexions via authentification unique ou les intégrations de base de données, par exemple Tivoli Common Reporting.

Les administrateurs de serveur TADDM peuvent annuler un verrouillage local ou général en utilisant le script `$COLLATION_HOME/bin/lockmgr.sh`. Vous pouvez exécuter le script depuis les serveurs suivants :

- Serveur de domaine, dans un déploiement de serveur de domaine
- Serveur de synchronisation, dans un déploiement de serveur de synchronisation

- Serveur de stockage principal, dans un déploiement de serveur de diffusion

Vous pouvez exécuter le script `lockmgr.sh` avec les options suivantes :

`lockmgr.sh -s`
Affiche le statut du verrouillage.

`lockmgr.sh -g`
Annule un verrouillage général actif.

`lockmgr.sh -u` *`nom_utilisateur`*
Annule un verrouillage local actif pour un utilisateur particulier.

`lockmgr.sh -h`
Affiche les informations d'aide du script `lockmgr.sh`.

Chiffrement

Le chiffrement est un processus de transformation des données pour les rendre inintelligibles ; de cette façon, les données originales ne peuvent pas être obtenues, ou peuvent seulement l'être à l'aide d'un processus de déchiffrement.

Fix Pack 5 TADDM se sert de la propriété "*com.collation.security.algo.aes.keylength*" afin de déterminer quel algorithme (AES 128 ou AES 256) du fournisseur de sécurité "*IBMJCEFIPS conforme aux normes FIPS*" utiliser pour chiffrer les éléments suivants :

- Mots de passe, dont les entrées dans les fichiers `collation.properties` et `userdata.xml`
- Les entrées de liste d'accès stockées dans la base de données

Par exemple :

Cette propriété définit la longueur de clé d'AES :
`com.collation.security.algo.aes.keylength=128`.

Lors de la première installation de TADDM, une clé de chiffrement est générée et les mots de passe sont chiffrés à l'aide celle-ci. L'emplacement par défaut pour la clé de chiffrement est le fichier `etc/TADDMSec.properties`.

Modification de l'emplacement de la clé de chiffrement de TADDM

Pour modifier l'emplacement de la clé de chiffrement, modifiez la valeur de la propriété `com.collation.security.key` dans le fichier `collation.properties`. Vous pouvez définir cette propriété sur un autre emplacement relatif au répertoire `$COLLATION_HOME`.

Pour éviter les pertes de données, enregistrez une copie de sauvegarde de la clé de chiffrement à un emplacement distinct. Elle peut être restaurée en cas de problème avec la copie originale.

Changement de la clé de chiffrement de TADDM dans un déploiement de serveur de domaine

Remarque : TADDM ne prend pas en charge le changement de la clé de chiffrement après installation dans un déploiement de serveur de diffusion et un déploiement de serveur de synchronisation.

Pour changer la clé de chiffrement TADDM dans un déploiement de serveur de domaine, utilisez le script `bin/changekey.sh` (ou le script de traitement par lots équivalent). Ce script migre les entrées chiffrées des fichiers `collation.properties` et `userdata.xml` et les entrées des listes d'accès stockées dans la base de données. Pour utiliser le script `bin/changekey.sh`, vérifiez que vous êtes connecté sous l'utilisateur non-superutilisateur qui a été défini lors de l'installation.

Vous devez redémarrer TADDM après avoir utilisé ce script.

Format d'exécution du script

```
./changekey.sh $COLLATION_HOME utilisateur_admin mdp_admin
```

Exemple

```
./changekey.sh /opt/IBM/taddm/dist administrator taddm
```

Compatibilité avec FIPS

Vous pouvez configurez TADDM pour qu'il fonctionne dans un mode employant des algorithmes compatibles FIPS pour le chiffrement, en définissant la propriété FIPSMode **com.collation.security.FIPSMode** à `true`.

Définissez la propriété **com.collation.security.FIPSMode** à `true` dans les fichiers suivants :

- `$COLLATION_HOME/dist/etc/collation.properties`
- `$COLLATION_HOME/dist/sdk/etc/collation.properties`
- `sdk/etc/collation.properties` de toutes les installations du kit de développement de logiciels (SDK) de TADDM qui se connectent à un TADDM compatible FIPS.

La valeur par défaut de la propriété **com.collation.security.FIPSMode** est `false`.

En mode FIPS, TADDM utilise les fournisseurs cryptographiques certifiés FIPS 140-2 suivants :

- IBMJCEFIPS (certificat 376)
- IBMJSSEFIPS (certificat 409)

Pour plus d'informations sur les certificats 376 et 409, voir le site Web du National Institute of Standards and Technology (NIST), http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2004.htm.

Le mode FIPS peut être utilisé avec tous les types de reconnaissances TADDM avec les exceptions suivantes :

- Reconnaissance SNMP de niveau 2
- Reconnaissance i5/OS de niveau 2
- Reconnaissance ZEnterprise de niveau 2
- Reconnaissance VMware ESXi de niveau 2
- Reconnaissance VMware Virtual Center de niveau 3
- Reconnaissance JBoss de niveau 3
- Reconnaissance Oracle Application Server de niveau 3
- Reconnaissance WebLogic de niveau 3
- Reconnaissance SAP CCMS et SLD de niveau 3
- Reconnaissance EMC de niveau 3
- Fix Pack 1 Reconnaissance Sybase de niveau 3

- Reconnaissances de niveau 2 et de niveau 3 dans lesquelles une session Windows Management Instrumentation (WMI) ou PowerShell (les sessions PowerShell sont prises en charge dans TADDM version 7.3.0.2 ou ultérieures) est utilisée pour reconnaître des plateformes Windows, uniquement si un serveur TADDM sous Windows, des passerelles Windows et des cibles de la reconnaissance Windows ne sont pas exécutés en mode compatible FIPS. Pour configurer des serveurs Windows pour qu'ils s'exécutent en mode compatible FIPS, reportez-vous à la documentation Windows, par exemple http://support.microsoft.com/kb/811833.

Si en mode FIPS, les détecteurs TADDM qui utilisent SSH ne peuvent pas se connecter aux serveurs prenant en charge uniquement le protocole SSHv1 ou uniquement le protocole SSHv2 avec des chiffrements trop faibles. TADDM n'est pas en mesure de vérifier que l'implémentation SSH sur des serveurs cible est compatible FIPS. Vous devez vérifier que les implémentations SSH que vous utilisez dans votre environnement sont compatibles FIPS.

En mode FIPS, lorsque vous utilisez le kit de développement de logiciels (SDK) de TADDM et la console de gestion de reconnaissance en mode sécurisé, seul IBM Java est pris en charge.

Concepts associés:

«Conformité à SP800-131»
Vous pouvez configurer TADDM pour prendre en charge la norme de sécurité SP800-131a du National Institute of Standards and Technology (NIST).

Conformité à SP800-131

Vous pouvez configurer TADDM pour prendre en charge la norme de sécurité SP800-131a du National Institute of Standards and Technology (NIST).

La norme de sécurité SP800-131a impose des longueurs de clé plus longues et une cryptographie plus robuste que pour d'autres normes, comme la norme FIPS 140-2. Elle nécessite également le protocole TLS (Transport Layer Security) v1.2. Pour plus d'informations, voir http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf.

Pour activer la norme SP800-131a, définissez la propriété `com.ibm.jsse2.sp800-131` sur `strict` dans les fichiers suivants :

- `$COLLATION_HOME/dist/etc/collation.properties`
- `$COLLATION_HOME/dist/sdk/etc/collation.properties`
- `sdk/etc/collation.properties` de chaque installation de TADDM qui se connecte à un TADDM compatible SP800-131.

Par défaut, la propriété `com.ibm.jsse2.sp800-131` n'est pas définie.

Le mode de conformité SP800-131a est pris en charge pour les mêmes types de reconnaissances TADDM que dans le cas du mode FIPS.

En mode SP800-131, TADDM utilise le protocole SSL le plus sécurisé (TLS v1.2) dans les communications chiffrées. Vérifiez que les exigences suivantes sont respectées.

- Si vous utiliser le portail de gestion de données sur un port SSL Web (HTTPS), vous devez d'abord configurer votre navigateur Web pour le prise en charge du protocole TLS v1.2.

- Si vous utilisez le kit de développement de logiciels (SDK) de TADDM et la console de gestion de reconnaissance en mode sécurisé, vous devez activer le protocole TLS v1.2 dans votre environnement Java Runtime Environment. En outre, seul IBM Java est pris en charge.
- Si votre certificat SSL n'est pas conforme à la norme SP800-131a, vous devez le re-créer. Pour les étapes requises, voir «Installation de certificats SSL personnalisés à utiliser dans TADDM», à la page 35.

Concepts associés:

«Compatibilité avec FIPS», à la page 23
Vous pouvez configurez TADDM pour qu'il fonctionne dans un mode employant des algorithmes compatibles FIPS pour le chiffrement, en définissant la propriété FIPSMode **com.collation.security.FIPSMode** à `true`.

Sécurité du déploiement d'un serveur de synchronisation

Si vous faites le déploiement d'un serveur de synchronisation, vous devez effectuez les changements de sécurité lors de la configuration du serveur de synchronisation pour votre environnement.

Si vous utilisez le registre TADDM basé sur les fichiers et qu'un domaine TADDM ait été ajouté à un serveur de synchronisation, vous devez recréer sur ce serveur les utilisateurs existant déjà dans le domaine, ainsi que les rôles qui leur sont affectés et les droits d'accès aux collections qui leur sont octroyés. Si vous utilisez un registre d'utilisateurs LDAP (Lightweight Directory Access Protocol) ou un registre d'utilisateurs des référentiels fédérés WebSphere, vous devez ajouter au serveur de synchronisation l'autorisation pour chaque utilisateur d'accéder à TADDM.

Lorsque vous ajoutez un domaine au serveur de synchronisation, les opérations d'authentification et d'autorisation relatives à ce domaine sont déléguées au serveur de synchronisation.

Les connexions au domaine sont traitées par le serveur de synchronisation. En outre, les appels de méthode du gestionnaire de sécurité sont traitées par le serveur de synchronisation.

La liste suivante répertorie les informations sur la sécurité que vous devez connaître pour configurer votre serveur de synchronisation :

- Le portail de gestion de données doit être en cours d'exécution sur le serveur de synchronisation pour que TADDM fonctionne correctement. Un domaine TADDM délègue les opérations de sécurité au portail de gestion de données et cette délégation est mise à jour toutes les 2,5 minutes. Si 5 minutes s'écoulent sans mise à jour, le domaine TADDM ne délègue plus les opérations de sécurité et se comporte comme si aucun serveur de synchronisation n'était présent. Vous devez alors redémarrer les interfaces utilisateur de TADDM pour rétablir les sessions avec le serveur de synchronisation.
- Dans chacune des situations suivantes, une interface utilisateur TADDM doit être redémarrée pour que les sessions avec le serveur de synchronisation approprié soient rétablies.
  - Le domaine dans lequel l'interface utilisateur s'exécute est ajouté au portail de gestion de données qui s'exécute sur un serveur de synchronisation.
  - L'interface utilisateur est ouverte dans un domaine alors que celui-ci est connecté à un portail de gestion de données, mais le serveur de synchronisation devient indisponible parce qu'il doit redémarrer ou parce qu'un problème s'est produit sur le réseau.

- Les rôles, les droits et les collections d'accès stockés dans le serveur TADDM sont synchronisés à partir du domaine vers le serveur de synchronisation. Les mappages entre utilisateurs et rôles ne sont pas synchronisés.
- Les rôles que vous avez créés pour le domaine peuvent être utilisés par le serveur de synchronisation une fois que ces objets sont synchronisés à partir du domaine dans le serveur de synchronisation.
- Les utilisateurs ne sont pas synchronisés dans le serveur de synchronisation.
- Un registre d'utilisateurs central tel qu'un registre LDAP ou un registre des référentiels fédérés WebSphere est le mode d'authentification préféré pour le serveur de synchronisation. En cas d'utilisation d'un registre d'utilisateurs central, les mots de passe des utilisateurs sont stockés en un même lieu.
- Les collections d'accès ne peuvent pas s'étendre sur plusieurs domaines.
- La synchronisation s'effectue à partir du domaine dans le serveur de synchronisation. Les objets créés dans le serveur de synchronisation ne sont pas propagés au domaine.
- Créez des collections d'accès dans le domaine, remplissez-les, puis synchronisez-les avec le serveur de synchronisation.
- Créez des rôles dans le domaine et synchronisez-les avec le serveur de synchronisation.
- Autorisez les utilisateurs du serveur de synchronisation à fournir un accès aux collections à partir de plusieurs domaines.

Sécurité du déploiement d'un serveur de diffusion en continu

Si vous utilisez un déploiement de serveur de diffusion en continu, l'authentification et l'autorisation sont déléguées au serveur de stockage principal.

Si vous utilisez le registre TADDM basé sur les fichiers, vous devez créer et autoriser les utilisateurs TADDM sur le serveur de stockage principal. Si vous utilisez un registre d'utilisateurs LDAP (Lightweight Directory Access Protocol) ou un registre d'utilisateurs des référentiels fédérés WebSphere, vous devez autoriser les utilisateurs TADDM sur le serveur de stockage principal. Les registres préférés pour l'authentification TADDM sont les registres d'utilisateurs centraux tels que les registres LDAP ou les registres des référentiels fédérés WebSphere.

Les connexions aux serveurs de reconnaissance et aux serveurs de stockage secondaires sont traitées au niveau du serveur de stockage principal. L'authentification de l'utilisateur est donc effectuée par rapport au registre d'utilisateurs pour lequel le serveur de stockage principal est configuré. En outre, les fonctions du gestionnaire de sécurité sont traitées par le serveur de stockage principal.

Le serveur de stockage principal doit être en cours d'exécution pour que TADDM fonctionne correctement.

Si le serveur de stockage principal est arrêté ou redémarré, une interface utilisateur TADDM doit être redémarrée pour établir de nouvelles sessions avec le serveur de stockage principal.

Configuration pour LDAP

Vous pouvez configurer un serveur LDAP externe pour l'authentification d'utilisateur.

Avant de commencer

Pour vous authentifier auprès d'un registre d'utilisateurs LDAP, configurez un registre LDAP V2 ou V3.

Pourquoi et quand exécuter cette tâche

Quand vous utilisez LDAP et/ou VMM, les utilisateurs et/ou les groupes LDAP sont toujours stockés dans LDAP/VMM et ne doivent pas être créés dans TADDM. TADDM sert uniquement à affecter des rôles aux utilisateurs et groupes LDAP. Seuls ces mappages utilisateur/groupe à rôle, appelés autorisations, doivent être créés et stockés dans TADDM. L'ID administrateur est un utilisateur TADDM interne spécial toujours traité à l'aide de la sécurité basée fichier du registre d'utilisateurs configuré. Cet utilisateur peut toujours servir à affecter des rôles aux utilisateurs et groupes LDAP.

Procédure

Pour utiliser LDAP ou VMM pour l'authentification d'utilisateurs, procédez comme suit :

1. Configurez TADDM pour utiliser le registre LDAP en configurant les propriétés appropriées dans le fichier collation.properties.
2. Connectez-vous au portail de gestion de données à l'aide de l'ID administrateur TADDM.
3. Exécutez l'une des étapes suivantes :
   - Dans le panneau Utilisateurs, servez-vous de la zone **Rechercher des utilisateurs** pour rechercher l'utilisateur approprié dans le registre LDAP.
   - Dans le panneau Groupes d'utilisateurs, servez-vous de la zone **Rechercher des groupes** pour rechercher le groupe d'utilisateurs approprié dans le registre LDAP.

   Remarque : Les résultats de la recherche répertorie les noms d'utilisateurs ou de groupes renvoyés par la recherche dans le registre LDAP. Vous ne pouvez pas créer des ou copier des utilisateurs de LDAP dans TADDM. Le but de cette liste est d'afficher les autorisations TADDM devant être créées pour les utilisateurs.
4. Une fois l'utilisateur (ou le groupe) répertorié, affectez-lui les rôles TADDM requis. Seules ces autorisations, et non les utilisateurs (ou groupes) LDAP, sont stockées dans TADDM.

Que faire ensuite

Pour configurer SSL pour LDAP, procédez comme suit :

1. Dans le fichier `collation.properties`, recherchez la propriété suivante et remplacez sa valeur `false` par `true` :

   ```
   com.collation.security.auth.ldapUseSSL
   ```
2. Configurez les propriétés de magasin de clés et de magasin de clés de confiance suivantes, comme approprié :

   ```
   com.collation.security.auth.ldapClientKeyStore
   com.collation.security.auth.ldapClientKeyStorePassphrase
   com.collation.security.auth.ldapClientTrustStore
   com.collation.security.auth.ldapClientTrustStorePassphrase
   ```

3. Si besoin est, changez le port sur lequel le serveur LDAP écoute les connexions SSL en configurant la propriété suivante :
   `com.collation.security.auth.ldapPortNumber`

Configuration pour les référentiels fédérés WebSphere

Si vous avez une application Tivoli WebSphere configurée pour un registre d'utilisateurs central utilisant les référentiels fédérés WebSphere, vous ne pouvez effectuer la configuration pour les référentiels fédérés WebSphere que dans un registre de référentiels fédérés.

Configuration du serveur TADDM en vue de l'utilisation des référentiels fédérés WebSphere

Les référentiels fédérés WebSphere sont des méta-référentiels de WebSphere qui prennent en charge plusieurs types de registres utilisateur, y compris Microsoft Active Directory.

Avant de commencer

Vous devez configurer TADDM pour utiliser les référentiels fédérés WebSphere si vous vous servez d'autres produits Tivoli dans votre environnement et que vous avez besoin d'une connexion unique entre TADDM et l'un des produits Tivoli suivants :

- IBM Tivoli Change and Configuration Management Database (CCMDB) ou IBM SmartCloud Control Desk (SCCD)
- IBM Tivoli Business Service Manager

TADDM requiert des services supplémentaires non présents dans la distribution WebSphere standard. Lorsque vous configurez TADDM pour les référentiels fédérés, vous devez donc utiliser l'une des installations de WebSphere suivantes :

- WebSphere Application Server Network Deployment, installé avec CCMDB ou SCCD
- WebSphere Application Server, tel qu'installé avec IBM Tivoli Business Service Manager

Pour connaître les versions prises en charge des produits, accédez à la section «Versions prises en charge», à la page 201.

Avant de démarrer cette procédure, vous devez déjà avoir configuré le service d'authentification des référentiels fédérés WebSphere sur un serveur WebSphere Application Server Network Deployment. Pour plus d'informations, voir la documentation d'IBM Tivoli Change and Configuration Management Database (CCMDB) ou d'IBM SmartCloud Control Desk (SCCD).

Pourquoi et quand exécuter cette tâche

Cette configuration permet une connexion unique entre des applications Tivoli avec des jetons WebSphere Lightweight Third-Party Authentication (LTPA). Par exemple, la configuration de TADDM en vue de l'utilisation des référentiels fédérés WebSphere utilisés par CCMDB ou SCCD prend en charge la connexion unique pour le lancement en contexte entre IBM Tivoli CCMDB ou IBM SCCD et TADDM.

Pour configurer automatiquement TADDM en vue de l'utilisation des référentiels fédérés WebSphere, installez TADDM et sélectionnez **Référentiels WebSphere Federated** en tant que registre d'utilisateurs lors de l'installation.

Cette configuration est prise en charge sur tous les types de serveur TADDM, sur tous les déploiements.

Procédure

Pour effectuer manuellement la configuration, procédez comme suit :

1. Arrêtez le serveur TADDM.
2. Indiquez le module de gestion des utilisateurs utilisé par ce serveur TADDM. Les valeurs suivantes sont valides :

   fichier Cette valeur est utilisée pour un registre d'utilisateurs basée sur le fichier (valeur par défaut).

   ldap Cette valeur est utilisée pour un registre d'utilisateurs LDAP.

   vmm Cette valeur est utilisée pour un registre d'utilisateurs qui utilise les référentiels fédérés de WebSphere Application Server.

   Par exemple, dans le fichier `$COLLATION_HOME/etc/collation.properties` :

   ```
   com.collation.security.usermanagementmodule=vmm
   ```

3. Définissez le nom d'hôte et le port WebSphere dans le fichier `collation.properties`. Par exemple :

   ```
   com.collation.security.auth.websphereHost=localhost
   com.collation.security.auth.websperePort=2809
   ```

   Lors de la spécification du port WebSphere dans le fichier `collations.properties`, utilisez la propriété suivante : `com.collation.security.auth.websperePort`. Le port WebSphere devrait être le port d'amorce pour le serveur WebSphere. Pour WebSphere Application Server et la version intégrée de WebSphere Application Server, le port par défaut est 2809. Pour WebSphere Application Server Network Deployment, qu'IBM Tivoli CCMDB ou IBM SCCD utilise, le port par défaut est le port 9809.
4. Indiquez le nom d'utilisateur et le mot de passe de l'administrateur WebSphere dans le fichier `collation.properties`. Par exemple :

   ```
   com.collation.security.auth.VMMAdminUsername=administrator
   com.collation.security.auth.VMMAdminPassword=password
   ```

5. Modifiez comme suit le fichier de configuration des services d'authentification :
   - Pour les systèmes d'exploitation Linux, AIX et Linux on System z, le fichier se trouve à l'emplacement suivant : `$COLLATION_HOME/etc/ibmessclientauthncfg.properties`.
   - Pour les systèmes d'exploitation Windows, le fichier se trouve à l'emplacement suivant : `%COLLATION_HOME%\etc\ibmessclientauthncfg.properties`.

   Dans la propriété `authnServiceURL`, remplacez le nom de domaine qualifié complet du système sur lequel votre instance WebSphere est installée et le port HTTP de cette instance WebSphere.

   ```
   # Ceci est l'adresse URL du service d'authentification
   authnServiceURL=http://localhost:9080/TokenService/services/Trust
   ```

6. Copiez les fichiers WebSphere `orb.properties` et `iwsorbutil.jar` dans le JRE utilisé par votre installation TADDM. Par exemple, dans une installation TADDM sur Linux, procédez comme suit :
   a. Copiez `dist/lib/websphere/6.1/orb.properties` dans `dist/external/jdk-Linux-i686/jre/lib/`.

b. Copiez `dist/lib/websphere/6.1/iwsorbutil.jar` dans `dist/external/jdk-Linux-i686/jre/lib/ext/`.

7. Définissez le nom d'hôte et le port WebSphere dans le fichier `sas.client.props` :
   - Pour les systèmes d'exploitation Linux, AIX et Linux sur System z, le fichier se trouve dans l'emplacement suivant : `$COLLATION_HOME/etc/sas.client.props`.
   - Pour les systèmes d'exploitation Windows, le fichier se trouve dans l'emplacement suivant : `%COLLATION_HOME%\etc\sas.client.props`, par exemple :

     ```
     com.ibm.CORBA.securityServerHost=host1.austin.ibm.com
     com.ibm.CORBA.securityServerPort=2809
     ```

   Remarque : Pour WebSphere Application Server et la version intégrée de WebSphere Application Server, le port par défaut est 2809. Pour WebSphere Application Server Network Deployment, qu'IBM Tivoli CCMDB ou IBM SCCD utilise, le port par défaut est 9809.
8. Définissez le nom d'utilisateur et le mot de passe de l'administrateur WebSphere dans le fichier `sas.client.props`. Par exemple :

   ```
   # Identité de l'utilisateur RMI/IIOP
   com.ibm.CORBA.loginUserid=administrator
   com.ibm.CORBA.loginPassword=password
   ```
9. Facultatif : Pour chiffrer le mot de passe de la connexion dans le fichier `sas.client.props`, procédez comme suit :
   a. Copiez le fichier `sas.client.props` sur le serveur TADDM dans le répertoire `$COLLATION_HOME/etc`.
   b. Chiffrez le mot de passe de la façon suivante, en fonction du système d'exploitation sur lequel vous avez installé WebSphere.
      - Pour les systèmes d'exploitation Linux, AIX et Linux sous System z :

        Utilisez la commande `PropFilePasswordEncoder.sh`.
      - Pour les systèmes d'exploitation Windows :

        Utilisez `PropFilePasswordEncoder.bat`. Par exemple :

        ```
        C:\WebSphere\profiles\AppSrv01\bin\PropFilePasswordEncoder C:\temp\sas
          .client.props com.ibm.CORBA.loginPassword
        ```
   c. Copiez le fichier `sas.client.props` dans le serveur TADDM, dans le répertoire `etc`.
10. Démarrez le serveur TADDM.

Que faire ensuite

Une fois l'installation terminée, vous pouvez utiliser l'utilisateur administrateur par défaut défini dans le référentiel basé sur le fichier TADDM pour configurer les utilisateurs TADDM supplémentaires, y compris les administrateurs TADDM. Ces utilisateurs sont authentifiés à l'aide des référentiels fédérés WebSphere.

Il existe des configurations de sécurité pour Tivoli CCMDB ou IBM SCCD qui permettent de créer et d'entretenir des groupes et des appartenances à des groupes dans les applications d'utilisateur et de groupe Maximo.

Lorsque Tivoli CCMDB ou IBM SCCD est configuré dans ce sens, TADDM utilise son propre référentiel séparé à partir de Tivoli CCMDB ou d'IBM SCCD. Des utilisateurs doivent être créés dans Tivoli CCMDB ou IBM SCCD/Maximo et TADDM.

TADDM peut être configuré de sorte à utiliser les définitions d'utilisateurs et de groupes dans des registres d'utilisateurs externes via les référentiels fédérés WebSphere. Toutefois, TADDM ne peut pas utiliser les définitions d'utilisateurs et de groupes stockées dans Tivoli CCMDB car elles ne sont pas prises en charge par les référentiels fédérés WebSphere.

Mise à jour des clés LTPA du service d'authentification

Si vous utilisez la connexion unique avec les référentiels fédérés WebSphere, les clés LTPA (Lightweight Third-Party Authentication) doivent rester synchronisées avec les clés utilisées par les référentiels fédérés WebSphere.

Procédure

Si les clés LTPA utilisées par les référentiels fédérés WebSphere sont modifiées, utilisez cette procédure pour resynchroniser les clés utilisées par le service d'authentification :

1. Exportez les nouvelles clés LTPA WebSphere :
   a. Dans la console d'administration de WebSphere, accédez à **Administration, applications et infrastructures sécurisées** > **Mécanismes d'authentification et expiration**.
   b. Pour la **connexion unique intercellule**, indiquez un nom de fichier et un mot de passe pour le fichier devant contenir les clés LTPA exportées.
2. A l'invite de commande, accédez au répertoire `bin` du profil WebSphere approprié.
3. Exécutez la commande WebSphere **`wsadmin`** suivante :

   ```
   wsadmin> $AdminTask importESSLTPAKeys {-pathname pathname -password password}
   ```

   où *nom_chemin* et *mot_de_passe* représentent les valeurs que vous avez spécifiées pour le nom de fichier et le mot de passe lors de l'exportation des clés LTPA.
4. Redémarrez le serveur WebSphere.

Sécurisation du canal d'authentification

Lorsque vous configurez TADDM pour utiliser des référentiels fédérés WebSphere, vous pouvez sécuriser les communications entre le client d'authentification et le service d'authentification.

Pourquoi et quand exécuter cette tâche

TADDM utilise un service d'authentification prenant en charge la connexion unique. Le service d'authentification est installé en même temps qu'IBM Tivoli Change and Configuration Management Database (IBM SmartCloud Control Desk (SCCD)) ou IBM Tivoli Business Service Manager.

Pour connaître les versions prises en charge des produits, accédez à la section «Versions prises en charge», à la page 201.

Vous pouvez sécuriser les communications entre un client d'authentification et un service d'authentification de deux façons :

- SSL
- Authentification du client

Configuration du canal d'authentification pour SSL :

Vous pouvez sécuriser les communications à l'aide de certificats de signataire WebSphere afin de configurer SSL entre le client d'authentification et le serveur d'authentification.

Procédure

Pour effectuer la configuration pour SSL entre le client d'authentification et le serveur d'authentification, procédez comme suit :

1. Procédez de l'une des façons suivantes :
   a. Si vous utilisez l'instance WebSphere installée par Tivoli Integrated Portal, sélectionnez **Certificat SSL et gestion des clés** > **Gérer les configurations de sécurité du noeud final** > **Node1** > **Fichiers de clés et certificats** > **NodeDefaultTrustStore** > **Certificats de signataire**.
   b. Si vous utilisez l'instance WebSphere installée par CCMDB (Tivoli Change and Configuration Management Database) ou IBM SmartCloud Control Desk, sélectionnez **Certificat SSL et gestion des clés** > **Gérer les configurations de sécurité du noeud final** > **ctgNode01** > **Fichiers de clés et certificats** > **NodeDefaultTrustStore** > **Certificats de signataire**.
2. Exportez les certificats de signataire WebSphere dans des fichiers (exportez par exemple dummyclientsigner dans `signer1.cert` et dummyserversigner dans `signer2.cert`). Si vous ne savez pas quels certificats exporter, vous devez exporter tous les certificats de signataire.
3. Copiez les fichiers `.cert` sur le serveur TADDM. Créez un fichier de clés certifiées et importez les certificats de signataire WebSphere en procédant comme suit :

```
$COLLATION_HOME/external/jdk-Linux-i686/jre/bin/keytool \
-genkey -alias truststore -keystore truststore.jks
$COLLATION_HOME/external/jdk-Linux-i686/jre/bin/keytool \
-import -trustcacerts -alias default -file signer1.cert -keystore truststore.jks
$COLLATION_HOME/external/jdk-Linux-i686/jre/bin/keytool \
-import -trustcacerts -alias dummyserversigner -file signer2.cert -keystore truststore.jks
```

4. Ajoutez le mot de passe et l'emplacement du fichier de clés certifiées dans les entrées suivantes du fichier `$COLLATION_HOME/etc/collation.properties` :

```
com.collation.security.auth.ESSClientTrustStore=/opt/IBM/taddm/dist/etc/truststore.jks
com.collation.security.auth.ESSClientTrustPwd=password
```

5. Mettez à jour l'URL de Tivoli Authentication Service dans le fichier `ibmessclientauthncfg.properties` de sorte à utiliser https et le port 9443. Vérifiez que le nom d'hôte WebSphere est correct en le remplaçant par localhost et vérifiez que l'entrée non HTTPS est mise en commentaire.

```
# This is the URL for the ESS Authentication Service
#authnServiceURL=http://localhost:9080/TokenService/services/Trust
authnServiceURL=https://localhost:9443/TokenService/services/Trust
```

Configuration de l'authentification client :

Pour configurer l'authentification client entre le client d'authentification et le serveur d'authentification, il est conseillé d'activer la sécurité d'application WebSphere.

Avant de commencer

Une fois la sécurité d'application WebSphere activée, vous pouvez ajouter le rôle TrustClientRole à l'utilisateur administrateur WebSphere que vous avez désigné lors de l'installation de TADDM. Cette méthode permet d'améliorer la sécurité du service d'authentification, puisque seuls les utilisateurs dotés du rôle

TrustClientRole peuvent s'authentifier auprès de ce service.

Procédure

Pour attribuer le rôle TrustClientRole à l'administrateur WebSphere désigné lors de l'installation de TADDM, procédez comme suit :

1. Connectez-vous à la console d'administration WebSphere.
2. Dans l'onglet **Sécurité**, cliquez sur **Applications d'entreprise**. Le panneau Applications d'entreprise s'affiche.
3. Dans la colonne Nom du tableau Applications d'entreprise, cliquez sur l'application Service d'authentification (authnsvc_ctges). La sous-fenêtre Applications d'entreprise > authnsvc_ctges s'affiche.
4. Dans la sous-fenêtre Applications d'entreprise > authnsvc_ctges, dans la liste Propriétés détaillées, cliquez sur **Mappage de rôle de sécurité sur un utilisateur/groupe**. La sous-fenêtre Applications d'entreprise > authnsvc_ctges > Mappage de rôle de sécurité sur un utilisateur/groupe s'affiche.
5. Dans le tableau de la sous-fenêtre Applications d'entreprise > authnsvc_ctges > Mappage de rôle de sécurité sur un utilisateur/groupe, procédez comme suit :
   - Dans le tableau, cochez la case en regard de TrustClientRole.
   - Désactivez la case à cocher **Tous**.
   - Cliquez sur le bouton de **recherche d'utilisateurs** ou de **recherche de groupes**. La sous-fenêtre Enterprise Applications > authnsvc_ctges > Mappage de rôle de sécurité sur un utilisateur/groupe > Recherche d'utilisateurs ou de groupes s'affiche.
   - Dans la sous-fenêtre Applications d'entreprise > authnsvc_ctges > Mappage de rôle de sécurité sur un utilisateur/groupe > Recherche d'utilisateurs ou de groupes, procédez comme suit :
     – Recherchez des utilisateurs ou des groupes à l'aide des zones de saisie Limite et Recherche. Lorsqu'un groupe ou un utilisateur est trouvé, il apparaît dans la liste Disponible.
     – Dans la liste Disponible, sélectionnez l'utilisateur ou le groupe souhaité.
     – Cliquez sur **Déplacer** pour ajouter cet utilisateur ou ce groupe à la liste **Sélectionné**.
   - Cliquez sur **OK**. La sous-fenêtre Applications d'entreprise > authnsvc_ctges > Mappage de rôle de sécurité sur un utilisateur/groupe s'affiche.
   - Dans la sous-fenêtre Applications d'entreprise > authnsvc_ctges > Mappage de rôle de sécurité sur un utilisateur/groupe, décochez la case **Tous**.
   - Cliquez sur **OK**. La sous-fenêtre Applications d'entreprise > authnsvc_ctges s'affiche.
   - Cliquez sur **Sauvegarder** pour sauvegarder la configuration. Le panneau Applications d'entreprise s'affiche.
   - Cliquez sur **OK**. La sous-fenêtre Applications d'entreprise > authnsvc_ctges s'affiche.

Configuration de Microsoft Active Directory

Vous pouvez utiliser Microsoft Active Directory en tant que méthode d'authentification pour TADDM en utilisant LDAP ou les référentiels fédérés de WebSphere comme intermédiaires. Si la connexion unique à TADDM est nécessaire, vous devez utiliser les référentiels fédérés WebSphere.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser les utilisateurs définis par un registre Active Directory, sans en définir de nouveaux, en configurant TADDM de sorte à utiliser Active Directory. Vous pouvez configurer TADDM en vue d'utiliser Active Directory en tant que registre LDAP ou en vue d'utiliser les référentiels fédérés WebSphere, puis configurer les référentiels fédérés WebSphere pour Active Directory.

Lorsque vous configurez TADDM en vue de l'utilisation d'Active Directory, vous pouvez également autoriser TADDM à utiliser n'importe quel utilisateur d'Active Directory en tant qu'administrateur TADDM. L'administrateur est autorisé à configurer l'accès à TADDM et à autoriser les autres utilisateurs à accéder aux objets et services TADDM.

Cette configuration est prise en charge sur tous les types de serveur TADDM, sur tous les déploiements.

Procédure

Pour configurer pour Microsoft Active Directory, procédez comme suit :

Procédez de l'une des façons suivantes :

- Pour configurer Microsoft Active Directory à l'aide de LDAP, procédez comme suit :
  1. Configurez TADDM pour LDAP. Pour plus d'informations sur cette configuration, voir «Configuration pour LDAP», à la page 26.
  2. Vérifiez que lorsque vous utilisez Active Directory, la propriété **com.collation.security.auth.ldapFollowReferrals** est définie sur *true* dans le fichier `collation.properties`.
- Pour configurer Microsoft Active Directory à l'aide des référentiels fédérés WebSphere, procédez comme suit :
  1. Configurez TADDM pour les référentiels fédérés WebSphere. Pour plus d'informations sur la configuration de TADDM pour les référentiels fédérés WebSphere, voir «Configuration du serveur TADDM en vue de l'utilisation des référentiels fédérés WebSphere», à la page 28.
  2. Configurez les référentiels fédérés WebSphere pour Microsoft Active Directory. Pour plus d'informations sur la configuration des types d'entité pris en charge dans une configuration de référentiel fédéré, reportez-vous à la section **Configuration de types d'entités pris en charge dans une configuration de référentiel fédéré** dans le *centre de documentation de WebSphere Application Server*, http://www-01.ibm.com/support/knowledgecenter/SSAW57_6.1.0/com.ibm.websphere.nd.doc/info/ae/ae/twim_entitytypes.html.

Sécurisation des services Web TADDM

Vous pouvez configurer TADDM pour désactiver le port HTTP en définissant la propriété `com.ibm.cdb.secure.tomcat` (TADDM version 7.3.0) ou la propriété `com.ibm.cdb.secure.liberty` (TADDM version 7.3.0.1 ou ultérieure) dans `collation.properties` sur `true`. En outre, vous pouvez définir un protocole SSL plus sécurisé à l'aide de l'indicateur `com.ibm.cdb.http.ssl.protocol`.

La valeur par défaut des propriétés com.ibm.cdb.secure.tomcat et com.ibm.cdb.secure.liberty est false. Lorsque le port HTTP est désactivé, l'accès à TADDM ne peut se faire que par le port HTTPS (HTTP sur SSL), par exemple https://example.com:9431.

Limitation : Lorsque TADDM est installé sur le déploiement de serveurs de diffusion en continu et que les serveurs de reconnaissance et les serveurs de mémoire de stockage secondaire fonctionnent et sont en cours d'exécution, vous pouvez définir la propriété com.ibm.cdb.secure.tomcat ou com.ibm.cdb.secure.liberty sur true. Dans ce cas, le port HTTP est désactivé et vous pouvez utiliser TADDM en mode sécurisé. Toutefois, si vous souhaitez ajouter un serveur de reconnaissance ou un serveur de stockage secondaire à votre déploiement, vous devez temporairement activer le port HTTP, car le programme d'installation de TADDM ne prend pas en charge le protocole HTTPS. Pour temporairement désactiver le mode sécurisé, procédez comme suit :

1. Modifiez la valeur de la propriété com.ibm.cdb.secure.tomcat ou com.ibm.cdb.secure.liberty sur false.
2. Redémarrez le serveur TADDM.
3. Installez un nouveau serveur de reconnaissance ou serveur de stockage secondaire.
4. Modifiez la valeur de la propriété com.ibm.cdb.secure.tomcat ou com.ibm.cdb.secure.liberty sur true.
5. Redémarrez le serveur TADDM.

La valeur par défaut de la propriété com.ibm.cdb.http.ssl.protocol est TLS. Les valeurs sécurisées sont TLS, TLSv1.1 et TLSv1.2. Pour utiliser les protocoles les plus sécurisés TLSv1.1 et TLSv1.2, vous devez d'abord configurer votre navigateur Web pour leur prise en charge.

Installation de certificats SSL personnalisés à utiliser dans TADDM

Vous pouvez installer vos propres certificats SSL personnalisés et les utiliser avec TADDM.

Procédure

1. Créez une copie de sauvegarde des fichiers de clés suivants :
   - $COLLATION_HOME/etc/serverkeys
   - $COLLATION_HOME/etc/jssecacerts.cert
2. Accédez au répertoire $COLLATION_HOME/etc, ouvrez la ligne de commande et entrez les paramètres keytool et TADDM sslpassphrase avec les valeurs définies comme suit :
   - Système d'exploitation Linux :

     ```
     keytool=../external/jdk-Linux-x86_64/bin/keytool
     pass=XXXXXXXX30374
     ```

   - Système d'exploitation Windows :

     ```
     set keytool=..\external\jdk-Windows-i386-64\bin\keytool.exe
     set pass=XXXXXXXX30374
     ```

   La valeur du paramètre pass est la valeur de la propriété com.collation.sslpassphrase qui est spécifiée dans le fichier collation.properties.
3. Supprimez le certificat autosigné et la clé de TADDM à l'aide des commandes suivantes :

- Système d'exploitation Linux :

```
$keytool -delete -alias collation -noprompt -keystore jssecacerts.cert
-storepass $pass
$keytool -delete -alias collation -noprompt -keystore serverkeys -storepass
$pass
```

- Système d'exploitation Windows :

```
%keytool% -delete -alias collation -noprompt -keystore jssecacerts.cert
-storepass %pass%
%keytool% -delete -alias collation -noprompt -keystore serverkeys -storepass
%pass%
```

4. Générez la clé SSL avec le nom usuel (CN), la validité, l'algorithme et d'autres paramètres, et sauvegardez-la dans le fichier `serverkeys`. Par exemple, vous pouvez exécuter la commande suivante :
   - Système d'exploitation Linux :

```
$keytool -genkey -alias collation -keystore serverkeys -validity 3650
-keyAlg RSA -sigalg SHA256WithRSA -keypass $pass -storepass $pass -dname
"CN=John Public, OU=Engineering, OU=NA, o=Company, L=Manhattan,
S=New York, c=US"
```

   - Système d'exploitation Windows :

```
%keytool% -genkey -alias collation -keystore serverkeys -validity 3650
-keyAlg RSA -sigalg SHA256WithRSA -keypass %pass% -storepass %pass% -dname
"CN=John Public, OU=Engineering, OU=NA, o=Company, L=Manhattan,
S=New York, c=US"
```

5. Créez une autre copie de sauvegarde du fichier `serverkeys`, là où vous avez sauvegardé la clé SSL générée.
6. Générez la demande de signature de certificat (fichier CSR) à l'aide de la commande suivante :
   - Système d'exploitation Linux :

```
$keytool -certreq -alias collation -storepass $pass -file
/tmp/certreq.csr -keystore serverkeys
```

   - Système d'exploitation Windows :

```
%keytool% -certreq -alias collation -storepass %pass% -file
C:\temp\certreq.csr -keystore serverkeys
```

7. Utilisez le fichier CSR pour obtenir le certificat SSL de l'autorité de certification officielle. Sauvegardez le certificat sur votre serveur TADDM, par exemple dans le répertoire `tmp` sur le système d'exploitation Linux, ou dans le répertoire `C:\temp` sur le système d'exploitation Windows en tant que fichier `cert.crt`.
8. Importez le certificat généré dans TADDM, dans les fichiers `serverkeys` et `jssecacerts.cert`, à l'aide des commandes suivantes :

   Important : Pour le paramètre `-file`, spécifiez le chemin d'accès au fichier dans lequel vous avez sauvegardé le certificat SSL lors de l'étape précédente, par exemple `/tmp/cert.crt` sur le système d'exploitation Linux ou `C:\temp\cert.crt` sur le système d'exploitation Windows.
   - Système d'exploitation Linux :

```
$keytool -import -trustcacerts -alias collation -noprompt -keystore
serverkeys -storepass $pass -keypass $pass -file /tmp/cert.crt
$keytool -import -trustcacerts -alias collation -noprompt -keystore
jssecacerts.cert -storepass $pass -keypass $pass -file /tmp/cert.crt
```

   - Système d'exploitation Windows :

```
%keytool% -import -trustcacerts -alias collation -noprompt -keystore
serverkeys -storepass %pass% -keypass %pass% -file C:\temp\cert.crt
%keytool% -import -trustcacerts -alias collation -noprompt -keystore
jssecacerts.cert -storepass %pass% -keypass %pass% -file C:\temp\cert.crt
```

9. Redémarrez le serveur TADDM.

Que faire ensuite

Conservez les copies de sauvegarde du fichier `serverkeys` que vous avez généré à l'étape 4, et le fichier dans lequel vous avez sauvegardé le certificat SSL à l'étape 7. Vous aurez besoin de ces fichiers pour remplacer ou renouveler le certificat. Pour remplacer ou renouveler le certificat, procédez comme suit :

1. Répétez les étapes 2 et 3.
2. Restaurez le fichier `serverkeys`.
3. Répétez les étapes 8 et 9.

Gestion des serveurs TADDM

Avant de configurer TADDM pour la reconnaissance, vous devez savoir comment gérer les serveurs TADDM, ce qui implique de nombreuses tâches.

Vérification du statut du serveur TADDM

Vous pouvez utiliser la console d'administration ou la commande **`control`** pour vérifier le statut du serveur TADDM.

Utilisation de la console d'administration pour vérifier le statut

Pour utiliser la console d'administration pour vérifier le statut, ouvrez un navigateur Web et entrez l'URL et le numéro de port du système sur lequel vous avez installé le serveur TADDM. Exemple d'URL :

```
http://system.company.com:9430
```

La console d'administration apparaît et répertorie les composants du serveur TADDM et leur statut.

Utilisation de la commande `control` pour vérifier le statut

Pour utiliser la commande**`control`** pour vérifier le statut, procédez comme suit :

1. Connectez-vous en tant qu'utilisateur non superutilisateur défini lors du processus d'installation.
2. A l'invite de commande, accédez au répertoire dans lequel vous avez installé le serveur TADDM.
3. Exécutez l'une des commandes suivantes :
   - Pour les systèmes d'exploitation AIX, Linux et Linux sous System z.
     ```
     $COLLATION_HOME/bin/control status
     ```
   - Pour les systèmes d'exploitation Windows :
     ```
     %COLLATION_HOME%\bin\control.bat status
     ```

   Le résultat suivant s'affiche en fonction du déploiement et du type de serveur sur lequel TADDM s'exécute dans le déploiement respectif :

   déploiement de serveur de synchronisation

   serveur de synchronisation

   - TADDM 7.3.0 :
     ```
     DbInit: Started
     Tomcat: Started
     EcmdbCore: Started

     TADDM: Running
     ```
   - TADDM versions 7.3.0.1 et ultérieures :

```
DbInit: Started
Liberty : Démarré
EcmdbCore: Started

TADDM: Running
```

serveur de domaine

- TADDM 7.3.0 :

```
Discover: Started
DbInit: Started
Tomcat: Started
Topology: Started
DiscoverAdmin: Started
Proxy: Started
EventsCore: Started

TADDM: Running
```

- TADDM versions 7.3.0.1 et ultérieures :

```
Discover: Started
DbInit: Started
Liberty : Démarré
Topology: Started
DiscoverAdmin: Started
Proxy: Started
EventsCore: Started

TADDM: Running
```

déploiement de serveurs de diffusion en continu

serveur de stockage

- TADDM 7.3.0 :

```
TADDM: Starting
EtaddmCore: Started
DbInit: Started
Tomcat: Started

TADDM: Running
```

- TADDM versions 7.3.0.1 et ultérieures :

```
TADDM: Starting
EtaddmCore: Started
DbInit: Started
Liberty : Démarré

TADDM: Running
```

serveur de reconnaissance

- TADDM 7.3.0 :

```
Discover: Started
Tomcat: Started
DiscoverAdmin: Started
ProxyLite: Started
EventsCore: Started

TADDM: Running
```

- TADDM versions 7.3.0.1 et ultérieures :

```
Discover: Started
Liberty : Démarré
DiscoverAdmin: Started
ProxyLite: Started
EventsCore: Started

TADDM: Running
```

Démarrage du serveur TADDM

Si vous avez choisi l'option **Démarrer à l'initialisation**, le serveur TADDM démarre automatiquement à chaque initialisation du système.

Pourquoi et quand exécuter cette tâche

Important : Un serveur de base de données local ou distant doit être démarré et en cours d'exécution avant le lancement du serveur TADDM. Le serveur TADDM ne peut pas s'initialiser ou s'exécuter correctement si la base de données n'est pas disponible.

Procédure

Pour démarrer manuellement le serveur TADDM, procédez comme suit :

1. Ne vous connectez pas en tant que superutilisateur (défini lors de l'installation).
2. Ouvrez une fenêtre d'invite de commande.

   Remarque : Sur un système Windows Server 2008 avec le contrôle des comptes utilisateur activé, ouvrez la fenêtre d'invite de commande à l'aide des droits d'administrateur. Pour cela, vous pouvez cliquer à l'aide du bouton droit de la souris sur l'icône Invite de commande, puis sélectionnez **Exécuter en tant qu'administrateur**.
3. Allez au répertoire d'installation du serveur TADDM.
4. Pour exécuter le script de démarrage, utilisez l'une des commandes suivantes :
   - Pour les systèmes d'exploitation Linux, AIX et Linux sous System z :
     ```
     $COLLATION_HOME/bin/control start
     ```
   - Pour les systèmes d'exploitation Windows :
     ```
     %COLLATION_HOME%\bin\startServer.bat
     ```

   Au démarrage du serveur sur un système Windows, le message d'erreur de dépassement de délai suivant peut s'afficher : `Error 1053: The service did not respond to the start or control request in a timely fashion.` Cette erreur se produit car le serveur TADDM peut prendre plus de temps que la durée autorisée pour démarrer. Vous pouvez ignorer ce message ; le processus de démarrage se poursuit.

   Si vous avez installé le serveur TADDM avec des privilèges de superutilisateur, démarrez-le en exécutant le script suivant :
   ```
   /etc/init.d/collation start
   ```

Arrêt du serveur TADDM

Vous pouvez arrêter manuellement le serveur TADDM et les processus de reconnaissance associés.

Procédure

Pour arrêter manuellement le serveur TADDM, procédez comme suit :

1. Ne vous connectez pas en tant que superutilisateur (défini lors de l'installation).
2. Ouvrez une fenêtre d'invite de commande.

   Remarque : Sur un système Windows Server 2008 avec le contrôle des comptes utilisateur activé, ouvrez la fenêtre d'invite de commande à l'aide des droits

d'administrateur. Pour cela, vous pouvez cliquer à l'aide du bouton droit de la souris sur l'icône Invite de commande, puis sélectionnez **Exécuter en tant qu'administrateur**.

3. Allez au répertoire d'installation du serveur TADDM.
4. Utilisez l'une des commandes suivantes pour exécuter le script d'arrêt :
   - Pour les systèmes d'exploitation Linux, AIX et Linux sous System z :
     ```
     $COLLATION_HOME/bin/control stop
     ```
   - Pour les systèmes d'exploitation Windows :
     ```
     %COLLATION_HOME%\bin\stopServer.bat
     ```

   Si vous avez installé le serveur TADDM avec des privilèges de superutilisateur, arrêtez-le en exécutant le script suivant :
   ```
   /etc/init.d/collation stop
   ```

Que faire ensuite

Certains détecteurs exécutent leur propre machine virtuelle Java spéciale. Lors d'une reconnaissance, si vous utilisez le script control (`./control stop`) pour arrêter TADDM, vous devez éventuellement arrêter manuellement ces autres machines virtuelles Java, appelées ancres locales. Si vous n'arrêtez pas les ancres locales, un comportement imprévu peut se produire. Par exemple, il peut s'agir de performances dégradées au niveau de certaines reconnaissances.

Pour vérifier que le processus pour l'ancre locale n'est plus en cours d'exécution, entrez la commande suivante :

```
% ps -ef |grep -i anchor
```

Cette commande identifie les processus d'ancre locale en cours d'exécution. Le résultat ressemble à l'exemple de code suivant :

```
 coll
23751  0.0  0.0  6136  428 ?   S  Jun02   0:00 /bin/sh
    local-anchor.sh 8494 <more information here>
```

Si un processus est en cours d'exécution, arrêtez-le en lançant la commande suivante :

```
-  % kill -9 23751
```

Une fois la commande exécutée, vérifiez que le processus s'est arrêté avec la commande suivante :

```
 % ps -ef |grep -i anchor
```

Sauvegarde de données

Sauvegardez régulièrement vos données afin de pouvoir effectuer une restauration en cas de panne système.

Avant de commencer

Avant de sauvegarder les données, arrêtez le serveur TADDM.

Procédure

Pour sauvegarder des fichiers sur le serveur TADDM, procédez comme suit :

Sauvegardez tous les fichiers dans le répertoire dans lequel vous avez installé le serveur TADDM.

- Pour les systèmes d'exploitation Linux, AIX et Linux sur System z, le chemin d'accès par défaut au répertoire est `/opt/IBM`.
- Pour les systèmes d'exploitation Windows, le chemin d'accès par défaut au répertoire est `C:\opt\IBM`.

Que faire ensuite

Pour sauvegarder les fichiers de base de données, utilisez la documentation du fournisseur de base de données.

Restauration des données

Après un arrêt anormal du système, vous pouvez restaurer la configuration, les données et les fichiers de base de données. Vous pouvez ensuite reprendre le fonctionnement à partir de la dernière sauvegarde effectuée avant l'arrêt.

Procédure

Pour restaurer les données depuis un support de sauvegarde, procédez comme suit :

1. Procédez de l'une des façons suivantes :
   - Restaurez le répertoire `/opt/IBM` et redémarrez TADDM.
   - Restaurez le répertoire `C:\opt\IBM` et redémarrez TADDM.
2. Localisez la copie de sauvegarde des fichiers de données.
3. Ouvrez une fenêtre d'invite de commande.
4. Accédez au répertoire d'installation du serveur TADDM.
5. Copiez la copie de sauvegarde des fichiers de données dans le répertoire d'installation.
6. Fermez la fenêtre d'invite de commande.
7. Démarrez le serveur TADDM.

Que faire ensuite

Si la base de données est affectée par l'arrêt du système, restaurez les fichiers de base de données à l'aide de la documentation fournie avec la base de données.

Copie des portées de reconnaissance, des profils et des modèles de serveur personnalisé entre les serveurs TADDM

Vous pouvez utiliser la commande **`DATAMOVER.sh|bat`** pour copier des portées de reconnaissance, des profils de reconnaissance et des modèles de serveur personnalisé entre les serveurs TADDM.

Vous pouvez exporter des portées de reconnaissance, des profils et des modèles de serveur personnalisé (toutes les entités) ou définir les entités à exporter. Vous pouvez alors importer la ou les entités dans le serveur de destination.

Restriction : Pour préserver l'intégrité des données, vous devez déplacer les données entre les serveurs TADDM de même version.

Pour copier des entités entre des serveurs TADDM, procédez comme suit :

1. Exécutez la commande suivante sur le serveur source pour exporter la ou les entités requises vers un fichier :

   ```
   datamover.sh|bat -u utilisateur -p mot_de_passe -a action [-t type ] [-f nom_fichier]
   ```

   où :

   utilisateur
   Nom d'utilisateur TADDM.

   mot_de_passe
   Mot de passe de l'utilisateur TADDM.

   action
   Indiquez l'une des actions suivantes : `import`, `export` ou `help`.

   Facultatif : *type*
   Indiquez l'une des actions suivantes : `all`, `scope`, `profile` ou `template`. La valeur par défaut est `all`.

   Facultatif : *nom_fichier*
   Indiquez un nom de fichier. La valeur par défaut est `datamover.xml`.

   Les profils de reconnaissance par défaut ne sont pas exportés, mais tous les modèles de serveur personnalisés, profils créés par les utilisateurs et portées peuvent être exportés.

   Après l'exécution de la commande, les informations sur les entités exportées sont affichées. Par exemple, si le fichier de sortie est `exporthost.xml`, les informations suivantes sont fournies :

   ```
   Exported 6 scopes
   Exported 1 profiles
   Exported 57 templates
   ```

2. Copiez le ou les fichiers sur le serveur de destination, exécutez la commande **DATAMOVER.sh|bat** et importez la ou les entités.

   Les règles suivantes s'appliquent lors de l'importation des entités :

   - Si une portée ou un profil de même nom existe sur le serveur, la portée ou le profil importé est renommé. Le nouveau nom est le suivant : *nom*_TADDM.
   - Si un modèle de même nom existe sur le serveur, le modèle est fusionné avec le modèle existant.

Déploiement de la console de gestion de reconnaissance

Une fois que vous avez confirmé que le serveur TADDM est disponible, vous pouvez déployer la console de gestion de reconnaissance.

Procédure

Pour déployer la console de gestion de reconnaissance, procédez comme suit :

1. Indiquez aux utilisateurs l'adresse URL (y compris le numéro de port) du système sur lequel vous avez installé le serveur TADDM.

   Par exemple, vous pouvez leur fournir une adresse URL semblable à celle-ci :

   ```
   http://system.company.com:9430
   ```

2. Attribuez un nom d'utilisateur et un mot de passe aux utilisateurs.
3. Indiquez s'ils doivent utiliser la couche Secure Sockets Layer (SSL).

   S'ils doivent l'utiliser, informez les utilisateurs qu'ils doivent sauvegarder un fichier de clés certifiées pour le serveur TADDM en suivant les instructions de la page d'installation et de démarrage de la console de gestion de reconnaissance. Pour plus d'informations, voi le *Guide d'installation* de TADDM.

Important : Nous vous recommandons d'utiliser le protocole SSL pour toutes les communications entre la console de gestion de reconnaissance et le serveur TADDM.

4. Les utilisateurs doivent disposer d'une version prise en charge de l'environnement d'exécution Java sur le système utilisé pour afficher la console de gestion de reconnaissance. Pour plus d'informations sur les prérequis des clients, voi le *Guide d'installation* de TADDM.
5. Fournissez aux utilisateurs le *Guide d'utilisation* de TADDM pour qu'ils disposent d'informations sur le démarrage de la console de gestion de reconnaissance.

Configuration de la communication TADDM

Pour établir une communication TADDM, vous devez configurer tous les services, connexions et pare-feux nécessaires.

Services TADDM

La connectivité TADDM peut se diviser en trois zones :

Connectivité publique
La connectivité publique couvre la connectivité du réseau effectuée en dehors de l'infrastructure TADDM. Par exemple, le portail de gestion de données, la console de gestion de reconnaissance ou des clients d'API se connectant au serveur TADDM. Il s'agit du niveau de connectivité le plus élevé.

Connectivité inter-serveur
La connectivité inter-serveur couvre la connectivité du réseau entre des éléments de l'infrastructure centrale de TADDM, à savoir les serveurs de reconnaissance et les serveurs de stockage. Il s'agit du niveau moyen de connectivité.

Connectivité locale
La connectivité locale couvre la connectivité du réseau entre les services locaux sur une machine. Il s'agit du niveau de connectivité le plus bas.

Vous pouvez configurer la connectivité pour chaque service lors de la phase d'installation, ou par la suite en modifiant les propriétés de configuration dans le fichier de configuration `collation.properties`.

Interface par défaut des services
Pour configure l'interface d'écoute par défaut des services, changez la propriété `com.ibm.cdb.global.hostname` dans le fichier `collation.properties`.

Tableau 2. Paramètres de l'interface par défaut des services

Nom	Propriété de configuration	Interface par défaut
Hôte de services globaux	com.ibm.cdb.global.hostname	0.0.0.0

Interface d'écoute qui dépend du type de communication
Pour configurer les interfaces d'écoute à part pour les services de chaque zone de connectivité, changez la propriété appropriée dans le fichier `collation.properties`.

Tableau 3. Paramètres de l'interface par défaut des services

Nom	Propriété de configuration	Interface par défaut
Hôte des services de connectivité publique	com.ibm.cdb.public.hostname	Défini par com.ibm.cdb.global.hostname
Hôte des services de connectivité inter-serveur	com.ibm.cdb.interserver.hostname	Défini par com.ibm.cdb.global.hostname
Hôte des services de connectivité locale	com.ibm.cdb.local.hostname	127.0.0.1

Remarque : Si aucune interface n'est définie ou qu'une interface a la valeur `0.0.0.0.`, une interface réseau externe locale doit être ouverte pour communiquer avec elle-même. Si une interface est spécifiée, elle doit être ouverte pour la communication avec elle-même.

Interface d'écoute pour des services spécifiques

Vous pouvez configurer un port TCP distinct pour chaque service lors de la phase d'installation, ou par la suite en modifiant la propriété correspondante dans le fichier`collation.properties`.

Configuration de l'interface de service

Pour configurer une interface d'écoute spécifique pour chaque service, modifiez la propriété appropriée avec le suffixe `host` dans le fichier `collation.properties`.

Exemple pour le service TopologyManager :

```
com.ibm.cdb.service.TopologyManager.host=192.168.1.5
```

Remarque : Cette convention de dénomination ne s'applique pas aux registres de services publics ou inter-serveur.

Configuration du port de service

Pour configurer un port d'écoute spécifique pour chaque service, modifiez la propriété appropriée avec le suffixe `port` dans le fichier `collation.properties`.

L'exemple suivant concerne le service TopologyManager :

```
com.ibm.cdb.service.TopologyManager.port=9550
```

Configuration du service SSL

Pour configurer un port ou une interface d'écoute pour chaque service SSL, modifiez la propriété appropriée avec l'infixe `secure` dans le fichier `collation.properties`.

L'exemple suivant concerne le service SecureApiServer :

- `com.ibm.cdb.service.SecureApiServer.secure.host=192.168.1.5`
- `com.ibm.cdb.service.SecureApiServer.secure.port=9531`

Configuration de l'interface pour le portail Web (HTTP et HTTPS)

Pour configurer une interface d'écoute pour un portail Web (HTTP et HTTPS), modifiez la propriété `com.ibm.cdb.service.web.host` dans le fichier `collation.properties`.

Remarque : L'hôte HTTP ou HTTPS est configuré en modifiant une propriété par rapport aux autres services.

Connexions de base de données

Pour configurer une connexion de base de données spécifique, modifiez les propriétés `com.collation.db.port` et `com.collation.db.server` dans le fichier `collation.properties`.

Par exemple :

- `com.collation.db.port=65432`
- `com.collation.db.server=9.156.47.156`

Connexions DNS

Pour utiliser des noms de domaines complets (FQDN) pour les communications, vérifiez que l'hôte sollicité peut résoudre ces noms à partir du service DNS.

Connexions du détecteur

La configuration des ports utilisés par le détecteur ping et le détecteur de port afin d'établir des connexions est décrite dans les documentations respectives. Vérifiez que les ports aux services à reconnaître sont ouverts.

Tableau 4. Ports par défaut des détecteurs Ping et de port

Nom du port	Port par défaut	Protocole
SSH	22	TCP
Telnet	23	TCP
DNS	53	TCP
WMI	135	TCP
Fix Pack 2 PowerShell	5985, 5986	TCP
LDAP	389	TCP
SMB	445	TCP
Oracle	1521	TCP
CiscoWorks	1741	TCP

Connexions d'ancrage

TADDM peut se connecter à un autre serveur à l'aide de l'un des types de connexion suivants : *ssh* ou *direct*. Pour configurer un type de connexion d'ancrage spécifique, remplacez la valeur de la propriété `com.collation.discover.anchor.connectType` dans le fichier `collation.properties` par *ssh* et *direct*.

Pour configurer un type de connexion d'ancrage spécifique pour une adresse donnée, modifiez la propriété `com.collation.discover.anchor.connectType` avec l'adresse IP comme suffixe dans le fichier `collation.properties`, par exemple :

`com.collation.discover.anchor.connectType.1.2.3.4=`*`direct`*

Par ailleurs, le port 8497 est défini par défaut pour la connexion à un serveur d'ancrage. Vous pouvez configurer ce port à l'aide de la console de gestion de reconnaissance.

- En mode *ssh*, ouvrez les ports pour la communication SSH sur une interface publique accessible depuis le serveur TADDM et depuis le port de connexion d'ancrage dans une interface de bouclage sur la machine hébergeant le serveur d'ancrage.
- En mode *direct*, ouvrez les ports pour la communication SSH et la connexion d'ancrage dans une interface publique accessible depuis le serveur TADDM.

Connexions de passerelle

TADDM peut se connecter à un serveur de passerelle à l'aide d'une connexion SSH.

Sur la passerelle, le port SSH de l'hôte doit être ouvert pour la communication dans une interface publique accessible depuis le serveur TADDM.

Résolution du nom d'hôte d'un serveur en nom de domaine complet

Pour que la communication fonctionne entre les serveurs, le serveur hôte doit pouvoir résoudre son nom d'hôte en un nom de domaine complet (FQDN) à l'aide de la bibliothèque du programme de résolution du système d'exploitation. L'une des conditions suivantes doit être remplie :

- Dans l'ordre de recherche de la résolution des hôtes du système d'exploitation, DNS doit précéder les fichiers locaux. Pour configurer ce paramètre, reportez-vous à la documentation de votre système d'exploitation.
- Dans le fichier hôte, le nom de domaine complet du serveur TADDM doit précéder le nom abrégé.

Si aucune de ces conditions ne peut être remplie, vous pouvez affecter à la propriété `com.collation.serverID` du fichier `collation.properties` l'adresse IP ou le nom d'hôte du serveur TADDM. En outre, vérifiez que l'ID serveur dans Serveur de synchronisation / Enterprise Server > Portail de gestion de données > Gestion du domaine > Nom d'hôte du domaine possède la même valeur.

Ports éphémères

La communication TADDM propose l'utilisation des ports éphémères. Ces ports temporaires sont propres à un système d'exploitation. Chaque système d'exploitation dispose d'une plage définie de numéros de port à partir desquels des ports spécifiques sont sélectionnés de manière aléatoire. TADDM ne définit pas ces ports. Pour plus d'informations sur la plage de ports, la configuration nécessaire et plus encore, consultez la documentation du système d'exploitation que vous utilisez.

Configuration des pare-feux

Pour établir une communication de TADDM, vous devez configurer les pare-feux nécessaires. Les détails de cette tâche changent selon si vous avez configuré un

déploiement de serveur de domaine, un déploiement de serveur de flux ou un déploiement de serveur de synchronisation.

Les informations sur la configuration de pare-feux sont présentées dans des tableaux. Chaque tableau inclut la direction de la communication. Sur la machine cible, le port du service cible doit être ouvert sur le pare-feu comme source des connexions sortantes et comme destination des connexions entrantes. Sur la machine source, le port du service cible doit être ouvert sur le pare-feu comme destination des connexions sortantes et comme source des connexions entrantes.

Important : Les services de niveau supérieur doivent aussi être disponibles depuis des clients de niveau inférieur. Par exemple, les services publics doivent aussi être ouverts pour la connectivité inter-serveur.

Quand la direction indiquée dans le tableau est le bouclage, toutes les communications doivent être ouvertes dans cette interface. Quand vous modifiez la configuration de l'un des ports par défaut, vérifiez que vous ouvrez les ports appropriés pour la configuration de votre environnement.

Configuration de pare-feux dans un déploiement de serveur de domaine

Vous devez configurer les pare-feux dans un déploiement de serveur de domaine pour que des ports spécifiques soient ouverts pour les communications.

La figure suivante montre la communication TADDM dans un déploiement de serveur de domaine.

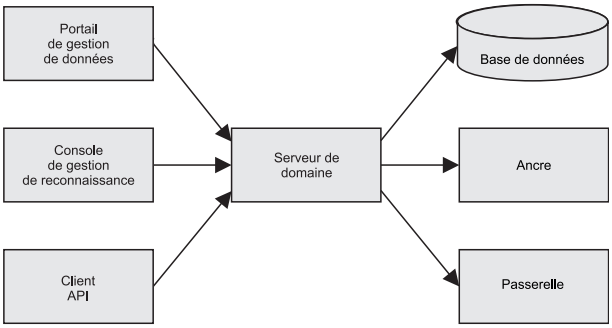

Figure 1. Communication TADDM dans un déploiement de serveur de domaine

Services de connectivité :

Pour un déploiement de serveur de domaine, vous pouvez configurer des services de connectivité publique, inter-serveur et locale.

Services de connectivité publique

Le tableau suivant montre les paramètres d'hôte par défaut pour les services de connectivité publique du serveur de domaine.

Tableau 5. Paramètres de l'hôte par défaut pour les services de connectivité publique du serveur de domaine

Nom	Propriété de configuration	Interface par défaut
Hôte de service public	com.ibm.cdb.public.hostname	Défini par com.ibm.cdb.global.hostname

Le tableau suivant montre les paramètres de port par défaut pour les services de connectivité publique du serveur de domaine.

Tableau 6. Paramètres de port par défaut pour les services de connectivité publique du serveur de domaine

Nom	Propriété de configuration	Protocole	Port par défaut
Port du serveur d'API	com.ibm.cdb.service.ApiServer.port	TCP	9530
Port du serveur d'API sécurisé	com.ibm.cdb.service.SecureApiServer.secure.port	TCP	9531
Port HTTP (sans SSL)	com.ibm.cdb.service.web.port	TCP	9430
Port HTTPS (avec SSL)	com.ibm.cdb.service.web.secure.port	TCP	9431
Port de communication du serveur d'interface graphique	com.ibm.cdb.service.ClientProxyServer.port	TCP	9435
Port de communication SSL du serveur d'interface graphique	com.ibm.cdb.service.SecureClientProxyServer.secure.port	TCP	9434
Port du registre de services publics	com.ibm.cdb.service.registry.public.port	TCP	9433

Services de connectivité locale

Les ports des services locaux ne sont pas définis de façon explicite. Tous les ports doivent être ouverts dans l'interface définie pour les services locaux. L'interface par défaut est celle de bouclage.

Le tableau suivant montre les paramètres de l'hôte par défaut pour les services de connectivité locale du serveur de domaine.

Tableau 7. Paramètres de l'hôte par défaut pour les services de connectivité locale du serveur de domaine

Nom	Propriété de configuration	Interface par défaut
Hôte de service local	com.ibm.cdb.local.hostname	127.0.0.1

Configuration de la communication dans le déploiement de serveur de domaine :

Pour établir une communication réussie dans le déploiement de serveur de domaine, configurez des services de connectivité publics et locaux.

Les tableaux qui suivent présentent les éléments que vous pouvez connecter dans le déploiement de serveur de domaine et les ports que vous devez ouvrir pour que la communication s'établisse.

Communication entre le serveur de base de données et le serveur de domaine

Tableau 8. Communication entre le serveur de base de données et le serveur de domaine.

Elément A	Port	Direction	Elément B	Propriété de configuration
Serveur de base de données	5000	←	Serveur de domaine	

Communication entre le portail de gestion de reconnaissance, les clients d'API et le portail Web, et entre les clients de portail de gestion de données et le serveur de domaine

Tableau 9. Communication entre le portail de gestion de reconnaissance, les clients d'API et le portail Web, et entre les clients de portail de gestion de données et le serveur de domaine.

Elément A	Port	Direction	Elément B	Propriété de configuration
Portail de gestion de reconnaissance	9433	→	Serveur de domaine - Registre de services publics	com.ibm.cdb.service.registry.public.port
	9435	→	Serveur de domaine - Serveur proxy client	com.ibm.cdb.service.ClientProxyServer.port
	9434	→	Serveur de domaine - Serveur proxy client sécurisé	com.ibm.cdb.service.SecureClientProxyServer.secure.port
Clients d'API	9433	→	Serveur de domaine - Registre de services publics	com.ibm.cdb.service.registry.public.port
	9530	→	Serveur de domaine - Serveur d'API	com.ibm.cdb.service.ApiServer.port
	9531	→	Serveur de domaine - Serveur d'API sécurisé	com.ibm.cdb.service.SecureApiServer.secure.port
Clients de portail Web et de portail de gestion de données	9430	→	Serveur de domaine - Web	com.ibm.cdb.service.web.port
	9431	→	Serveur de domaine - Web sécurisé	com.ibm.cdb.service.web.secure.port

Communication entre l'ancre et la passerelle, et le serveur de domaine

Tableau 10. Communication entre l'ancre et la passerelle, et le serveur de domaine.

Elément A	Port	Direction	Elément B	Propriété de configuration
Ancre (en mode ssh) - SSH	22	←	Serveur de domaine (en mode ssh)	
Ancre (en mode direct) - SSH		←	Serveur de domaine (en mode direct)	
Ancre (en mode ssh) - Acheminement du tunnel SSH	8497	↔	Serveur de domaine (en mode ssh)	
Ancre (en mode direct) - Direct		←	Serveur de domaine (en mode direct)	
Passerelle - SSH	22	←	Serveur de domaine	

Communication locale

Tableau 11. Configuration des communications pour la connectivité locale pour un serveur de domaine.

Communication locale	Direction	Propriété de configuration
Serveur de domaine - Registre de services locaux	⟷	com.ibm.cdb.local.hostname
Serveur de domaine - Services locaux		
Serveur de domaine - 127.0.0.1		

Configuration de pare-feux dans un déploiement de serveur de flux

Vous devez configurer les pare-feux dans un déploiement de serveur de flux afin que des ports spécifiques soient ouverts pour les communications.

La figure suivante montre la communication TADDM dans un déploiement de serveur de flux.

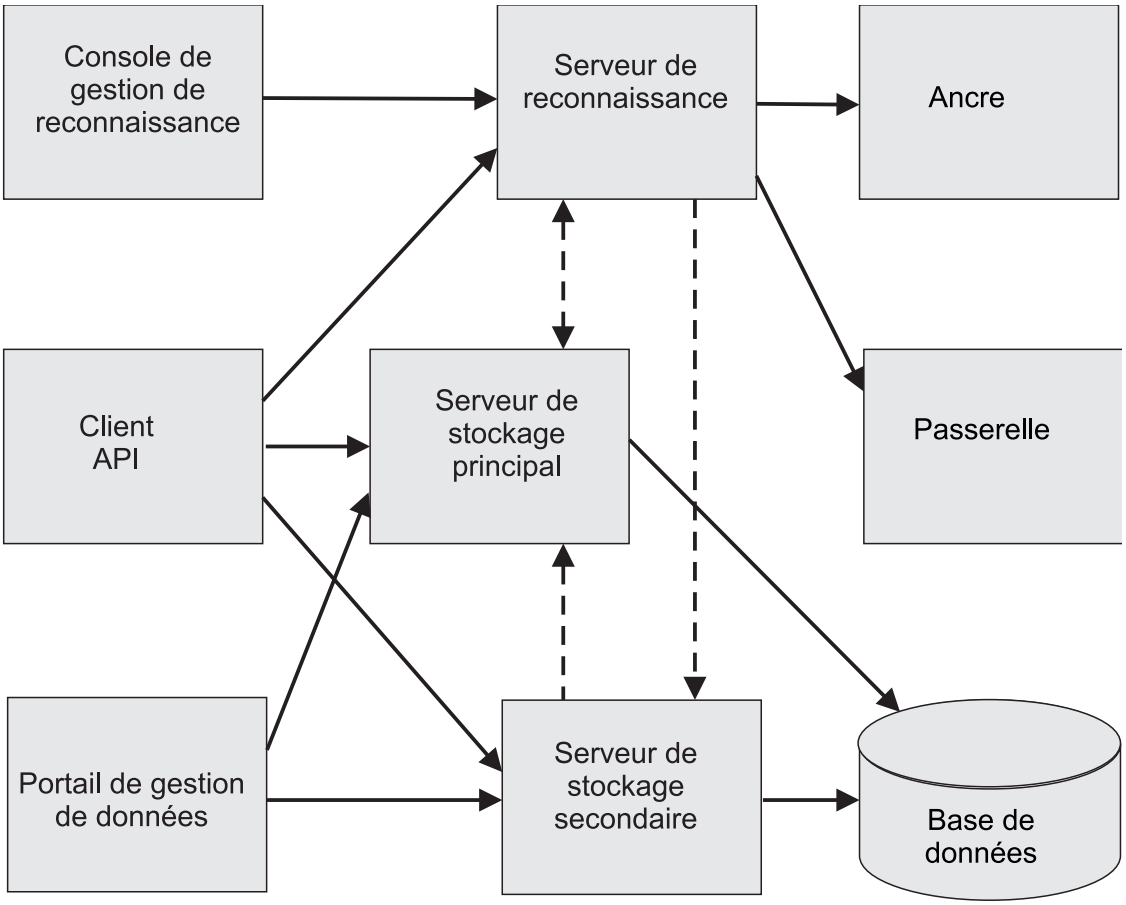

Figure 2. Communication TADDM dans un déploiement de serveur de flux

Services de connectivité :

Pour un déploiement de serveur de flux, vous pouvez configurer des services de connectivité publique, inter-serveur et locale.

Important : Les ports par défaut utilisés pour les propriétés décrites dans la suite de cette section s'appliquent uniquement aux propriétés répertoriées dans le fichier `collation.properties`. Si une propriété n'est pas codée ou figure en commentaire

dans le fichier `collation.properties`, elle prend par défaut la valeur d'un port choisi de manière aléatoire. En particulier, assurez-vous que la propriété `com.ibm.cdb.service.RegistriesURLProvider.port` figure dans le fichier `collation.properties` pour que le démarrage du serveur aboutisse.

Services de connectivité publique

Le tableau suivant montre les paramètres d'hôte par défaut pour les services de connectivité publique de serveur de stockage principal, de serveur de stockage secondaire et de serveur de reconnaissance.

Tableau 12. Paramètres d'hôte par défaut pour les services de connectivité publique de serveur de stockage principal, de serveur de stockage secondaire et de serveur de reconnaissance

Nom	Propriété de configuration	Interface par défaut
Hôte de service public	com.ibm.cdb.public.hostname	Défini par com.ibm.cdb.global.hostname

Le tableau suivant montre les paramètres de port par défaut pour les services de connectivité publique de serveur de stockage principal, de serveur de stockage secondaire et de serveur de reconnaissance.

Tableau 13. Paramètres de port par défaut pour les services de connectivité publique de serveur de stockage principal, de serveur de stockage secondaire et de serveur de reconnaissance

Nom	Propriété de configuration	Protocole	Port par défaut
Port du serveur d'API	com.ibm.cdb.service.ApiServer.port	TCP	9530
Port du serveur d'API sécurisé	com.ibm.cdb.service.SecureApiServer.secure.port	TCP	9531
Port HTTP (sans SSL)	com.ibm.cdb.service.web.port	TCP	9430
Port HTTPS (avec SSL)	com.ibm.cdb.service.web.secure.port	TCP	9431
Port de communication du serveur d'interface graphique	com.ibm.cdb.service.ClientProxyServer.port	TCP	9435
Port de communication SSL du serveur d'interface graphique	com.ibm.cdb.service.SecureClientProxyServer.secure.port	TCP	9434
Port du registre de services publics	com.ibm.cdb.service.registry.public.port	TCP	9433

Services de connectivité inter-serveur

Le tableau suivant montre les paramètres d'hôte par défaut pour les services de connectivité inter-serveur de serveur de stockage principal et de serveur de stockage secondaire.

Tableau 14. Paramètres d'hôte par défaut pour les services de connectivité inter-serveur de serveur de stockage principal et de serveur de stockage secondaire

Nom	Propriété de configuration	Interface par défaut
Hôte de service inter-serveur	com.ibm.cdb.interserver.hostname	Défini par com.ibm.cdb.global.hostname

Le tableau suivant montre les paramètres de port par défaut pour les services de connectivité inter-serveur de serveur de stockage principal.

Tableau 15. Paramètres de port par défaut pour les services de connectivité inter-serveur de serveur de stockage principal

Nom	Propriété de configuration	Protocole	Port par défaut
Port du gestionnaire de topologie	com.ibm.cdb.service.TopologyManager.port	TCP	9550
Port du gestionnaire de sécurité	com.ibm.cdb.service.SecurityManager.port	TCP	9540
Port du fournisseur d'URL de registres	com.ibm.cdb.service.RegistriesURLProvider.port	TCP	9560
Port du registre de services inter-serveur	com.ibm.cdb.service.registry.interserver.port	TCP	4160

Le tableau suivant montre les paramètres de port par défaut pour les services de connectivité inter-serveur de serveur de stockage secondaire.

Tableau 16. Paramètres de port par défaut pour les services de connectivité inter-serveur de serveur de stockage secondaire

Nom	Propriété de configuration	Protocole	Port par défaut
Port du gestionnaire de topologie	com.ibm.cdb.service.TopologyManager.port	TCP	9550
Port du fournisseur d'URL de registres	com.ibm.cdb.service.RegistriesURLProvider.port	TCP	9560
Port du registre de services inter-serveur	com.ibm.cdb.service.registry.interserver.port	TCP	4160

Services de connectivité locale

Les ports des services locaux ne sont pas définis de façon explicite. Tous les ports doivent être ouverts dans l'interface définie pour les services locaux. L'interface par défaut est celle de bouclage.

Le tableau suivant montre les paramètres d'hôte par défaut pour les services de connectivité locale de serveur de stockage principal, de serveur de stockage secondaire et de serveur de reconnaissance.

Tableau 17. Paramètres d'hôte par défaut pour les services de connectivité locale de serveur de stockage principal, de serveur de stockage secondaire et de serveur de reconnaissance

Nom	Propriété de configuration	Interface par défaut
Hôte du service de zone de connectivité locale	com.ibm.cdb.local.hostname	127.0.0.1

Configuration de la communication dans le déploiement de serveur de diffusion en continu :

Pour établir une communication réussie dans le déploiement de serveur de diffusion en continu, configurez des services de connectivité publics, inter-serveur et locaux.

Les tableaux qui suivent présentent les éléments que vous pouvez connecter dans le déploiement de serveur de diffusion en continu et les ports que vous devez ouvrir pour que la communication s'établisse.

Communication inter-serveur

Tableau 18. Configuration de la communication de connectivité inter-serveur dans le déploiement de serveur de diffusion en continu.

Elément A	Port	Direction	Elément B	Propriété de configuration	Prise en charge de TLS
Serveur de reconnaissance			**Serveur de stockage principal**		
	9433	→	Serveur de stockage principal	com.ibm.cdb.service.registry.public.port	Oui
	4160	→	Serveur de stockage principal - Registre de services inter-serveur	com.ibm.cdb.service.registry.interserver.port	Non
	9560	→	Serveur de stockage principal - Registres de registres	com.ibm.cdb.service.RegistriesURLProvider.port	Oui
	9540	→	Serveur de stockage principal - Gestionnaire de sécurité	com.ibm.cdb.service.SecurityManager.port	Oui
	9550	→	Serveur de stockage principal - Gestionnaire de topologie	com.ibm.cdb.service.TopologyManager.port	Oui
	9430	←	Serveur de stockage principal - Web	com.ibm.cdb.service.web.port	Non
Serveur de reconnaissance			**Serveur de stockage secondaire**		
	4160	→	Serveur de stockage secondaire - Registre de services inter-serveur	com.ibm.cdb.service.registry.interserver.port	Non
	9560	→	Serveur de stockage secondaire - Fournisseur d'URL de registres	com.ibm.cdb.service.RegistriesURLProvider.port	Oui
	9550	→	Serveur de stockage secondaire - Gestionnaire de topologie	com.ibm.cdb.service.TopologyManager.port	Oui

Tableau 18. Configuration de la communication de connectivité inter-serveur dans le déploiement de serveur de diffusion en continu. (suite)

Elément A	Port	Direction	Elément B	Propriété de configuration	Prise en charge de TLS
Serveur de stockage secondaire			**Serveur de stockage principal**		
	4160	→	Serveur de stockage principal - Registre de services inter-serveur	com.ibm.cdb. service.registry. interserver.port	Non
	9560	→	Serveur de stockage principal - Registres de registres	com.ibm.cdb. service.Registries URLProvider.port	Oui
	9540	→	Serveur de stockage principal - Gestionnaire de sécurité	com.ibm.cdb. service.Security Manager.port	Oui
	9550	→	Serveur de stockage principal - Gestionnaire de topologie	com.ibm.cdb. service.Topology Manager.port	Oui
Serveur de base de données	5000	←	**Serveur de stockage principal**		Non
Serveur de base de données	5000	←	**Serveur de stockage secondaire**		Non

Communication entre le portail de gestion de reconnaissance, les clients d'API et le portail Web, et entre les clients de portail de gestion de données et les serveurs TADDM

Tableau 19. Communication entre le portail de gestion de reconnaissance, les clients d'API et le portail Web, et entre les clients de portail de gestion de données et les serveurs TADDM.

Elément A	Port	Direction	Elément B	Propriété de configuration	Prise en charge de TLS
Portail de gestion de reconnaissance	9433	→	Serveur de reconnaissance - Registre de services publics	com.ibm.cdb.service. registry.public.port	Oui
	9435	→	Serveur de reconnaissance - Serveur proxy client	com.ibm.cdb.service. ClientProxyServer.port	Non
	9434	→	Serveur de reconnaissance - Serveur proxy client sécurisé	com.ibm.cdb.service. SecureClientProxy Server.secure.port	Oui

Tableau 19. Communication entre le portail de gestion de reconnaissance, les clients d'API et le portail Web, et entre les clients de portail de gestion de données et les serveurs TADDM. (suite)

Elément A	Port	Direction	Elément B	Propriété de configuration	Prise en charge de TLS
Clients d'API	9433	→	• Serveur de reconnaissance - Registre de services publics • Serveur de stockage principal - Registre de services publics • Serveur de stockage secondaire - Registre de services publics	com.ibm.cdb.service.registry.public.port	Oui
	9530	→	• Serveur de reconnaissance - Serveur d'API • Serveur de stockage principal - Serveur d'API • Serv	com.ibm.cdb.service.ApiServer.port	Non
	9531	→	• Serveur de reconnaissance - Serveur d'API sécurisé • Serveur de stockage principal - Serveur d'API sécurisé • Serveur de stockage secondaire - Serveur d'API sécurisé	com.ibm.cdb.service.SecureApiServer.secure.port	Oui

Tableau 19. Communication entre le portail de gestion de reconnaissance, les clients d'API et le portail Web, et entre les clients de portail de gestion de données et les serveurs TADDM. (suite)

Elément A	Port	Direction	Elément B	Propriété de configuration	Prise en charge de TLS
Clients de portail Web et de portail de gestion de données	9430	→	• Serveur de reconnaissance - Web • Serveur de stockage principal - Web • Serveur de stockage secondaire - Web	com.ibm.cdb.service.web.port	Non
	9431	→	• Serveur de reconnaissance - Web sécurisé • Serveur de stockage principal - Web sécurisé • Serveur de stockage secondaire - Web sécurisé	com.ibm.cdb.service.web.secure.port	Oui

Communication entre l'ancre et la passerelle, et le serveur de reconnaissance

Tableau 20. Communication entre l'ancre et la passerelle, et le serveur de reconnaissance.

Elément A	Port	Direction	Elément B	Propriété de configuration
Ancre (en mode ssh) - SSH	22	←	Serveur de reconnaissance (en mode ssh)	
Ancre (en mode direct) - SSH		←	Serveur de reconnaissance (en mode direct)	
Ancre (en mode ssh) - Acheminement du tunnel SSH	8497	↔	Serveur de reconnaissance (en mode ssh)	
Ancre (en mode direct) - Direct		←	Serveur de reconnaissance (en mode direct)	
Passerelle - SSH	22	←	Serveur de reconnaissance	

Communication locale

Tableau 21. Configuration de la communication de connectivité locale dans le déploiement de serveur de diffusion en continu.

Communication locale	Direction	Propriété de configuration
Serveur de reconnaissance		

Tableau 21. Configuration de la communication de connectivité locale dans le déploiement de serveur de diffusion en continu. (suite)

Communication locale	Direction	Propriété de configuration
Serveur de reconnaissance - Registre de services locaux	⟷	com.ibm.cdb.local.hostname
Serveur de reconnaissance - Services locaux		
Serveur de reconnaissance - 127.0.0.1		
Serveur de stockage principal		
Serveur de stockage principal - Registre de services locaux	⟷	com.ibm.cdb.local.hostname
Serveur de stockage principal - Services locaux		
Serveur de stockage principal - 127.0.0.1		
Serveur de stockage secondaire		
Serveur de stockage secondaire - Registre de services locaux	⟷	com.ibm.cdb.local.hostname
Serveur de stockage secondaire - Services locaux		
Serveur de stockage secondaire - 127.0.0.1		

Configuration de pare-feux dans un déploiement de serveur de synchronisation

Vous devez configurer les pare-feux dans un déploiement de serveur de synchronisation pour que des ports spécifiques soient ouverts pour les communications.

La figure suivante montre la communication TADDM dans un déploiement de serveur de synchronisation.

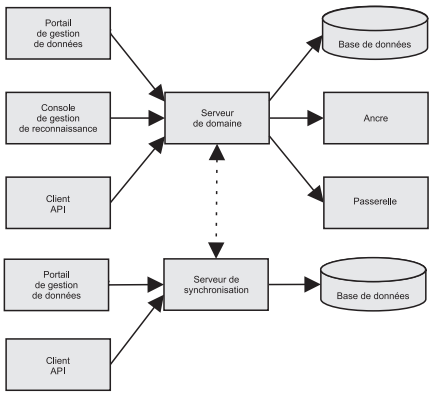

Figure 3. Communication TADDM dans un déploiement de serveur de synchronisation

Configuration des services de connectivité :

Pour un déploiement de serveur de synchronisation, vous pouvez configurer des services de connectivité publique, inter-serveur et locale.

Important : Les ports par défaut utilisés pour les propriétés décrites dans la suite de cette section s'appliquent uniquement aux propriétés répertoriées dans le fichier `collation.properties`. Si une propriété n'est pas codée ou figure en commentaire dans le fichier `collation.properties`, elle prend par défaut la valeur d'un port choisi de manière aléatoire. En particulier, assurez-vous que la propriété `com.ibm.cdb.service.RegistriesURLProvider.port` figure dans le fichier `collation.properties` pour que le démarrage du serveur aboutisse.

Services de connectivité publique

Le tableau suivant montre les paramètres d'hôte par défaut pour les services de connectivité publique du serveur de domaine et du serveur de synchronisation.

Tableau 22. Paramètres de l'hôte par défaut pour les services de connectivité publique du serveur de domaine et du serveur de synchronisation

Nom	Propriété de configuration	Interface par défaut
Hôte de service public	com.ibm.cdb.public.hostname	Défini par com.ibm.cdb.global.hostname

Le tableau suivant montre les paramètres de port par défaut pour les services de connectivité publique du serveur de domaine.

Tableau 23. Paramètres de l'hôte par défaut pour les services de connectivité publique du serveur de domaine

Nom	Propriété de configuration	Protocole	Port par défaut
Port du serveur d'API	com.ibm.cdb.service.ApiServer.port	TCP	9530
Port du serveur d'API sécurisé	com.ibm.cdb.service.SecureApiServer.secure.port	TCP	9531
Port HTTP (sans SSL)	com.ibm.cdb.service.web.port	TCP	9430
Port HTTPS (avec SSL)	com.ibm.cdb.service.web.secure.port	TCP	9431
Port de communication du serveur d'interface graphique	com.ibm.cdb.service.ClientProxyServer.port	TCP	9435
Port de communication SSL du serveur d'interface graphique	com.ibm.cdb.service.SecureClientProxyServer.secure.port	TCP	9434
Port du registre de services publics	com.ibm.cdb.service.registry.public.port	TCP	9433

Le tableau suivant montre les paramètres de port par défaut pour les services de connectivité publique du serveur de synchronisation.

Tableau 24. Paramètres de port par défaut pour les services de connectivité publique du serveur de synchronisation

Nom	Propriété de configuration	Protocole	Port par défaut
Port du serveur d'API	com.ibm.cdb.service.ApiServer.port	TCP	9530
Port du serveur d'API sécurisé	com.ibm.cdb.service.SecureApiServer.secure.port	TCP	9531
Port HTTP (sans SSL)	com.ibm.cdb.service.web.port	TCP	9430
Port HTTPS (avec SSL)	com.ibm.cdb.service.web.secure.port	TCP	9431

Tableau 24. Paramètres de port par défaut pour les services de connectivité publique du serveur de synchronisation (suite)

Nom	Propriété de configuration	Protocole	Port par défaut
Port du registre de services publics	com.ibm.cdb.service.registry.public.port	TCP	9433

Services de connectivité inter-serveur

Le tableau suivant montre les paramètres d'hôte par défaut pour les services de connectivité inter-serveur du serveur de domaine et du serveur de synchronisation.

Tableau 25. Paramètres de l'hôte par défaut pour les services de connectivité inter-serveur du serveur de domaine et du serveur de synchronisation

Nom	Propriété de configuration	Interface par défaut
Hôte de service inter-serveur	com.ibm.cdb.interserver.hostname	Défini par com.ibm.cdb.global.hostname

Le tableau suivant montre les paramètres de port par défaut pour les services de connectivité inter-serveur du serveur de domaine.

Tableau 26. Paramètres de port par défaut pour les services de connectivité inter-serveur du serveur de domaine

Nom	Propriété de configuration	Protocole	Port par défaut
Port du gestionnaire de topologie	com.ibm.cdb.service.TopologyManager.port	TCP	9550
Port du gestionnaire de sécurité	com.ibm.cdb.service.SecurityManager.port	TCP	9540
Port du fournisseur d'URL de registres	com.ibm.cdb.service.RegistriesURLProvider.port	TCP	9560
Port du registre de services inter-serveur	com.ibm.cdb.service.registry.interserver.port	TCP	4160

Le tableau suivant montre les paramètres de port par défaut pour les services de connectivité inter-serveur du serveur de synchronisation.

Tableau 27. Paramètres de port par défaut pour les services de connectivité inter-serveur du serveur de synchronisation

Nom	Propriété de configuration	Protocole	Port par défaut
Port du fournisseur d'URL de registres	com.ibm.cdb.service.RegistriesURLProvider.port	TCP	9560
Port du gestionnaire de sécurité entreprise	com.ibm.cdb.service.EnterpriseSecurityManager.port	TCP	9570
Port du registre de services inter-serveur	com.ibm.cdb.service.registry.interserver.port	TCP	4160

Services de connectivité locale

Les ports des services locaux ne sont pas définis de façon explicite. Tous les ports doivent être ouverts dans l'interface définie pour les services locaux. L'interface par défaut est celle de bouclage.

Le tableau suivant montre les paramètres d'hôte par défaut pour les services de connectivité locale du serveur de domaine et du serveur de synchronisation.

Tableau 28. Paramètres de l'hôte par défaut pour les services de connectivité locale du serveur de domaine et du serveur de synchronisation

Nom	Propriété de configuration	Interface par défaut
Hôte de service local	com.ibm.cdb.local.hostname	127.0.0.1

Configuration de la communication dans le déploiement de serveur de synchronisation :

Pour établir une communication réussie dans le déploiement de serveur de synchronisation, configurez des services de connectivité publics, inter-serveur et locaux.

Les tableaux qui suivent présentent les éléments que vous pouvez connecter dans le déploiement de serveur de synchronisation et les ports que vous devez ouvrir pour que la communication s'établisse.

Communication inter-serveur

Tableau 29. Configuration de la communication de connectivité inter-serveur dans le déploiement de serveur de synchronisation.

Elément A	Port	Direction	Elément B	Propriété de configuration
Serveur de domaine			**Serveur de synchronisation**	
	4160	→	Serveur de synchronisation - Registre de services inter-serveur	com.ibm.cdb.service.registry.interserver.port
	9560	→	Serveur de synchronisation - Fournisseur d'URL de registres	com.ibm.cdb.service.RegistriesURLProvider.port
	9570	→	Serveur de synchronisation - Gestionnaire de sécurité entreprise	com.ibm.cdb.service.EnterpriseSecurityManager.port
Serveur de domaine			**Serveur de synchronisation**	

Tableau 29. Configuration de la communication de connectivité inter-serveur dans le déploiement de serveur de synchronisation. (suite)

Elément A	Port	Direction	Elément B	Propriété de configuration
Serveur de domaine - Registre de services inter-serveur	4160	←	Serveur de synchronisation	com.ibm.cdb.service.registry.interserver.port
Serveur de domaine - Fournisseur d'URL de registres	9560	←		com.ibm.cdb.service.RegistriesURLProvider.port
Serveur de domaine - Gestionnaire de topologie	9540	←		com.ibm.cdb.service.SecurityManager.port
Serveur de domaine - Gestionnaire de topologie	9550	←		com.ibm.cdb.service.TopologyManager.port
Serveur de base de données	5000	←	**Serveur de domaine**	
Serveur de base de données	5000	←	**Serveur de synchronisation**	

Communication entre le portail de gestion de reconnaissance, les clients d'API et le portail Web, et entre les clients de portail de gestion de données et les serveurs de synchronisation

Tableau 30. Communication entre le portail de gestion de reconnaissance, les clients d'API et le portail Web, et entre les clients de portail de gestion de données et les serveurs de synchronisation.

Elément A	Port	Direction	Elément B	Propriété de configuration
Portail de gestion de reconnaissance	9433	→	Serveur de domaine - Registre de services publics	com.ibm.cdb.service.registry.public.port
	9435	→	Serveur de domaine - Serveur proxy client	com.ibm.cdb.service.ClientProxyServer.port
	9434	→	Serveur de domaine - Serveur proxy client sécurisé	com.ibm.cdb.service.SecureClientProxyServer.secure.port

Tableau 30. Communication entre le portail de gestion de reconnaissance, les clients d'API et le portail Web, et entre les clients de portail de gestion de données et les serveurs de synchronisation. (suite)

Elément A	Port	Direction	Elément B	Propriété de configuration
Clients d'API	9433	→	• Serveur de domaine - Registre de services publics • Serveur de synchronisation - Registre de services publics	com.ibm.cdb.service.registry.public.port
	9530	→	• Serveur de domaine - Serveur d'API • Serveur de synchronisation - Serveur d'API	com.ibm.cdb.service.ApiServer.port
	9531	→	• Serveur de domaine - Serveur d'API sécurisé • Serveur de synchronisation - Serveur d'API sécurisé	com.ibm.cdb.service.SecureApiServer.secure.port
Clients de portail Web et de portail de gestion de données	9430	→	• Serveur de domaine - Web • Serveur de synchronisation - Web	com.ibm.cdb.service.web.port
	9431	→	• Serveur de domaine - Web sécurisé • Serveur de synchronisation - Web sécurisé	com.ibm.cdb.service.web.secure.port

Communication entre l'ancre et la passerelle, et le serveur de domaine

Tableau 31. Communication entre l'ancre et la passerelle, et le serveur de domaine.

Elément A	Port	Direction	Elément B	Propriété de configuration
Ancre (en mode ssh) - SSH	22	←	Serveur de domaine (en mode ssh)	
Ancre (en mode direct) - SSH		←	Serveur de domaine (en mode direct)	
Ancre (en mode ssh) - Acheminement du tunnel SSH	8497	↔	Serveur de domaine (en mode ssh)	
Ancre (en mode direct) - Direct		←	Serveur de domaine (en mode direct)	
Passerelle - SSH	22	←	Serveur de domaine	

Communication locale

Tableau 32. Configuration de la communication de connectivité locale dans le déploiement de serveur de synchronisation.

Communication locale	Direction	Propriété de configuration
Serveur de domaine		

Tableau 32. Configuration de la communication de connectivité locale dans le déploiement de serveur de synchronisation. (suite)

Communication locale	Direction	Propriété de configuration
Serveur de domaine - Registre de services locaux	⟷	com.ibm.cdb.local.hostname
Serveur de domaine - Services locaux		
Serveur de domaine - 127.0.0.1		
Serveur de synchronisation		
Serveur de synchronisation - Registre de services locaux	⟷	com.ibm.cdb.local.hostname
Serveur de synchronisation - Services locaux		
Serveur de synchronisation - 127.0.0.1		

Référence des propriétés du serveur TADDM

Le fichier `collation.properties` contient les propriétés du serveur TADDM. Vous pouvez éditer certaines de ces propriétés.

Le fichier `collation.properties` se trouve dans le répertoire `$COLLATION_HOME/etc`. Il contient des commentaires sur chaque propriété.

Si vous mettez à jour le fichier `collation.properties`, vous devez le sauvegarder et redémarrer le serveur pour que les changements s'appliquent.

Propriétés sectorisées et non sectorisées

Le fichier `collation.properties` contient deux types de propriétés : sectorisées et non sectorisées.

Propriété sectorisée
: Propriété à laquelle vous pouvez ajouter une adresse IP ou le nom d'un ensemble de portées. Une fois cette adresse ou ce nom ajouté, la propriété devient dépendante du système hôte en cours de reconnaissance. Vous pouvez utiliser uniquement des noms d'ensembles de portées qui ne contiennent ni espace, ni apostrophe ('), ni point (.) ni barre oblique (/).

Propriété non sectorisée
: Propriété que vous ne pouvez pas réduire à une propriété spécifique à un objet.

Les propriétés suivantes, par exemple, ne sont pas des propriétés non sectorisées :

- `com.collation.log.filesize`
- `com.collation.discover.agent.command.lsof.Linux`

Toutefois, la propriété `com.collation.discover.agent.command.lsof.Linux` peut être une propriété sectorisée si vous lui ajoutez une adresse IP ou un nom d'ensemble de portées, comme illustré dans les exemples suivants :

- Exemple d'ajout de l'adresse IP `129.42.56.212` :
  ```
  com.collation.discover.agent.command.lsof.Linux.129.42.56.212=sudo lsof
  ```
- Exemple d'ajout d'un ensemble de portées nommé «scope1» :
  ```
  com.collation.discover.agent.command.lsof.Linux.scope1=sudo lsof
  ```

Propriétés à ne pas modifier

La modification de certaines propriétés du fichier `collation.properties` peut rendre votre système inopérant.

Vous ne devez pas modifier les propriétés suivantes :

com.collation.version
Identifie la version du produit.

com.collation.branch
Identifie la branche du code.

com.collation.buildnumber
Identifie le numéro de compilation. Ce numéro est défini par le processus de construction.

com.collation.oalbuildnumber
Identifie le numéro de compilation d'un autre processus de construction.

com.collation.SshWeirdReauthErrorList=Droit refusé
La valeur de cette propriété doit être `Droit refusé`.

La propriété est nécessaire car les systèmes Windows peuvent refuser de façon aléatoire des tentatives valides de connexion. Vous pouvez tenter d'utiliser le nom d'utilisateur et le mot de passe qui ont fonctionné lors des précédentes exécutions de la reconnaissance.

Propriétés de mise en cache des données d'identification d'accès

Ces propriétés s'appliquent à la mise en cache des données d'identification d'accès.

com.ibm.cdb.security.auth.cache.disabled=false
La valeur par défaut est `false`.

Cette propriété détermine si la mise en cache des données d'identification d'accès est désactivée.

Il s'agit d'une propriété sectorisée et profilée. Vous pouvez ajouter une adresse IP, le nom d'un ensemble de portées ou un nom de profil. Vous pouvez également la définir dans la configuration des profils, dans Discovery Management Console.

com.ibm.cdb.security.auth.cache.fallback.failed=true
La valeur par défaut est `true`.

Cette propriété active la rétromigration, lorsqu'un cache contient des données d'identification valides, mais lors de l'extraction, la validation échoue. Si la rétromigration est activée et que les données d'identification en cache ne sont plus valides, le cache effectue une itération sur tous les types d'entrée d'accès disponibles jusqu'à ce qu'une correspondance soit détectée.

Il s'agit d'une propriété sectorisée et profilée. Vous pouvez ajouter une adresse IP, le nom d'un ensemble de portées ou un nom de profil.

Les entrées suivantes sont des exemples d'entrée du fichier `collation.properties` :

```
com.ibm.cdb.security.auth.cache.fallback.failed=false
com.ibm.cdb.security.auth.cache.fallback.failed.10.160.160.11=true
com.ibm.cdb.security.auth.cache.fallback.failed.ScopeA=true
com.ibm.cdb.security.auth.cache.fallback.failed.GroupA=true
com.ibm.cdb.security.auth.cache.fallback.failed.Level_2_Discovery=false
```

Vous pouvez également définir cette propriété dans Discovery Management Console, dans la configuration des profils, dans l'onglet **Propriétés de la plateforme**.

com.ibm.cdb.security.auth.cache.fallback.invalid=true
La valeur par défaut est `true`.

Cette propriété active la rétromigration si l'entrée lue dans le cache contient une tentative non valide (le dernier accès a échoué, il n'existe pas de données d'identification valides). Si la rétromigration est activée, le cache effectue une itération sur tous les types d'entrée d'accès disponibles jusqu'à ce qu'une correspondance soit détectée.

Cette propriété est une propriété sectorisée et profilée. Vous pouvez ajouter une adresse IP, le nom d'un ensemble de portées ou un nom de profil.

Les entrées suivantes sont des exemples d'entrée du fichier `collation.properties` :

```
com.ibm.cdb.security.auth.cache.fallback.invalid=false
com.ibm.cdb.security.auth.cache.fallback.invalid.10.160.160.11=true
com.ibm.cdb.security.auth.cache.fallback.invalid.ScopeA=true
com.ibm.cdb.security.auth.cache.fallback.invalid.GroupA=true
com.ibm.cdb.security.auth.cache.fallback.invalid.Level_2_Discovery=false
```

Vous pouvez également définir cette propriété dans Discovery Management Console, dans la configuration des profils, dans l'onglet **Propriétés de la plateforme**.

Fix Pack 5 **com.ibm.cdb.security.auth.cache.itm.disabled=true**
La valeur par défaut est `true`.

Cette propriété détermine si la mise en cache des données d'identification d'accès est désactivée pour la reconnaissance OSLC.

Il s'agit d'une propriété sectorisée et profilée. Vous pouvez ajouter une adresse IP, le nom d'un ensemble de portées ou un nom de profil. Vous pouvez également la définir dans la configuration des profils, dans Discovery Management Console.

Concepts associés:

«Mise en cache des dernières données d'identification ayant fonctionné», à la page 15
TADDM peut placer en cache les dernières données d'identification d'accès ayant fonctionné. Elles peuvent être réutilisées lors de la prochaine reconnaissance (niveau 2 ou basées sur un script).

Propriétés de port API

Ces propriétés s'appliquent aux ports API.

com.ibm.cdb.service.ApiServer.port=9530
La valeur par défaut est `9530`. Il doit s'agir d'un entier.

Cette propriété définit le port qui communique avec le serveur d'API pour les demandes non SSL. La valeur peut être définie sur n'importe quel port disponible du serveur. Le client qui utilise l'interface de programme d'application pour la connexion doit spécifier ce port pour une connexion non SSL.

com.ibm.cdb.service.SecureApiServer.secure.port=9531
La valeur par défaut est `9531`. Il doit s'agir d'un entier.

Cette propriété définit le port qui communique avec le serveur d'API pour les demandes SSL. La valeur peut être définie sur n'importe quel port

disponible du serveur. Le client qui utilise l'interface de programme d'application pour la connexion doit spécifier ce port pour une connexion SSL.

Propriétés des agents de nettoyage

Les agents de nettoyage suppriment les alias et éléments de configuration orphelins ou corrigent les lignes manquantes dans les tables. La plupart d'entre eux lisent des propriétés définies dans le fichier `collation.properties`.

AliasesCleanupAgent

L'agent supprime les alias de la table ALIASES qui ne correspondent plus aux attributs de noms d'EC. Il supprime également les alias et les lignes de la table PERSOBJ qui ne contiennent aucun EC correspondant. L'agent lit les propriétés suivantes dans le fichier `collation.properties` :

Fix Pack 2 **com.ibm.cdb.topomgr.topobuilder.deleteAliasesWithoutMaster**
La valeur par défaut est `true`.

La propriété indique si les alias auxquels aucun alias maître correspondant n'est associé sont supprimés de la table ALIASES. Par défaut, la suppression est activée.

com.ibm.cdb.topomgr.topobuilder.max.row.fetch
La valeur par défaut est `1000`.

La propriété configure la taille de lot utilisée pour extraire des alias de la table ALIASES.

Si vous définissez la propriété sur `-1`, l'agent ne vérifie pas les alias.

com.ibm.cdb.topomgr.topobuilder.max.row.delete
La valeur par défaut est `5000`.

La propriété configure la taille de lot utilisée pour supprimer les alias.

Si vous définissez la propriété sur `-1`, l'agent ne supprime pas les alias, mais signale seulement les alias endommagés.

com.ibm.cdb.topomgr.topobuilder.agents.AliasesCleanupAgent.maxNumberOfMastersToScan
La valeur par défaut est `1000`.

La propriété configure le nombre d'EC nécessitant une vérification d'alias au cours d'une exécution unique de l'agent.

com.ibm.cdb.topomgr.topobuilder.cleanupOrphanedAliasesAndPersobj
La valeur par défaut est `true`. L'agent effectue le nettoyage.

La propriété active ou désactive le nettoyage des alias de la table ALIASES et des identificateurs globaux uniques de la table PERSOBJ qui ne contiennent aucun EC correspondant.

com.ibm.cdb.topomgr.topobuilder.DelayToRemoveAliases
La valeur par défaut est 12 (heures). Les alias orphelins de plus de 12 heures sont supprimés par l'agent.

La propriété définit le temps en heures au bout duquel les alias sans EC correspondant sont supprimés par l'agent. Elle protège les nouveaux alias qui risquent de ne pas contenir d'EC correspondant car le stockage d'EC n'est pas terminé.

Utilisez cette propriété avec précaution. Ne la paramétrez pas sur une valeur inférieure.

AliasesJnTableCleanupAgent

Cet agent supprime les lignes obsolètes de la table ALIASES_JN. Cette table contient l'historique des changements apportés à la table ALIASES. Elle permet de rechercher les éventuels excès de fusion des éléments de configuration dans la base de données. L'agent lit les propriétés suivantes dans le fichier `collation.properties` :

Fix Pack 2

com.ibm.cdb.topomgr.topobuilder.agents.AliasesJnTableCleanupAgent.maxRow
La valeur par défaut est `5000`. Il est recommandé de ne pas modifier la valeur par défaut.

Cette propriété indique le nombre maximal de lignes pouvant être supprimées en même temps par l'agent.

com.ibm.cdb.topomgr.topobuilder.agents.AliasesJnTableCleanupAgent.removeOlderThanDays
La valeur par défaut est `30` (jours).

Cette propriété supprime les lignes antérieures à la valeur indiquée. Par défaut, elle supprime les lignes datant de plus de 30 jours.

Si vous définissez cette propriété sur `0` ou une valeur inférieure, l'agent est désactivé.

com.ibm.cdb.topomgr.topobuilder.agents.AliasesJnTableCleanupAgent.timeout
La valeur par défaut est `1800` (secondes).

Cette propriété indique le délai après lequel l'agent dépasse le délai d'attente. Si le délai indiqué n'est pas suffisant pour supprimer toutes les lignes obsolètes, l'agent tente de les supprimer lors de sa prochaine exécution.

Agent DependencyCleanupAgent

L'agent supprime les objets de relation dormants. L'agent lit les propriétés suivantes dans le fichier `collation.properties` :

com.ibm.cdb.topomgr.topobuilder.agents.DependencyCleanupAgent.timeout
La valeur par défaut exprimée en secondes est `600`. Une fois ce temps écoulé, l'agent arrête la suppression des objets, même s'il en reste encore quelques uns.

com.ibm.cdb.topomgr.topobuilder.agents.DependencyCleanupAgent.removeOlderThanDays
La valeur par défaut exprimée en jours est `90`. Les objets de relation plus anciens que la valeur spécifiée sont traités comme des objets dormants.

ObjectsWithoutAliasesCleanupAgent

L'agent supprime les EC qui ne contiennent pas d'alias dans la table ALIASES. L'agent lit la propriété suivante dans le fichier `collation.properties` :

com.ibm.cdb.topomgr.topobuilder.agents.ObjectsWithoutAliasesCleanupAgent.maxToRemove
La valeur par défaut est `1000`

La propriété limite le nombre d'EC que l'agent supprime au cours d'une exécution. Si vous définissez la propriété sur `-1`, l'agent se ferme sans effectuer de nettoyage et affiche le message `ObjectsWithoutAliasesCleanupAgent is disabled`.

PersobjCleanupAgent

L'agent corrige toutes les lignes manquantes de la table PERSOBJ. Il n'utilise pas de configuration dans le fichier `collation.properties`. L'agent affiche le récapitulatif du nombre de lignes corrigées, comme dans l'exemple suivant :

```
2012-08-22 18:12:21,500 TopologyBuilder [TopologyBuilderEngineThread$Cleanup@4.0]
INFO agents.PersobjCleanupAgent - Fixed 10 rows in PERSOBJ table
```

Agent StorageExtentCleanupAgent

L'agent supprime les objets StorageExtent dormants. L'agent lit les propriétés suivantes dans le fichier `collation.properties` :

com.ibm.cdb.topomgr.topobuilder.agents.StorageExtentCleanupAgent.timeout
La valeur par défaut exprimée en secondes est `1800`. Une fois ce temps écoulé, l'agent arrête la suppression des objets, même s'il en reste encore quelques uns.

com.ibm.cdb.topomgr.topobuilder.agents.StorageExtentCleanupAgent.removeOlderThanDays
La valeur par défaut exprimée en jours est 1. Les objets StorageExtent qui sont plus anciens de 1 jour que leurs systèmes informatiques (ComputerSystems) parent sont traités comme des objets dormants.

Agent VlanInterfaceCleanupAgent

L'agent supprime les objets VlanInterface dormants. L'agent lit les propriétés suivantes dans le fichier `collation.properties` :

com.ibm.cdb.topomgr.topobuilder.agents.VlanInterfaceCleanupAgent.timeout
La valeur par défaut exprimée en secondes est `1800`. Une fois ce temps écoulé, l'agent arrête la suppression des objets, même s'il en reste encore quelques uns.

com.ibm.cdb.topomgr.topobuilder.agents.VlanInterfaceCleanupAgent.removeOlderThanDays
La valeur par défaut exprimée en jours est 1. Les objets VlanInterface qui sont plus anciens de 1 jour que leurs réseaux locaux virtuels parent sont traités comme des objets dormants.

Commandes pouvant nécessiter des privilèges élevés

Ces propriétés indiquent les commandes du système d'exploitation qu'utilise TADDM et qui peuvent demander un privilège élevé (root ou superutilisateur) pour une exécution sur le système cible.

Généralement, la commande sudo est utilisée sur les systèmes UNIX et Linux pour garantir une escalade des privilèges. Les solutions suivantes peuvent être employées à la place de sudo :

- Activer le droit d'accès setuid sur le programme exécutable cible
- Ajouter le compte de service de reconnaissance au groupe associé au programme exécutable cible

- Utiliser les privilèges d'administrateur pour le compte de service de reconnaissance (solution non préférentielle)

Pour chaque propriété, la commande sudo peut être configurée globalement. Cela signifie donc exécuter la commande avec sudo sur chaque cible de système d'exploitation ou la restreindre à un ensemble d'adresses IP ou de portée spécifique.

Important : Sur chaque système cible nécessitant une escalade des privilèges, la commande sudo doit être configurée avec l'option NOPASSWD. Sinon, la reconnaissance se bloque jusqu'au dépassement du délai de la commande sudo.

com.collation.discover.agent.command.hastatus.Linux=sudo /opt/VRTSvcs/bin/hastatus
com.collation.discover.agent.command.haclus.Linux=sudo /opt/VRTSvcs/bin/haclus
com.collation.discover.agent.command.hasys.Linux=sudo /opt/VRTSvcs/bin/hasys
com.collation.discover.agent.command.hares.Linux=sudo /opt/VRTSvcs/bin/hares
com.collation.discover.agent.command.hagrp.Linux=sudo /opt/VRTSvcs/bin/hagrp
com.collation.discover.agent.command.hatype.Linux=sudo /opt/VRTSvcs/bin/hatype
com.collation.discover.agent.command.hauser.Linux=sudo /opt/VRTSvcs/bin/hauser

- Ces propriétés sont nécessaires pour reconnaître les composants Veritas Cluster.
- Pour exécuter ces commandes sans sudo, le compte du service TADDM doit être membre du groupe d'administration Veritas sur la cible.

com.collation.discover.agent.command.vxdisk=vxdisk
com.collation.discover.agent.command.vxdg=vxdg
com.collation.discover.agent.command.vxprint=vxprint
com.collation.discover.agent.command.vxlicrep=vxlicrep
com.collation.discover.agent.command.vxupgrade=vxupgrade

- Ces propriétés reconnaissent des informations de stockage standard sur Veritas, ainsi que des informations plus spécifiques, comme le groupe de disques, les volumes Veritas, les multisystèmes et les sous-disques.

com.collation.platform.os.command.ps.SunOS=/usr/ucb/ps axww
com.collation.platform.os.command.psEnv.SunOS=/usr/ucb/ps axwweee
com.collation.platform.os.command.psParent.SunOS=ps -elf -o ruser,pid,ppid,comm
com.collation.platform.os.command.psUsers.SunOS=/usr/ucb/ps auxw

- Ces propriétés sont nécessaires pour reconnaître les informations de processus sur des systèmes Solaris.

  Vous pouvez spécifier une version Solaris en particulier en ajoutant le numéro de version SunOS au nom de la propriété. La propriété suivante est par exemple spécifique à Solaris 10 :

  ```
  com.collation.platform.os.command.ps.SunOS5.10=sudo /usr/ucb/ps axww
  ```

com.collation.platform.os.command.ps.Linux=ps axww
com.collation.platform.os.command.psEnv.Linux=ps axwweee
com.collation.platform.os.command.psParent.Linux=ps -ax -o ruser,pid,ppid,comm
com.collation.platform.os.command.psUsers.Linux=ps auxw

- Ces propriétés sont nécessaires pour reconnaître les informations de processus sur les systèmes Linux.

com.collation.platform.os.command.ps.AIX=ps axww
com.collation.platform.os.command.psEnv.AIX=ps axwweee
com.collation.platform.os.command.psParent.AIX=ps -elf -o ruser,pid,ppid,comm
com.collation.platform.os.command.psUsers.AIX=ps auxw

- Ces propriétés sont nécessaires pour reconnaître les informations de processus sur les systèmes AIX.

com.collation.platform.os.command.ps.HP-UX=sh UNIX95= ps -elfx -o pid,tty,state,time,args
com.collation.platform.os.command.psEnv.HP-UX=ps -eflx
com.collation.platform.os.command.psParent.HP-UX=sh UNIX95= ps -elfx -o ruser,pid,ppid,comm
com.collation.platform.os.command.psUsers.HP-UX=ps -efx

- Ces propriétés sont nécessaires pour reconnaître les informations de processus sur les systèmes HP-UX.

com.collation.discover.agent.command.lsof.Vmnix=lsof
com.collation.discover.agent.command.lsof.Linux=lsof
com.collation.discover.agent.command.lsof.SunOS.1.2.3.4=sudo lsof
com.collation.discover.agent.command.lsof.Linux.1.2.3.4=sudo lsof
com.collation.discover.agent.command.lsof.HP-UX=lsof
com.collation.discover.agent.command.lsof.AIX=lsof

- Ces propriétés sont nécessaires pour reconnaître les informations de port ou processus.

  Vous pouvez spécifier une version Solaris en particulier en ajoutant le numéro de version SunOS au nom de la propriété. La propriété suivante est par exemple spécifique à Solaris 10 :

  ```
  com.collation.discover.agent.command.lsof.SunOS5.10=sudo /usr/local/bin/lsof
  ```

com.collation.discover.agent.command.dmidecode.Linux=dmidecode
com.collation.discover.agent.command.dmidecode.Linux.1.2.3.4=sudo dmidecode

- Ces propriétés sont nécessaires pour reconnaître le fabricant, le modèle et le numéro de série sur les systèmes Linux.

com.collation.discover.agent.command.vmcp.Linux=
Cette propriété peut être utilisée pour reconnaître un ID utilisateur invité sur un système virtuel Linux cible s'exécutant sur un système d'exploitation z/VM.

com.collation.discover.agent.command.cat.SunOS=cat
com.collation.discover.agent.command.cat.SunOS.1.2.3.4=sudo cat

- Cette propriété est nécessaire pour reconnaître les informations de configuration d'un pare-feu de point de contrôle sous Solaris.

com.collation.discover.agent.command.interfacesettings.SunOS=sudo ndd
com.collation.discover.agent.command.interfacesettings.Linux=sudo mii-tool
com.collation.discover.agent.command.interfacesettings.SunOS.1.2.3.4=sudo ndd
com.collation.discover.agent.command.interfacesettings.Linux.1.2.3.5=sudo mii-tool
com.collation.discover.agent.command.interfacesettings.HP-UX=lanadmin
com.collation.discover.agent.command.interfacesettings.AIX=netstat

- Ces propriétés sont nécessaires pour reconnaître les informations d'interface réseau avancées (vitesse de l'interface, par exemple).

com.collation.discover.agent.command.adb.HP-UX=adb
com.collation.discover.agent.command.adb.HP-UX.1.2.3.4=sudo adb

- Cette propriété est nécessaire pour reconnaître les informations de processeur sur les systèmes HP.

com.collation.discover.agent.command.kmadmin.HP-UX=kmadmin
com.collation.discover.agent.command.kmadmin.HP-UX.1.2.3.4=sudo /usr/sbin/kmadmin

- Cette propriété est nécessaire pour reconnaître les modules de noyau sur les systèmes HP.

com.collation.platform.os.command.partitionTableListing.SunOS=prtvtoc

- Cette propriété est utilisée pour reconnaître les informations de table de partition sous Solaris.

com.collation.platform.os.command.lvm.lvdisplay.1.2.3.4=sudo lvdisplay -c
com.collation.platform.os.command.lvm.vgdisplay.1.2.3.4=sudo vgdisplay -c
com.collation.platform.os.command.lvm.pvdisplay.1.2.3.4=sudo pvdisplay -c

- Ces propriétés sont nécessaires pour reconnaître les informations relatives au volume de stockage.

com.collation.platform.os.command.lputil.SunOS.1.2.3.4=sudo /usr/sbin/lpfc/lputil

- Cette propriété est nécessaire pour reconnaître les informations relatives aux adaptateurs de bus de contrôle de canal optique Emulex sous Solaris.

com.collation.platform.os.command.crontabEntriesCommand.SunOS=crontab -l
com.collation.platform.os.command.crontabEntriesCommand.Linux=crontab -l -u
com.collation.platform.os.command.crontabEntriesCommand.AIX=crontab -l
com.collation.platform.os.command.crontabEntriesCommand.HP-UX=crontab -l

- Ces propriétés sont nécessaires pour reconnaître les entrées **crontab**. Vous pouvez indiquer ces propriétés sous forme de propriété à portée, en leur ajoutant une adresse IP ou un nom d'ensemble de portées. L'exemple suivant montre l'ajout d'une adresse IP :

  ```
  com.collation.platform.os.command.crontabEntriesCommand.AIX.1.2.3.4=crontab -l
  ```

com.collation.platform.os.command.filesystems.Linux=df -kTP
com.collation.platform.os.command.filesystems.SunOS=df -k | grep -v 'No such file or directory' | grep -v 'Input/output error' | awk '{print $1, $2, $4, $6}'
com.collation.platform.os.command.filesystems.AIX=df -k | grep -v 'No such file or directory' | grep -v 'Input/output error' | awk '{print $1, $2, $3, $7}
com.collation.platform.os.command.filesystems.HP-UX=df -kP | grep -v 'No such file or directory' | grep -v 'Input/output error' | grep -v Filesystem

- Ces propriétés sont nécessaires pour reconnaître les systèmes de fichiers.

com.collation.platform.os.command.fileinfo.ls=sudo ls
com.collation.platform.os.command.fileinfo.ls.1.2.3.4=sudo ls
com.collation.platform.os.command.fileinfo.cksum=sudo cksum
com.collation.platform.os.command.fileinfo.cksum.1.2.3.4=sudo cksum
com.collation.platform.os.command.fileinfo.dd=sudo dd
com.collation.platform.os.command.fileinfo.dd.1.2.3.4=sudo dd

- Ces propriétés sont nécessaires pour la capture des fichiers privilégiés.

- La capture de fichiers privilégiés s'utilise quand le compte de service de reconnaissance ne dispose pas d'un accès en lecture aux fichiers de configuration d'application nécessaires pour la reconnaissance.

com.collation.discover.agent.WebSphereVersionAgent.versionscript=sudo
Cette propriété peut être activée de sorte à accéder au fichier WebSphere `versionInfo.sh` si l'utilisateur de la reconnaissance n'a pas accès au système WebSphere Application Server cible.

com.collation.platform.os.command.fileinfo.OnlyDirectoryRecursive
Cet indicateur modifie le mode de reconnaissance des fichiers. La valeur par défaut est `False`.

Si vous définissez cet indicateur sur `True`, ce mécanisme n'utilise pas la commande find pour reconnaître le contenu d'un répertoire de manière récursive.

Si vous définissez l'indicateur sur `False`, ce mécanisme utilise la commande find pour reconnaître un fichier de manière récursive sans que soit indiqué l'emplacement exact du fichier.

Propriétés du service de menu contextuel et du service d'intégration des données

Ces propriétés s'appliquent au service de menu contextuel et au service d'intégration des données.

com.ibm.cdb.DisCmsIntegration.enabled=true
La valeur par défaut est définie sur `true`.

Cette propriété définit si l'agent de générateur de topologie CMSDISAgent doit procéder à des mises à jour des données TADDM enregistrées auprès du service de menu contextuel et du service d'intégration des données.

com.ibm.cdb.DisCmsIntegration.dbUser=*utilisateur*
Cette propriété définit l'ID utilisateur de la base de données pour le service de menu contextuel et le service d'intégration des données.

com.ibm.cdb.DisCmsIntegration.dbPassword=*mot_de_passe*
Cette propriété définit le mot de passe pour le service de menu contextuel et le service d'intégration des données.

com.ibm.cdb.DisCmsIntegration.dbUrl=*url*
Cette propriété définit l'URL de base de données pour le service de menu contextuel et le service d'intégration des données.

com.ibm.cdb.DisCmsIntegration.dbDriver=*pilote*
Cette propriété définit le pilote de base de données pour le service de menu contextuel et le service d'intégration des données.

com.ibm.cdb.DisCmsIntegration.changehistory.days_previous=30
La valeur par défaut est `30`.

Cette propriété définit le nombre de jours d'historique des modifications à afficher dans les rapports de modification pour le service de menu contextuel et le service d'intégration des données.

Propriétés de la base de données

Ces propriétés s'appliquent à la base de données TADDM.

com.collation.db.password=mot_de_passe
Cette propriété définit le mot de passe de la base de données, qui est stocké sur le serveur TADDM, pour l'utilisateur de la base de données.

com.collation.db.archive.password=mot_de_passe
Cette propriété définit le mot de passe de la base de données, qui est stocké sur le serveur TADDM, pour l'utilisateur d'archive de la base de données.

com.ibm.cdb.db.max.retries
Cette propriété indique le nombre de tentatives pour essayer d'établir la connexion à la base de données.

com.ibm.cdb.db.timeout
Cette propriété indique le temps de sommeil entre deux tentatives d'un nouvel essai.

com.ibm.cdb.db.connection.ssl.enable=false
Cette propriété indique si la connexion à la base de données est établie en mode SSL (couche Secure Sockets Layer) pour l'utilisateur de base de données.

La valeur par défaut est `false`.

com.ibm.cdb.db.connection.ssl.truststore.file=nom_fichier
Cette propriété indique un fichier de mémoire protégée qui est utilisé pour la connexion SSL à la base de données pour l'utilisateur de base de données. Le fichier de mémoire protégée doit être dans le répertoire `$COLLATION_HOME/etc/`.

com.ibm.cdb.db.connection.ssl.truststore.password=mot_de_passe
Cette propriété indique un mot de passe de la mémoire protégée qui est utilisé pour la connexion SSL à la base de données pour l'utilisateur de base de données.

com.ibm.cdb.db.archive.connection.ssl.enable=false
Cette propriété indique si la connexion à la base de données est établie en mode SSL (couche Secure Sockets Layer) pour l'utilisateur de base d'archives.

La valeur par défaut est `false`.

com.ibm.cdb.db.archive.connection.ssl.truststore.file=nom_fichier
Cette propriété indique un fichier de mémoire protégée qui est utilisé pour la connexion SSL à la base de données pour l'utilisateur de base d'archives. Le fichier de mémoire protégée doit être dans le répertoire `$COLLATION_HOME/etc/`.

com.ibm.cdb.db.archive.connection.ssl.truststore.password=mot_de_passe
Cette propriété indique un mot de passe de la mémoire protégée qui est utilisé pour la connexion SSL à la base de données pour l'utilisateur de base d'archives.

Pour chiffrer les mots de passe dans le fichier `collation.properties` procédez comme suit :

1. Editez l'utilisateur de la base de données ou archivez le mot de passe de l'utilisateur à l'aide d'un texte en clair, ou les deux.
2. Arrêtez le serveur TADDM.
3. Exécutez le fichier `encryptprops.sh` ou `encryptprops.bat` (situé dans le répertoire `$COLLATION_HOME/bin`). Ce script chiffre les mots de passe.
4. Redémarrez le serveur TADDM.

Propriétés de reconnaissance

Ces propriétés s'appliquent en général à la reconnaissance. Les propriétés du serveur TADDM affectant un détecteur spécifique sont indiquées dans le *Guide de référence des détecteurs* de TADDM pour chaque détecteur.

Fix Pack 4 **com.discover.anchor.maxChannelNumber**

Cette propriété indique le nombre maximal de canaux ouverts simultanément dans la session SSH entre le serveur TADDM et l'ancrage. Si ce nombre est trop élevé, la reconnaissance d'un tel ancrage peut se bloquer et les capteurs inclus dans une telle portée peuvent dépasser le délai d'attente. Dans pareils cas, utilisez cette propriété pour contrôler le nombre de canaux ouverts.

La valeur par défaut est `50`.

Fix Pack 4 **com.collation.platform.os.copyToLocal.preferScpCommand**

Cette propriété indique si la commande **scp** externe peut être utilisée pour copier des fichiers d'hôtes distants, habituellement des cibles de reconnaissance, sur le serveur TADDM. La commande **scp** externe est définie dans la propriété `com.collation.platform.os.scp.command`. Pour activer l'utilisation de la commande **scp** externe, définissez cette propriété sur `true`.

La valeur par défaut de cette propriété est `false`.

Remarque : Cette propriété s'applique uniquement aux sessions SSH qui sont établies via une procédure de connexion basée sur clé (voir «Configuration de la reconnaissance avec Secure Shell (SSH)», à la page 120). En cas d'authentification avec un nom d'utilisateur et un mot de passe, la commande **scp** interne est utilisée indépendamment de la valeur de la propriété `com.collation.platform.os.copyToLocal.preferScpCommand`.

Il s'agit d'une propriété sectorisée. Vous pouvez lui adjoindre une adresse IP ou le nom d'un ensemble de portées. Par exemple :

```
com.collation.platform.os.copyToLocal.preferScpCommand.12.234.255.4=true
```

com.collation.platform.os.scp.command

Cette propriété spécifie le chemin d'accès à la commande de système d'exploitation **scp**. Vous pouvez y recourir lorsqu'un client SSH interne ne parvient pas à envoyer des fichiers entre le serveur TADDM et des hôtes distincts, généralement des cibles de reconnaissance. Il est possible d'utiliser une commande de remplacement à condition que sa syntaxe soit identique à celle de la commande **scp**.

Exemple de valeur : `/usr/local/bin/scp`.

Fix Pack 3 **com.collation.platform.session.ssh.winAuth**

Cette propriété indique si une tentative de connexion avec des informations d'identification Windows peut avoir lieu lorsque la session SSH est utilisée. La valeur par défaut est `true`.

Vous pouvez définir la valeur sur `false` si des tentatives de connexion à des serveurs non Windows avec des informations d'identification Windows risquent de se produire pendant la reconnaissance. La définition de cette valeur peut empêcher le blocage des comptes Windows Active Directory.

Fix Pack 3 **com.collation.platform.os.ignoreL2InterfaceDescription**

Cette propriété spécifie les descriptions des interfaces L2 reconnues qui seront ignorées pendant le calcul de la signature de système informatique.

Par exemple, si vous ne voulez pas que l'interface d'équilibreur de charge Microsoft soit utilisée pour calculer la signature d'un système informatique, spécifiez la valeur suivante :

```
com.collation.platform.os.ignoreL2InterfaceDescription=Microsoft Load
Balancer Interface
```

La valeur de cette propriété est traitée comme une expression régulière, ce qui signifie que vous pouvez ajouter plusieurs descriptions de l'interface et que vous n'avez pas besoin d'utiliser de séparateur comme la virgule.

Fix Pack 3 **com.ibm.cdb.topomgr.topobuilder.agents.ConnectionDependencyAgent2.dependencyPlaceholders**

Lorsqu'elle est définie sur `true`, cette propriété crée des serveurs d'applications de marque de réservation pour les dépendances non reconnues.

Remarque : Cette propriété n'est pas fournie dans le fichier `collation.properties` par défaut. Vous devez l'y ajouter.

Lorsque vous définissez la valeur sur `true` pour la première fois, vous devez redémarrer TADDM afin d'activer les attributs étendus pour les classes LogicalConnection et SSoftwareServer. Ces attributs étendus sont nécessaires au bon fonctionnement de cette fonction.

Pour plus d'informations sur les espaces réservés, voir «Configuration pour la reconnaissance des marques de réservation», à la page 135.

com.collation.platform.session.EncodingOverRide

Cette propriété indique le type de codage utilisé pendant une session de reconnaissance. Elle s'avère particulièrement utile lorsque vos serveurs cibles utilisent un codage différent de celui du serveur TADDM.

La valeur de cette propriété est le nom du codage, par exemple `UTF-8`. Cette propriété n'est pas fournie dans le fichier `collation.properties` par défaut. Vous devez l'ajouter

Vous pouvez également ajouter une portée ou une adresse IP à cette propriété. Par exemple :

```
com.collation.platform.session.EncodingOverRide.37.53.105.24=UTF-8
```

com.collation.discover.anchor.forceDeployment=true

La valeur par défaut est `true`.

Cette propriété définit si les ancrages de la portée reconnue doivent être déployés lors du démarrage de la reconnaissance.

Lorsque vous définissez cette valeur sur `false`, les ancrages sont déployés uniquement si l'une des deux conditions suivantes est remplie :

- Aucune adresse IP de la portée ne répond à une commande ping
- Le port 22 n'est accessible sur aucune adresse IP reconnue

Si des ancres existent dans une chaîne, cette condition s'applique à toutes les ancres de la chaîne. Si une ancre dans la chaîne comporte une condition, les ancres précédentes doivent remplir la condition pour que toutes les ancres puissent être déployées.

com.collation.discover.anchor.lazyDeployment=false

La valeur par défaut est `false`.

Cette propriété définit si les fichiers requis par un détecteur sont copiés lors du déploiement d'un ancrage (la valeur est `false`) ou lors du démarrage de ce détecteur (la valeur est `true`).

Par exemple, des dépendances existent pour le détecteur IBM WebSphere dans le répertoire `dist/lib/websphere`. La taille du répertoire est de 130 Mo. Si cette propriété est associée à la valeur `false`, les données de dépendance sont copiées dans l'hôte cible lorsque l'ancrage est déployé. Si la propriété est associée à la valeur `true`, les données sont copiées lorsque le détecteur WebSphere doit être exécuté sur l'ancrage. Si aucun détecteur WebSphere n'est exécuté via l'ancrage, les 130 Mo ne sont pas envoyés à l'hôte distant.

com.collation.discover.DefaultAgentTimeout=600000

La valeur est `600000` (en millisecondes), soit 10 minutes.

Cette propriété indique le délai d'attente des détecteurs en millisecondes. Le délai d'attente par défaut ne doit pas être modifié. Vous pouvez à la place indique le délai d'attente pour des détecteurs individuels.

Pour modifier le délai d'attente d'un détecteur particulier, ajoutez la ligne suivante au fichier `collation.properties` :

```
com.collation.discover.agent.sensorNameSensor.timeout=
  durée_en_millisecondes
```

Par exemple :

```
com.collation.discover.agent.OracleSensor.timeout=1800000
```

com.collation.IpNetworkAssignmentAgent.defaultNetmask=*démarrage_ip-ip_end/netmask*[, ...]

Cette propriété détermine comment les adresses IP reconnues lors d'une reconnaissance de niveau 1 sont affectées à des sous-réseaux générés. La reconnaissance de niveau 1 ne permet pas de reconnaître les sous-réseaux. Des objets IpNetwork sont générés pour contenir des interfaces non associées à un sous-réseau existant reconnu lors d'une reconnaissance de niveau 2 ou 3. Cette propriété de configuration définit les objets IpNetwork à créer et le nombre de noeuds que doit contenir chaque sous-réseau. (Elle s'applique aussi à toute interface reconnue pendant une reconnaissance de niveau 2 ou 3 et qui, pour une raison donnée, ne peut pas être affectée à un sous-réseau reconnu.)

La valeur de cette propriété tient sur une seule ligne, avec une ou plusieurs entrées séparées par des virgules. Chaque entrée décrit une plage d'adresses IP dans la notation décimale à points IPv4, ainsi qu'un masque de sous-réseau défini sous forme d'entier entre 8 et 31. Les interfaces reconnues dans la plage définie sont ensuite placées dans les sous-réseaux créés, dont la taille n'est pas supérieure à celle définie par le masque de sous-réseau.

Par exemple, la valeur suivante définit deux plages d'adresses de sous-réseau avec des masques de sous-réseau distincts :

```
9.0.0.0-9.127.255.255/23, 9.128.0.0-9.255.255.255/24
```

Les plages d'adresses indiquées peuvent se chevaucher. Si une adresse IP reconnue tombe dans plusieurs plages, elle est affectée au premier sous-réseau correspondant, dans l'ordre où elles apparaissent dans la valeur de la propriété.

Après la création ou la modification de cette propriété de configuration et le redémarrage du serveur TADDM, toutes les reconnaissances de niveau 1

utilisent les sous-réseaux définis. Pour réaffecter des objets IpInterface existants dans la base de données TADDM, allez au répertoire `$COLLATION_HOME/bin` et exécutez l'une des commandes suivantes :

- **`adjustL1Networks.sh`** (systèmes Linux et UNIX)
- **`adjustL1Networks.bat`** (systèmes Windows)

Si la valeur n'est pas définie correctement, les messages appropriés s'affichent uniquement lors de l'exécution de l'utilitaire de ligne de commande **`adjustL1Networks.sh`** (systèmes Linux et UNIX) ou **`adjustL1Networks.bat`** (systèmes Windows). Sinon, les messages sont placés dans le fichier `TopologyBuilder.log`, à l'intérieur du répertoire `$COLLATION_HOME/log/services` et dans le fichier `IpNetworkAssignmentAgent.log` à l'intérieur du répertoire `$COLLATION_HOME/log/agents`.

Ce script réaffecte tous les objets IpInterface reconnus pendant les reconnaissances de niveau 1 aux sous-réseaux appropriés, comme décrit dans la propriété de configuration. Tout objet IpNetwork généré ne contenant pas d'interfaces est alors supprimé de la base de données. Au terme de l'exécution du script, l'interface TADDM peut présenter plusieurs notifications concernant des composants modifiés en raison de modifications apportées à des objets. Vous pouvez effacer ces notifications en actualisant la fenêtre.

Remarque : Avant d'utiliser cette commande, vérifiez que le serveur TADDM est actif et qu'aucune opération de reconnaissance ou de chargement en bloc n'est en cours. Ce script n'est pas pris en charge sur le serveur de synchronisation.

com.collation.number.persist.discovery.run=30
La valeur par défaut est `30`.

Indique le nombre de reconnaissances pour lesquelles des informations sont sauvegardées dans l'historique de reconnaissance, dans le portail de gestion de données et la console de gestion de reconnaissance.

Pour modifier la valeur par défaut dans un déploiement de serveurs de diffusion en continu, entrez la nouvelle valeur sur le serveur de stockage principal.

com.collation.platform.os.hostappdescriptorfiles.dir="*chemin*"
Définit le chemin d'accès complet au répertoire dans lequel les fichiers descripteurs d'application pour les systèmes informatiques (hôtes) sont déployés. Cette propriété est requise si vous souhaitez ajouter des systèmes informatiques à des applications métier à l'aide de descripteurs d'application. Vous pouvez configurer cette propriété pour un nom d'hôte ou une adresse IP spécifique afin de définir un emplacement différent pour chaque hôte. Les exemples suivants montrent comment définir le chemin du descripteur d'application hôte :

- Systèmes Linux et UNIX : `/home/taddm/hostappdescriptors`
- Systèmes Windows : `c://taddm//hostappdescriptors`

com.collation.platform.session.GatewayForceSsh
Indique si la passerelle doit être forcée à agir indépendamment de l'ancrage. Les valeurs valides sont *true* et *false*. Paramétrez la valeur sur `true` pour résoudre les problèmes Cygwin lorsque la passerelle et l'ancrage résident sur le même système. Lorsque la valeur est paramétrée sur true,

une session SSH, plutôt qu'une session locale, est utilisée pour le transfert du trafic entre la passerelle et l'ancrage.

com.collation.rediscoveryEnabled=`false`
La valeur par défaut est `false`.

Cette propriété s'applique à la nouvelle reconnaissance d'un élément de configuration déjà reconnu. La fonction de nouvelle reconnaissance est disponible dans le portail de gestion de données.

Restriction : La nouvelle reconnaissance ne peut pas utiliser les données d'identification d'un profil personnalisé, elle utilise les données d'identification d'une liste globale.

Remarque :

Pour activer la fonction de nouvelle reconnaissance dans un déploiement de serveur de domaine, associez cette propriété à la valeur `true`.

Pour activer la fonction de nouvelle reconnaissance dans un déploiement de serveurs de diffusion en continu, associez cette propriété à la valeur `true` sur le serveur de reconnaissance et le serveur de stockage.

Nouvelle reconnaissance dans un déploiement de serveurs de diffusion en continu

Lorsque la nouvelle reconnaissance est utilisée dans un déploiement de serveurs de diffusion en continu, un élément de configuration peut être reconnu par différents serveurs de reconnaissance, mais seul le dernier serveur de reconnaissance ayant reconnu cet élément peut le reconnaître de nouveau. Comme il existe plusieurs serveurs de reconnaissance, les informations de reconnaissance relatives à un élément de configuration sont écrasées par le serveur de reconnaissance suivant.

Lorsque vous activez la fonction de nouvelle reconnaissance sur le serveur de reconnaissance, des informations supplémentaires relatives à la nouvelle reconnaissance sont créées pour chaque objet reconnu.

Lorsque vous activez la fonction de nouvelle reconnaissance sur le serveur de stockage, chaque objet reconnu est stocké avec les informations supplémentaires sur la nouvelle reconnaissance.

Si la nouvelle reconnaissance est activée sur le serveur de reconnaissance mais désactivée sur le serveur de stockage, les informations associées ne seront pas disponibles dans la base de données TADDM. En outre, vous devez vérifier que les mêmes autorisations d'accès sont utilisées pour le serveur de reconnaissance et le serveur de stockage.

com.ibm.cdb.discover.sensor.sys.utilization.workingdir=`/tmp/taddm`
La valeur par défaut est `/tmp/taddm`.

Cette propriété spécifie la racine des scripts de détection d'utilisation IBM Tivoli à exécuter sur le système cible. Si vous ne spécifiez pas cette valeur, le chemin défini par la propriété `com.ibm.cdb.taddm.script.path` est utilisé.

com.ibm.cdb.locationTag
Spécifie l'attribut de balise d'emplacement de chaque élément de configuration créé sur le serveur TADDM. L'attribut de balise

d'emplacement, qui identifie l'emplacement d'un élément de configuration, est utilisé pour prendre en charge les balises d'emplacement statiques. Avant de spécifier cette balise, vous devez définir `com.ibm.cdb.locationTaggingEnabled` sur `true`.

com.ibm.cdb.locationTaggingEnabled=false
La valeur par défaut est `false`.

Indique si la fonctionnalité de balise d'emplacement est activée. Définissez cette propriété sur `true` pour :

- Spécifier l'attribut de balise d'emplacement de chaque élément de configuration créé sur le serveur TADDM (balises d'emplacement statiques). Consultez la propriété `com.ibm.cdb.locationTag` pour plus d'informations.
- Spécifier une balise d'emplacement dynamique pour les éléments de configuration créés pendant une reconnaissance unique, à l'aide de l'interface de ligne de commande. Les balises d'emplacement dynamiques remplacent les balises d'emplacement qui existent déjà (balises d'emplacement statiques).
- Spécifier une balise d'emplacement dynamique pour les éléments de configuration créés lors du chargement de données, à l'aide du programme de chargement en bloc.
- Spécifier une balise d'emplacement lors de l'exécution d'un rapport BIRT pour filtrer les données et informations de rapport concernant uniquement l'emplacement spécifié.
- Créer une valeur de balise d'emplacement pour les éléments de configuration créés pendant un processus de construction de topologie.

com.ibm.cdb.taddm.host
Indique l'alias de l'hôte de serveur TADDM. Si vous ne spécifiez pas cette valeur, le nom d'hôte système est utilisé. Si le serveur TADDM ne parvient pas à résoudre le nom d'hôte système ou s'il le résout en système hôte local, vous devez spécifier cette propriété manuellement.

com.ibm.cdb.taddm.script.path=/tmp/taddm
La valeur par défaut est `/tmp/taddm`.

Cette propriété spécifie la racine des scripts de détection à exécuter sur le système cible. Une arborescence de sous-répertoires est créée à cet emplacement, qui suit le format : `alias_hôte/numéro_reconnaissance/nom_détecteur`. Le nom `alias_hôte` est extrait de la propriété `com.ibm.cdb.taddm.host`. Si vous ne spécifiez pas cette propriété, le nom d'hôte système est utilisé. Pour distinguer les différentes reconnaissances sur le même serveur de reconnaissance, un numéro est attribué au répertoire `numéro_reconnaissance`. Les scripts et résultats de reconnaissance sont enregistrés dans cette structure de répertoires.

com.collation.discover.agent.signature.ignore.*1.2.3.4*=true
Cette propriété permet d'ignorer une adresse IP pendant le calcul de signature.

Dans le cas de certaines configurations, la signature relative à un système informatique peut apparaître comme étant non unique, ce qui peut se traduire par des problèmes lors du rapprochement avec les entrées existantes dans la base de données de TADDM. Par exemple, cette situation peut se rencontrer lorsque vous utilisez des machines virtuelles dont les cartes réseau virtuelles possèdent une adresse matérielle et une adresse IP valides. Dans de tels cas, vous devez exclure le calcul de

signature et utiliser une autre règle de nommage, comme le modèle du produit, le fabricant ou le numéro de série.

Pour chaque adresse IP que vous voulez ignorer, ajoutez la propriété `com.collation.discover.agent.signature.ignore.1.2.3.4=true`, où *1.2.3.4* représente l'adresse IP à ignorer.

Pour ignorer plusieurs adresses IP, vous pouvez créer une portée de reconnaissance. Ajoutez la propriété `com.collation.discover.agent.signature.ignore.listenoire=true` au fichier `collation.properties`, *listenoire* représentant la portée de reconnaissance avec toutes les adresses IP à ignorer.

Propriétés de reconnaissance avancées :

Les propriétés de reconnaissance avancées spécifient la capacité de la mémoire tampon pour le stockage des éléments de travail, le nombre de redémarrages autorisé pour des éléments de reconnaissance spécifiques ou la valeur temporelle pour l'enregistrement des statistiques dans un journal. Ne modifiez pas ces propriétés sauf si vous devez configurer précisément le processus de reconnaissance.

com.ibm.cdb.discover.buffers.workitem.capacity=64
La valeur par défaut est `64`. Cette valeur est toujours égale au double de la valeur de la propriété `com.collation.discover.dwcount`, qui est `32` par défaut.

Cette propriété spécifie la capacité de la mémoire tampon pour le stockage des éléments de travail de reconnaissance. Elle est utilisée pour limiter les besoins en mémoire du processus de reconnaissance et ainsi éviter les erreurs OutOfMemory. Pour chaque reconnaissance, un nouveau détecteur est démarré.

Ne définissez pas cette propriété sur une valeur inférieure au nombre d'agents de reconnaissance spécifié dans la propriété `com.collation.discover.dwcount` ou certains d'entre eux resteront en état de veille.

com.ibm.cdb.discover.buffers.workitem.maxresets=10
La valeur par défaut est `10`.

Cette propriété indique le nombre de redémarrages autorisé pour les détecteurs en cas d'échec inattendu, par exemple l'échec d'une machine JVM TADDM responsable de la reconnaissance.

De même, le nombre de redémarrages des éléments du processus de reconnaissance est limité par la propriété `com.ibm.cdb.discover.runrestartlimit` qui spécifie ce nombre.

com.ibm.cdb.discover.buffers.seed.capacity=100
La valeur par défaut est `100`.

Cette propriété spécifie la capacité de la mémoire tampon pour le stockage des éléments de travail de valeur de départ. Elle est utilisée pour limiter les besoins en mémoire du processus de reconnaissance et ainsi éviter les erreurs OutOfMemory.

com.ibm.cdb.discover.buffers.result.capacity=100
La valeur par défaut est `100`.

Cette propriété spécifie la capacité de la mémoire tampon pour le stockage des éléments de travail de résultat. Elle est utilisée pour limiter les besoins

en mémoire du processus de reconnaissance et ainsi éviter les erreurs OutOfMemory. Pour chaque élément de travail de résultat, un nouveau détecteur peut démarrer.

Définissez cette propriété sur la même valeur que la propriété`com.ibm.cdb.discover.buffers.discovered.capacity`.

com.ibm.cdb.discover.buffers.result.maxresets=10
La valeur par défaut est `10`.

Cette propriété indique le nombre de démarrages de nouveau détecteur autorisé pour le processus de reconnaissance en cas d'échec inattendu, par exemple l'échec d'une machine JVM TADDM responsable de la reconnaissance.

De même, le nombre de redémarrages des éléments du processus de reconnaissance est limité par la propriété `com.ibm.cdb.discover.runrestartlimit` qui spécifie ce nombre.

com.ibm.cdb.discover.buffers.discovered.capacity=100
La valeur par défaut est `100`.

Cette propriété spécifie la capacité de la mémoire tampon pour le stockage des éléments de travail reconnus. Chaque élément de travail reconnu correspond à un résultat de reconnaissance enregistré dans la base de données.

Ne définissez pas cette propriété sur une valeur inférieure au nombre d'unités d'exécution d'écriture dans la base de données spécifié dans la propriété `com.collation.discover.topopumpcount`.

com.ibm.cdb.discover.buffers.statistics.interval.seconds=60
La valeur par défaut est `60`. Spécifiez la valeur en secondes.

Cette propriété spécifie la valeur temporelle pour l'enregistrement des statistiques de mémoire tampon de reconnaissance dans un journal. Le journal se trouve dans le répertoire `/log/services/DiscoveryState.log`.

com.ibm.cdb.discover.buffers.timeout.interval.seconds=600
La valeur par défaut est `600`, ce qui correspond à 10 minutes. Spécifiez la valeur en secondes.

Cette propriété spécifie la valeur temporelle pour la vérification du délai d'attente des éléments de travail.

com.ibm.cdb.discover.runcontroller.statistics.interval.seconds=60
La valeur par défaut est `60`. Spécifiez la valeur en secondes.

Cette propriété spécifie la valeur temporelle pour l'enregistrement des statistiques de mémoire tampon de reconnaissance dans un journal. Le journal se trouve dans le répertoire `/log/services/DiscoveryRunController.log`.

com.ibm.cdb.discover.runrestartlimit=11
La valeur par défaut est `11`.

Cette propriété spécifie le nombre de redémarrages autorisé après un échec pour les reconnaissances non initialisées. La reconnaissance se trouve dans un état non initialisé lorsque le processus n'a pas démarré pour tous les éléments de la portée de reconnaissance.

com.collation.discovery.oracle.tablelimit=1000
La valeur par défaut est `1000`. La propriété prend en charge uniquement les valeurs positives.

Cette propriété contrôle la quantité de données des tables reconnues par le détecteur Oracle.

Propriétés de reconnaissance simultanée :

Ces propriétés s'appliquent à la reconnaissance simultanée.

com.collation.discover.concurrent.discovery=true
La valeur par défaut est définie sur `true`.

Cette propriété est utilisée pour activer la reconnaissance simultanée.

com.collation.discover.max.concurrent.discoveries=10
La valeur par défaut est `10`.

Cette propriété définit le nombre maximal de reconnaissances simultanées.

Propriétés de la reconnaissance asynchrone :

Ces propriétés s'appliquent à la reconnaissance asynchrone.

com.ibm.cdb.discover.asd.AsyncDiscoveryResultsDirectory=var/asdd
La valeur par défaut est `var/asdd`, qui est relatif au répertoire `com.collation.home`.

Cette propriété définit l'emplacement du répertoire racine des fichiers archive contenant les résultats de la reconnaissance asynchrone sur le serveur TADDM. L'emplacement peut être un chemin relatif ou absolu. Un chemin relatif au répertoire `com.collation.home`.

com.ibm.cdb.discover.asd.ProcessUnreachableIPs=false
La valeur par défaut est `false`.

Cette propriété est utilisée pour activer le traitement des adresses IP inaccessibles qui sont utilisées lors d'une reconnaissance asynchrone. Pour activer le traitement de ces adresses, définissez la valeur sur `TRUE`.

com.ibm.cdb.tarpath=tar
La valeur par défaut est `tar`.

Cette propriété spécifie le chemin de la commande **tar** *sur le serveur TADDM* dans une reconnaissance asynchrone.

Sur les systèmes d'exploitation tels qu'AIX ou Linux, cette propriété n'est généralement pas nécessaire car la commande **TAR** est déjà installée et disponible. Pour générer un package de script de reconnaissance asynchrone ou pour traiter les fichiers archive de reconnaissance sur un serveur TADDM qui exécute le système d'exploitation Windows, vous devez cependant installer un programme tar tiers et indiquer le nom de chemin complet de ce programme.

L'exemple suivant montre comment indiquer le chemin de la commande **tar** sur le serveur TADDM qui exécute le système d'exploitation AIX :

```
com.ibm.cdb.tarpath=tar
```

com.ibm.cdb.targettarpath=tar
La valeur par défaut est `tar`.

Cette propriété définit le chemin de la commande **TAR** sur le système cible lors d'une reconnaissance asynchrone.

Sur les systèmes d'exploitation cible tels qu'AIX ou Linux, cette propriété n'est généralement pas nécessaire car la commande **TAR** est déjà installée et

disponible. Toutefois, pour générer des fichiers d'archive de reconnaissance, sur les systèmes d'exploitation Solaris, en raison d'une limitation relative à la longueur des noms de fichier, vous devez utiliser l'utilitaire d'archivage gtar et spécifier le chemin d'accès à cet utilitaire.

Les exemples suivants montrent comment spécifier le chemin de la commande **tar** *sur le système cible*, en fonction du système d'exploitation :

Pour AIX

```
com.ibm.cdb.targettarpath.AIX=tar
```

Pour Solaris

```
com.ibm.cdb.targettarpath.SunOS=/usr/sfw/bin/gtar
```

Propriétés de la reconnaissance dépendante d'un script :

Ces propriétés s'appliquent à la reconnaissance dépendante d'un script.

Fix Pack 4 **com.ibm.cdb.discover.enableOutputFileSplittingProcess=true**
La valeur par défaut est `true`.

Cette propriété indique si le fichier de sortie principal qui est créé pendant une reconnaissance dépendante d'un script doit être fractionné en fichiers plus petits. Le fractionnement est le paramètre par défaut. Ce paramètre évite les problèmes de performance qui peuvent survenir lorsque le fichier de sortie est volumineux. Reportez-vous également la propriété `com.ibm.cdb.discover.numberOfLinesForOutputFileSplittingProcess`.

Fix Pack 4
com.ibm.cdb.discover.numberOfLinesForOutputFileSplittingProcess=10000
La valeur par défaut est `10000`.

Cette propriété est utilisée uniquement lorsque la propriété `com.ibm.cdb.discover.enableOutputFileSplittingProcess` est définie sur `true`.
Cette propriété indique le nombre de lignes approximatif autorisé dans les petits fichiers de sortie qui ont été créés en fractionnant le fichier de sortie principal. Le nombre de lignes exact est déterminé par le format du fichier. Après le nombre de lignes spécifié, le fichier est fractionné seulement lorsque la fin de l'ensemble de données signicatif est atteinte afin de garantir que le format du fichier entier est correct. Cela signifie que lorsque la valeur est définie sur `10000`, les fichiers plus petits peuvent compter, par exemple, 10200 lignes.

com.ibm.cdb.taddm.asd.prefix=sh
La valeur par défaut est `sh`.

Cette propriété spécifie le préfixe à ajouter au script exécuté pendant une reconnaissance, par exemple *préfixe* `script.sh`. Cette propriété est une propriété sectorisée. Vous pouvez lui ajouter une adresse IP ou le nom d'un ensemble de portées.

com.ibm.cdb.discover.DeleteScriptDiscoveryOutputs=true
La valeur par défaut est `true`.

Cette propriété définit s'il faut supprimer la sortie du script qui, au cours de la reconnaissance basée sur un script, est copiée sur le serveur TADDM afin d'être traitée par les détecteurs. Cette sortie peut être utile pour l'identification et la résolution des problème, mais elle est par défaut

supprimée lorsque la reconnaissance est terminée. Si vous définissez la valeur de cette propriété sur `false`, la sortie du script ne sera pas supprimée.

com.ibm.cdb.discover.DeleteRemoteBeforeScriptsRun=`false`
La valeur par défaut est `false`.

Cette propriété indique si TADDM supprime du répertoire distant toutes les entrées qui ont été laissées par la reconnaissance précédente, avant de tenter d'exécuter une nouvelle reconnaissance.

com.ibm.cdb.discover.PreferScriptDiscovery=`false`
La valeur par défaut est `false`.

Cette propriété permet d'activer la reconnaissance basée sur un script. Elle concerne uniquement les détecteurs qui prennent en charge ce type de reconnaissance. Lorsque vous définissez cette valeur sur `true`, la reconnaissance basée sur un script est activée.

com.ibm.cdb.discover.smallFileSizeLimit=`1048576`
La valeur par défaut est `1048576` (1024*1024 - 1 Mo).

Cette propriété définit la limite de la taille du fichier exprimée en octets pour des opérations de copie qui déclenchent l'utilisation du total de contrôle. Les fichiers dont la taille est en dessous de cette limite sont copiés sans les calculs des totaux de contrôle. Les fichiers dont la taille est égale ou supérieure à la limite ne sont copiés que s'ils ne sont pas présents dans le répertoire cible et que leur total de contrôle ne correspond pas au fichier (source) local.

Vous pouvez désactiver la limite en utilisant les valeurs suivantes :

- `0` - l'opération de copie utilise toujours le total de contrôle.
- `-1` - l'opération de copie évite toujours d'utiliser le total de contrôle.

Propriétés de la reconnaissance à l'aide d'IBM Tivoli Monitoring (ancienne méthode) :

Ces propriétés s'appliquent à la reconnaissance avec IBM Tivoli Monitoring (ancienne méthode).

Ancienne méthode d'intégration

Cette section s'applique à une méthode obsolète d'intégration de TADDM à IBM Tivoli Monitoring. A partir de TADDM version 7.3.0, il est recommandé d'effectuer l'intégration à IBM Tivoli Monitoring 6.3 via une automatisation OSLC. L'ancienne méthode d'intégration à l'aide d'un détecteur IBM Tivoli Monitoring Scope est obsolète et sera retirée des prochaines éditions. Pour plus d'informations sur les propriétés utilisées pour configurer le processus de reconnaissance à l'aide de l'automatisation OSLC, voir «Intégration de TADDM à IBM Tivoli Monitoring via une automatisation OSLC», à la page 202 et «Propriétés pour une reconnaissance via une session d'automatisation OSLC», à la page 86.

Propriétés affectant la façon dont TADDM reconnaît des noeuds finaux Tivoli Monitoring

La reconnaissance TADDM de niveau 2 et 3 requiert normalement un serveur de domaine (dans un déploiement de serveur de domaine ou de synchronisation) ou

un serveur de reconnaissance (dans un déploiement de serveur de diffusion en continu) pour se connecter directement à un système cible de l'une des façons suivantes :

- Secure Shell (SSH) pour les systèmes cible basés UNIX
- Windows Management Instrumentation (WMI) pour les systèmes Windows

Pour utiliser ces méthodes, le serveur de domaine ou de reconnaissance doivent connaître les données d'identification de l'utilisateur (compte et mot de passe).

La reconnaissance avec IBM Tivoli Monitoring permet à TADDM de reconnaître des informations de niveau 2 (et certaines de niveau 3) sur les systèmes cible pour lesquels aucune donnée d'identification de l'utilisateur n'est disponible. Les détecteurs s'exécutent via l'infrastructure Tivoli Monitoring, et seules les données d'identification de Tivoli Enterprise Portal Server sont requises. Une fois le détecteur IBM Tivoli Monitoring Scope configuré et exécuté, les reconnaissances ultérieures de niveau 2 se servent par défaut de Tivoli Monitoring. Si vous ne souhaitez pas ce comportement par défaut dans votre environnement, TADDM fournit les propriétés de serveur suivantes pour vérifier si la reconnaissance se fait via Tivoli Monitoring ou une connexion directe (SSH ou WMI). Ces propriétés peuvent être définies à un niveau global ou pour une portée ou un profil de reconnaissance spécifique.

com.ibm.cdb.session.allow.ITM=true
: La valeur par défaut est `true`, ce qui signifie que TADDM peut utiliser IBM Tivoli Monitoring pour reconnaître des noeuds finaux Tivoli Monitoring.

  Cette propriété détermine si TADDM peut utiliser IBM Tivoli Monitoring pour reconnaître des noeuds finaux Tivoli Monitoring.

  Pour se connecter directement à un noeud final Tivoli Monitoring, définissez la valeur à `false`.

  Vous pouvez aussi utiliser cette propriété pour indiquer une portée de reconnaissance personnalisée, comme indiqué dans l'exemple suivant :

  com.ibm.cdb.session.allow.ITM.*adresse_ip*=false
  : L'exemple suivant indique que TADDM se sert de la portée de reconnaissance `10.20.30.40` et se connecte directement au noeud final, même s'il est surveillé par Tivoli Monitoring :

    ```
    com.ibm.cdb.session.allow.ITM.10.20.30.40=false
    ```

com.ibm.cdb.session.prefer.ITM=true
: La valeur par défaut est `true`, ce qui signifie que TADDM utilise IBM Tivoli Monitoring pour reconnaître des noeuds finaux Tivoli Monitoring.

  Cette propriété indique si TADDM utilise IBM Tivoli Monitoring comme méthode de prédilection pour la reconnaissance de noeuds finaux Tivoli Monitoring, à condition que ce mode de reconnaissance soit autorisé pour les noeuds finaux. Si TADDM se sert d'IBM Tivoli Monitoring pour la reconnaissance et que celle-ci échoue, il établit une connexion directe aux noeuds finaux. De la même façon, si la reconnaissance avec IBM Tivoli Monitoring n'est pas celle préférée et que la connexion directe aux noeuds finaux échoue, TADDM tente de se connecter aux noeuds finaux à l'aide d'IBM Tivoli Monitoring, à condition une fois encore que ce mode de reconnaissance soit autorisé pour les noeuds finaux.

  Vous pouvez aussi utiliser cette propriété pour indiquer une portée de reconnaissance personnalisée, comme indiqué dans l'exemple suivant :

com.ibm.cdb.session.prefer.ITM.*adresse_ip*=false
L'exemple suivant indique que TADDM utilise la portée de reconnaissance 10.20.30.40 et se connecte directement aux noeuds finaux Tivoli Monitoring :

```
com.ibm.cdb.session.prefer.ITM.10.20.30.40=false
```

com.ibm.cdb.session.prefer.ITM.Level_3_Discovery=false
La valeur par défaut est false, ce qui signifie que TADDM se connecte directement aux noeuds finaux Tivoli Monitoring si vous utilisez un profil de reconnaissance de niveau 3 ; pour les autres niveaux de reconnaissance, TADDM utilise IBM Tivoli Monitoring pour reconnaître les noeuds finaux Tivoli Monitoring, en fonction des valeurs des propriétés suivantes :

- **com.ibm.cdb.session.allow.ITM**
- **com.ibm.cdb.session.prefer.ITM**

Cette propriété indique si TADDM utilise IBM Tivoli Monitoring pour reconnaître des noeuds finaux Tivoli Monitoring en cas d'utilisation d'un profil de reconnaissance de niveau 3.

Si vous définissez la valeur à true, TADDM peut utiliser IBM Tivoli Monitoring pour reconnaître les noeuds finaux Tivoli Monitoring à partir d'un profil de reconnaissance de niveau 3.

Propriétés pour améliorer la connexion entre le serveur TADDM et le serveur de portail

Pour une reconnaissance de niveau 2 avec IBM Tivoli Monitoring, TADDM utilise les propriétés suivantes du serveur TADDM afin d'améliorer le comportement de reprise de connexion si la connexion entre le serveur TADDM et Tivoli Enterprise Portal Server est décalée :

com.collation.discover.agent.ITM.CmdWrapperSelectionPattern=
Cette propriété indique les commandes à insérer dans un script lors de l'exécution d'une reconnaissance via un environnement IBM Tivoli Monitoring.

com.collation.platform.session.ITMSessionConnectionCooldownPeriod=60000
Cette propriété indique l'intervalle en millisecondes avant que la connexion à Tivoli Enterprise Portal Server ne soit réinitialisée après la détection d'un échec.

com.collation.platform.session.ITMSessionConnectionRetryLimit=5
Cette propriété indique le nombre de tentatives d'accès à une connexion si la connexion initiale échoue avant de signaler une erreur.

com.collation.platform.session.ITMSessionNumProgressChecks=600
Cette propriété indique le nombre de fois que la progression d'une connexion est vérifiée avant que la connexion échoue.

com.collation.platform.session.ITMSessionProgressCheckInterval=1000
Cette propriété indique l'intervalle en millisecondes entre chaque vérification de la progression d'une connexion.

Propriétés pour une reconnaissance via une session d'automatisation OSLC :

Ces propriétés s'appliquent à une reconnaissance via une session d'automatisation OSLC.

Propriétés liées à une intégration sur OSLC

com.ibm.cdb.topobuilder.integration.oslc.automationprovider
Cette propriété indique des adresses URL directes des fournisseurs de services d'automatisation d'exécution OSLC qui ne sont pas enregistrés dans les services de registre de Jazz SM.

L'exemple suivante montre des adresses URL du fournisseur de services d'automatisation d'exécution OSLC pour ITM :

```
com.ibm.cdb.topobuilder.integration.oslc.automationprovider=
http://<HOTE_INSTALLATION_FOURNISSEUR_SERVICES_AUTOMATISATION>:15210/itmautomationprovider
```

L'exemple suivant montre comment spécifier des adresses URL pour plusieurs fournisseurs de services d'automatisation d'exécution OSLC :

```
com.ibm.cdb.topobuilder.integration.oslc.automationprovider.1=
http://9.1.1.1:15210/itmautomationprovider
com.ibm.cdb.topobuilder.integration.oslc.automationprovider.2=
http://9.2.2.2:15210/itmautomationprovider
```

com.ibm.cdb.topobuilder.integration.oslc.automation.scope.alwaysrefresh=false
La valeur par défaut est `false`.

Cette propriété est une propriété globale qui indique si l'agent OSLCAutomationAgent régénère des ensembles de portées lors de chacune des exécutions. La régénération des ensembles de portées nécessite une connexion aux services de registre dans Jazz SM ou aux fournisseurs de services d'automatisation d'exécution OSLC, ou aux deux.

Si vous avez défini cette propriété à `true`, l'agent régénère l'ensemble de portées, même si le plan d'automatisation fourni par le fournisseur de services d'automatisation d'exécution OSLC ne change pas depuis la dernière exécution de l'agent.

com.ibm.cdb.topobuilder.integration.oslc.frsurl
Cette propriété indique l'adresse IP des services de registre de Jazz SM qui est utilisée dans une intégration à d'autres produits sur OSLC. Le format de l'adresse des services de registre de Jazz SM doit être le suivant :

```
protocol://ip_ou_nomhôte:port
```

Cette propriété est également utilisée par l'agent OSLCAgent.

com.ibm.cdb.topobuilder.integration.oslc.automation.frsurl
Cette propriété indique l'adresse IP sous la forme d'un chemin d'accès complet à la collection d'enregistrements des services de registre de Jazz SM (FRS). Elle peut être utilisée si des services de registre de Jazz SM utilisent d'autres services que ceux par défaut `/oslc`.

Propriétés liées à une reconnaissance via une session d'automatisation

com.ibm.cdb.session.oslcautomation.pluginId=com.ibm.cdb.session.oslcautomation_1.0.0
La valeur par défaut est `com.ibm.cdb.session.oslcautomation_1.0.0`.

Cette propriété spécifie l'ID du bundle OSGi du module d'extension de la session d'automatisation OSLC.

com.ibm.cdb.session.itm.endpointClass=com.collation.platform.session.oslcautomation.OSLCAutomationEndpoint
La valeur par défaut est `com.collation.platform.session.oslcautomation.OSLCAutomationEndpoint`.

Cette propriété spécifie la classe du noeud final à utiliser.

com.ibm.cdb.session.allow.OSLCAutomation=true
La valeur par défaut est définie sur `true`.

Cette propriété est une propriété de portée qui indique si TADDM peut utiliser une session d'automatisation OSLC pendant la reconnaissance.

Exemple d'utilisation :

```
com.ibm.cdb.session.allow.OSLCAutomation=true
com.ibm.cdb.session.allow.OSLCAutomation.9.100.1.0=true
com.ibm.cdb.session.allow.OSLCAutomation.scope_set2=true
```

com.ibm.cdb.session.prefer.OSLCAutomation=true
La valeur par défaut est définie sur `true`.

Cette propriété est une propriété de portée qui indique si une session d'automatisation est une session préférée pour une reconnaissance. La valeur de propriété a priorité sur toute autre valeur préférée, comme une session ITM standard.

Exemple d'utilisation :

```
com.ibm.cdb.session.prefer.OSLCAutomation=true
com.ibm.cdb.session.prefer.OSLCAutomation.9.100.100.200=true
com.ibm.cdb.session.prefer.OSLCAutomation.scope_name1=true
```

com.ibm.cdb.session.oslcautomation.timeout.httpconnect=60000
La valeur par défaut est `60000` (60 secondes). La valeur est exprimée en millisecondes.

Cette propriété est une propriété globale qui spécifie un délai d'attente pour la connexion au fournisseur de services d'automatisation d'exécution OSLC.

com.ibm.cdb.session.oslcautomation.timeout.httpread=240000
La valeur par défaut est `240000` (4 minutes). La valeur est exprimée en millisecondes.

Cette propriété est une propriété globale qui spécifie un délai d'attente pour la lecture de données à partir du fournisseur de services d'automatisation d'exécution OSLC.

com.ibm.cdb.session.oslcautomation.request.async.maxretries=60
La valeur par défaut est `60`.

Cette propriété est une propriété qui spécifie le nombre maximum de requêtes consécutives pour des résultats d'automatisation AutomationResults générés en mode asynchrone.

com.ibm.cdb.session.oslcautomation.request.async.delay=10000
La valeur par défaut est `10000` (10 secondes). La valeur est exprimée en millisecondes.

Cette propriété est une propriété qui spécifie le retard entre des requêtes consécutives pour des résultats d'automatisation AutomationResults générés en mode asynchrone.

Remarque : Fix Pack 4 Dans le cas où la session SSH vers le serveur échoue en raison de problèmes de délai d'attente, essayez de configurer une valeur optimale pour la propriété ci-dessous :

com.collation.mindterm.Ssh2Preferences= hello-timeout=30; alive = 25; compression= 9

com.collation.discover.agent.app.packagedapp.mysap.SLDServerPortList = 51200
Cette propriété permet de changer le port SLD et le port spécifié doit être ajouté à la configuration du capteur.

com.ibm.cdb.security.auth.cache.itm.disabled=true
La valeur par défaut est définie sur `true`.

Cette propriété détermine si la mise en cache des données d'identification d'accès est désactivée pour la reconnaissance OSLC.

Il s'agit d'une propriété sectorisée et profilée. Vous pouvez ajouter une adresse IP, le nom d'un ensemble de portées ou un nom de profil. Vous pouvez également la définir dans la configuration des profils, dans Discovery Management Console.

Propriétés de personnalisation des recherches DNS

Ces propriétés s'appliquent à la personnalisation des recherches DNS

com.collation.platform.os.disableDNSLookups=false
La valeur par défaut est `false`.

Les valeurs valides sont `true` ou `false`. Si vous définissez la propriété sur `true`, les recherches DNS sont désactivées sur le serveur TADDM.

com.collation.platform.os.disableRemoteHostDNSLookups=false
La valeur par défaut est `false`.

Les valeurs valides sont `true` ou `false`. Si vous indiquez la valeur `true`, les recherches de nom (DNS uniquement) sont désactivées sur les systèmes hôte reconnus éloignés. Cette propriété force toutes les recherches par nom à se produire sur le même serveur TADDM.

com.collation.platform.os.command.fqdn=nslookup $1 | grep Name | awk '{print $2}'
La valeur par défaut est `nslookup $1 | grep Name | awk '{print $2}'`.

Cette commande permet de rechercher le nom de domaine complet. Dans la plupart des situations, cette propriété n'est pas nécessaire car l'algorithme du nom de domaine qualifié (FQDN) fonctionne dans la plupart des environnements de production. Si cette propriété n'est pas nécessaire, vous devez la mettre en commentaire. En revanche, dans les environnements où le nom de domaine complet doit être dérivé du nom d'hôte, vous souhaiterez probablement activer cette propriété. Par exemple, activez cette propriété si les noms d'hôte sont configurés comme alias dans le système de nom de domaine.

Si vous utilisez cette propriété, assurez-vous que le système de nom de domaine est disponible et correctement configuré. A défaut, la commande **nslookup** risque d'échouer ou d'avoir un temps de réponse très long.

Si cette propriété est activée, elle est uniquement utilisée sur le serveur TADDM. Actuellement, seuls les systèmes d'exploitation AIX et Linux sont pris en charge. Cette propriété n'est pas prise en charge par un serveur TADDM Windows.

Propriétés de l'interface graphique

Ces propriétés s'appliquent à l'interface graphique TADDM.

Fix Pack 3 **com.ibm.cdb.gui.supportedJRE.warning=true**
Cette propriété indique si le message d'avertissement CTJTG0034E s'affiche au démarrage de la console de gestion de reconnaissance. Ce message vous avertit que votre version de l'environnement d'exécution Java n'est pas

prise en charge. Pour utiliser TADDM avec la version non prise en charge de l'environnement d'exécution Java et pour ne plus afficher ce message, définissez cette propriété sur `false`.

La valeur par défaut de cette propriété est `true`.

Propriétés de la mémoire de la machine JVM de l'interface graphique :

Ces propriétés s'appliquent à la mémoire de la machine JVM de l'interface graphique.

com.collation.gui.initial.heap.size=128m

La valeur par défaut est `128m`.Taille initiale de la pile pour l'interface utilisateur TADDM.

com.collation.gui.max.heap.size=512m

La valeur par défaut est `512m`.Taille maximale de la pile pour l'interface utilisateur de TADDM.

Ces paramètres sont appropriés pour un domaine TADDM de petite taille. Pour le redimensionnement, les catégories suivantes de serveurs TADDM sont utilisées (en fonction des équivalents des serveurs) :

- Petit : jusqu'à 1000 équivalents de serveurs
- Moyen : de 1000 à 2500 équivalents de serveur
- Grand : de 2500 à 5000 équivalents de serveur

L'augmentation de ces valeurs pour les environnements moyens et les grands environnements améliore les performances de certaines opérations de l'interface graphique. Certaines vues n'apparaissent pas correctement si la mémoire affectée à TADDM est insuffisante au moment de l'action.

Pour un environnement moyen :

com.collation.gui.initial.heap.size=256m

La valeur par défaut est `256m`.

com.collation.gui.max.heap.size=768m

La valeur par défaut est `768m`.

Pour un environnement grand :

com.collation.gui.initial.heap.size=512m

La valeur par défaut est `512m`.

com.collation.gui.max.heap.size=1024m

La valeur par défaut est `1024m`.

Propriétés des ports de l'interface graphique :

Ces propriétés s'appliquent aux ports de l'interface graphique.

com.collation.tomcatshutdownport=9436 (TADDM 7.3.0 uniquement)
La valeur par défaut est `9436`.

Port utilisé par la commande d'arrêt Tomcat.

com.ibm.cdb.service.web.port=9430
La valeur par défaut est 9430.

Port HTTP utilisé sans couche SSL.

com.ibm.cdb.service.web.secure.port=9431
La valeur par défaut est 9431.

Port HTTP utilisé avec couche SSL.

com.ibm.cdb.service.ClientProxyServer.port=9435
La valeur par défaut est 9435.

Point d'accès RMI à utiliser sans couche SSL.

com.ibm.cdb.service.SecureClientProxyServer.secure.port=9434
La valeur par défaut est 9434.

Point d'accès RMI à utiliser avec couche SSL.

com.ibm.cdb.service.registry.public.port=9433
La valeur par défaut est 9433.

Port de registre de services.

Propriétés LDAP

Ces propriétés s'appliquent à LDAP.

Il est possible d'utiliser un serveur LDAP externe pour l'authentification des utilisateurs. Avec un serveur LDAP externe, l'authentification anonyme et l'authentification par mot de passe sont prises en charge.

Vous pouvez configurer le nom d'hôte, le numéro de port, le nom distinctif de base, le nom distinctif de liaison et le passe de passe (obligatoire pour l'authentification par mot de passe) du serveur LDAP dans le fichier `collation.properties`. Vous pouvez aussi configurer l'attribut de dénomination spécifique qui peut faire l'objet d'une recherche pour qu'il corresponde à l'ID d'utilisateur (UID).

La configuration LDAP est recommandée pour les déploiements de serveurs de synchronisation et de serveurs de domaine. Dans un environnement d'entreprise, configurez le serveur de domaine et le serveur de synchronisation de telle sorte qu'ils utilisent le même registre d'utilisateurs. Lorsque vous vous connectez à un serveur de domaine connecté à un serveur de synchronisation, la connexion est traitée par le serveur de synchronisation. Si un problème de connexion réseau se produit entre les deux serveurs, vous pouvez vous connecter au serveur de domaine sans procéder à une reconfiguration si le serveur de domaine est configuré de sorte à utiliser le même registre d'utilisateurs que le serveur de synchronisation.

com.collation.security.auth.ldapAuthenticationEnabled=true
La valeur par défaut est définie sur `true`.

Cette propriété est utilisée pour activer l'authentification LDAP.

com.collation.security.auth.ldapBaseDN=ou=People,dc=ibm,dc=com
La valeur par défaut est `ou=people,dc=ibm,dc=com`.

Cette propriété définit le nom distinctif de base LDAP. Le nom distinctif de base LDAP est le point de départ de toutes les recherches LDAP.

com.collation.security.auth.ldapBaseGroupDN
Dans le fichier `collation.properties`, cette propriété est mise en commentaire par défaut.

Cette propriété définit la branche racine de LDAP pour la recherche dans les groupes, qui peut être différente de la branche racine de toutes les requêtes LDAP. Pour indiquer plusieurs branches racine LDAP pour rechercher des groupes, séparez-les par le caractère «;».

Si vous n'indiquez pas de valeur pour cette propriété, la valeur par défaut est la valeur de la propriété `com.collation.security.auth.ldapBaseDN`.

com.collation.security.auth.ldapBindDN=uid=ruser,dc=ibm,dc=com
La valeur par défaut est `uid=people,dc=ibm,dc=com`.

Si une authentification simple est utilisée, cette propriété définit l'identifiant d'utilisateur employé pour s'authentifier à LDAP.

Important :

- Si aucune valeur n'est fournie pour `com.collation.security.ldapBindDN` ou que la propriété est ignorée, une connexion anonyme au protocole LDAP est tentée. L'exemple suivant montre comment la propriété peut être mise en commentaire à l'aide du signe dièse (#) :

  ```
  #com.collation.security.auth.ldapBindDN=uid=ruser,
  dc=ibm,dc=com
  ```

- Si une valeur est indiquée pour `com.collation.security.auth.ldapBindDN`, l'authentification simple est utilisée et
- une valeur pour `com.collation.security.auth.ldapBindPassword` doit aussi être entrée.

com.collation.security.auth.ldapBindPassword=ruser
La valeur par défaut est `ruser`.

Si l'authentification simple est utilisée, cette propriété définit le mot de passe de l'utilisateur employée pour s'authentifier à LDAP.

com.collation.security.auth.ldapClientKeyStore=*ks_path*
Cette propriété définit l'emplacement du fichier de clés qui contient les certificats sur le serveur TADDM. Le fichier doit contenir le certificat client pour authentifier le serveur TADDM avec le serveur LDAP.

com.collation.security.auth.ldapClientKeyStorePassphrase=*ks_passphrase*
Facultatif : cette propriété définit le mot de passe du fichier de clés.

com.collation.security.auth.ldapClientTrustStore=*ts_path*
Cette propriété définit l'emplacement du fichier de clés certifiées qui contient les certificats sur le serveur TADDM server. Le fichier doit contenir le certificat du serveur LDAP.

com.collation.security.auth.ldapClientTrustStorePassphrase=*ts_passphrase*
Facultatif : cette propriété définit le mot de passe du fichier de clés certifiées.

com.collation.security.auth.ldapGroupMemberAttribute=membre
La valeur par défaut est `membre`.

Cette propriété définit le nom de l'attribut utilisé pour contenir les membres d'un groupe dans le protocole LDAP.

com.collation.security.auth.ldapGroupNamingAttribute=cn
La valeur par défaut est `cn`.

Cette propriété définit le nom de l'attribut utilisé pour nommer les groupes dans le protocole LDAP.

com.collation.security.auth.ldapGroupObjectClass=groupe_noms
La valeur par défaut est `groupe_noms`.

Cette propriété définit la classe utilisée pour représenter les groupes d'utilisateurs dans le protocole LDAP.

com.collation.security.auth.ldapHostName=ldap.ibm.com
La valeur par défaut est `ldap.ibm.com`.

Cette propriété définit le nom d'hôte du serveur LDAP.

com.collation.security.auth.ldapPortNumber=389
La valeur par défaut est `389`.

Cette propriété définit le port du serveur LDAP.

com.collation.security.auth.ldapUIDNamingAttribute=numéro_identification_utilisateur
La valeur par défaut est `numéro_identification_utilisateur`.

Cette propriété définit le nom de l'attribut utilisé pour nommer les utilisateurs dans le protocole LDAP.

com.collation.security.auth.ldapUserObjectClass=person
La valeur par défaut est `person`.

Cette propriété définit le nom de la classe utilisée pour représenter les utilisateurs dans le protocole LDAP.

com.collation.security.auth.ldapUseSSL=false
La valeur par défaut est `false`.

Cette propriété est utilisée pour activer l'authentification sur un registre d'utilisateurs de serveur LDAP avec une connexion SSL.

com.collation.security.usermanagementmodule=ldap
La valeur par défaut est `ldap`.

Cette propriété définit le module de gestion utilisateur employé par le serveur TADDM. Les valeurs valides sont :

- `file` pour un registre d'utilisateurs basé sur les fichiers. La valeur par défaut est true.
- `ldap` pour un registre d'utilisateurs LDAP.
- `vmm` pour un registre d'utilisateurs utilisant les répertoires fédérés de WebSphere Application Server

Propriétés de verrouillage

Ces propriétés s'appliquent aux verrouillages.

com.collation.security.lockout.treshold=3
La valeur par défaut est `3`.

Cette propriété indique le nombre de tentatives de connexion d'un utilisateur spécifique après lequel un verrouillage se déclenche pour l'utilisateur.

com.collation.security.lockout.timeout=30
La valeur par défaut est `30`.

Cette propriété indique la durée, en minutes, pendant laquelle l'utilisateur qui a déclenché le verrouillage local n'a plus accès à TADDM.

com.collation.security.lockout.globalthreshold=100
La valeur par défaut est 100.

Cette propriété indique le nombre de verrouillages individuels simultanés qui déclenche un verrouillage général.

com.collation.security.lockout.globaltimeout=30
La valeur par défaut est 30.

Cette propriété indique la durée, en minutes, pendant laquelle tous les utilisateurs n'ont plus accès à TADDM lorsqu'un verrouillage général se déclenche.

com.collation.security.lockout.failedloginthreshold=1000
La valeur par défaut est 1000.

Cette propriété indique le nombre de tentatives de connexion d'utilisateurs individuels après lequel un verrouillage général se déclenche.

Propriétés de consignation

Ces propriétés s'appliquent à la consignation.

com.collation.log.filesize=20MB
La valeur par défaut est 20MB.

Taille maximale du fichier journal. Lorsque le fichier atteint cette limite, un nouveau fichier journal est créé. Le fichier actuel est alors sauvegardé avec l'extension *.N*. *N* est une valeur comprise entre 1 et le nombre défini dans la propriété **com.collation.log.filecount**. La propriété **com.collation.log.filecount** permet de définir le nombre de fichiers journaux pouvant être créés et conservés avant la rotation des fichiers.

Vous pouvez saisir le nombre d'octets directement ou indiquer le nombre de kilooctets ou de mégaoctets à l'aide des symboles Ko et Mo, respectivement.

Les exemples suivants sont des valeurs de taille de fichier journal valides :

- 1000000
- 512 Ko
- 10 Mo

com.collation.log.filecount=5
La valeur par défaut est 5.

Nombre de fichiers journaux conservés.

com.collation.log.level.vm.*vmName*=INFO
La valeur par défaut est INFO.

Définit le niveau de consignation pour chaque système virtuel.

vmName est un système virtuel Java associé à un nom de service TADDM. Les autres options valides sont classées ci-dessous :

- Topologie
- DiscoverAdmin
- EventsCore
- Proxy
- Reconnaissance
- EcmdbCore
- StorageService

- DiscoveryService

Les autres options valides sont classées ci-dessous :

- FATAL
- ERROR
- WARNING
- INFO
- DEBUG (L'option DEBUG réduit les performances du système.)
- TRACE (L'option TRACE entraîne la consignation des mots de passe.)

Propriétés des performances

Ces propriétés s'appliquent aux performances TADDM.

com.collation.discover.dwcount=32

La valeur par défaut est 32. Il doit s'agir d'un entier.

Cette propriété affecte le taux de reconnaissance. Une unité d'exécution de reconnaissance est une unité d'exécution qui exécute des détecteurs. Cette propriété indique le nombre d'unités d'exécution de tâche qui peuvent s'exécuter simultanément et s'applique uniquement à un serveur de reconnaissance dans un déploiement de serveur de diffusion ou à un serveur de domaine dans un déploiement de serveur de domaine.

Pour la reconnaissance à l'aide d'IBM Tivoli Monitoring (ancienne méthode qui utilise un détecteur de portée IBM Tivoli Monitoring), la valeur doit être 16. Pour tous les autres types de reconnaissance, la plage de valeurs valides est de 32 à 160.

com.collation.discover.observer.topopumpcount=16

La valeur par défaut est 16. Il doit s'agir d'un entier.

Cette propriété affecte la vitesse de stockage des résultats de reconnaissance dans la base de données TADDM. Elle indique le nombre d'unités d'exécution d'écriture créées pour la communication avec la base de données TADDM.

Pour un serveur de reconnaissance dans un déploiement de serveur de diffusion, cette propriété contrôle le nombre d'unités d'exécution que le serveur de reconnaissance utilise pour envoyer les résultats de reconnaissance au pool de serveurs de stockage.

Pour un serveur de stockage dans un déploiement de serveur de diffusion, cette propriété contrôle le nombre d'unités d'exécution qui reçoivent les résultats de reconnaissance des serveurs de reconnaissance.

Pour un serveur de domaine dans un déploiement de serveur de domaine, cette propriété contrôle le nombre d'unités d'exécution qui reçoivent les résultats de reconnaissance des unités d'exécution de tâche de reconnaissance.

Les unités d'exécution utilisent ensuite une connexion de base de données du pool de connexion pour communiquer avec la base de données TADDM (par exemple, pour enregistrer des résultats et récupérer des données). Si aucune connexion JDBC de pool n'existe, l'unité d'exécution crée une connexion non regroupée en pool.

com.ibm.cdb.discover.observer.topopump.threshold=0,7
com.ibm.cdb.discover.observer.topopump.threshold.*nom_gpe_agent_topo_agent*=0.7

La valeur par défaut est 0,7. La valeur doit être une constante flottante.

Cette propriété indique le nombre d'unités d'exécution d'écriture de base de données que vous pouvez démarrer lorsque les agents de topologie sont en cours d'exécution. Vous pouvez indiquer une valeur de seuil pour un groupe d'agents spécifique ou pour tous les agents à la fois. Si vous ne spécifiez aucune valeur pour le groupe d'agents, la valeur de seuil générale est utilisée. Cette valeur permet de limiter le nombre d'unités d'exécution qui enregistrent les résultats de reconnaissance dans la base de données TADDM lorsque les agents de topologie sont en cours d'exécution.

com.ibm.cdb.typesServiceRefreshInterval=120
La valeur par défaut est `120`. La valeur minimale est `30` la valeur maximale `1800`.

Cette propriété définit, en secondes, l'intervalle d'actualisation nécessaire à la mise à jour des types de composant lors de la création d'une requête personnalisée, de l'affichage de l'historique des changements ou des informations de comparaison des composants.

com.ibm.cdb.ea.metaRefreshFrequency=20
La valeur par défaut est `20`. Il doit s'agir d'un entier.

Cette propriété indique, en secondes, l'intervalle d'actualisation pour la mise à jour d'informations relatives aux attributs étendus définis, par exemple dans les serveurs de stockage.

Propriétés SSH (Secure Shell)

Ces propriétés s'appliquent à SSH (Secure Shell).

Fix Pack 1 **com.ibm.cdb.platform.SshVersionSessionSkipList**
Cette propriété indique les versions des serveurs SSH pour lesquels la session n'est pas établie. En pareil cas, le détecteur de session se termine sans erreur.

La valeur de cette propriété est une liste séparée par des virgules, par exemple `Cisco,Data ONTAP,SSH-2.0-OpenSSH_5.9 PKIX FIPS,OpenSSH_OA`.

com.collation.SshLogInput=false
La valeur par défaut est `false`.

Les valeurs valides sont `true` ou `false`. Si vous indiquez la valeur `true`, l'entrée SSH est consignée.

com.collation.SshPort=22
La valeur par défaut est `22`. Il doit s'agir d'un entier.

Cette propriété indique le port utilisé par le serveur pour toutes les connexions SSH.

com.collation.SshSessionCommandTimeout=120000
La valeur par défaut est `120000`. Il doit s'agir d'un entier.

Cette valeur indique la durée (en millisecondes) accordée pour exécuter la commande SSH. Si cette propriété est utilisée à partir d'un agent, sa valeur doit être inférieure à celle de la propriété **AgentRunnerTimeout** pour pouvoir s'appliquer.

com.collation.SshWeirdReauthErrorList=Droit refusé

Cette propriété permet de saisir à nouveau le nom d'utilisateur et le mot de passe en vigueur lors des précédentes exécutions de la reconnaissance. La propriété est nécessaire car les systèmes Windows refusent de façon aléatoire des tentatives valides de connexion. La propriété doit posséder le paramètre `Droit refusé`. Ne modifiez pas cette propriété.

com.collation.WmiInstallProviderTimeout=240000
La valeur par défaut est `240 000`. Il doit s'agir d'un entier.

Cette valeur indique le temps d'attente autorisé (en millisecondes) pour l'exécution du script InstallProvider WMI.

com.collation.SshSessionReuseSuppressList
Certaines versions du serveur SSH ne prennent pas en charge la réutilisation de connexions telles qu'elles sont implémentées par TADDM. Les versions du serveur SSH qui ne sont pas prises en charge pour une réutilisation doivent être ajoutées à cette propriété pour permettre à TADDM de reconnaître correctement des cibles qui exécutent des versions de serveurs SSH.

La valeur de cette propriété est une liste séparée par des virgules. Elle est suffisante pour spécifier uniquement le début de la version du serveur SSH, par exemple `SSH-2.0-BoKS_SSH_6`.

Vous pouvez trouver la version du serveur SSH dans le fichier journal du détecteur de session.

Propriétés de sécurité

Ces propriétés s'appliquent à la sécurité.

Fix Pack 3 **com.ibm.cdb.secure.server=false**
La valeur par défaut est `false`.

Cette propriété indique si tous les services TADDM dans les registres RMI externes et publics sont sécurisés. Si la propriété est définie sur `true`, tous les services publics non sécurisés (ClientProxyServer et APIServer) sont déplacés vers le registre RMI interne. Par ailleurs, le protocole SSL est appliqué aux services externes, par exemple, RegistriesURLProvider, SecurityManager et TopologyManager.

Si vous définissez cette propriété sur `true`, définissez également les propriétés `com.collation.security.enablesslforconsole` et `com.collation.security.enforceSSL` sur `true`.

Cette propriété pourrait affecter l'intégration aux autres produits qui se connectent à TADDM avec une connexion non sécurisée.

Si vous modifiez la valeur par défaut de cette propriété, définissez-la dans les emplacements suivants :

- `$COLLATION_HOME/dist/etc/collation.properties`
- `$COLLATION_HOME/dist/sdk/etc/collation.properties`
- `sdk/etc/collation.properties` de chaque installation du logiciel SDK TADDM.

Fix Pack 5 Si le serveur est exécuté en mode sécurisé (`com.ibm.cdb.secure.server = true`), le port suivant sera sécurisé à l'aide du protocole SSL :

- `com.ibm.cdb.service.registry.public.port (Default Value:9433)`

Si le serveur est exécuté en mode sécurisé (`com.ibm.cdb.secure.server = true`), la case "Etablir une session sécurisée (SSL)" doit être cochée lors du lancement de la console de gestion des données :

Fix Pack 1 **com.ibm.cdb.secure.liberty=false**
La valeur par défaut est `false`.

Les valeurs valides sont `true` ou `false`. Pour désactiver le port HTTP non sécurisé, définissez cet indicateur à `true`.

com.collation.security.privatetruststore=true
La valeur par défaut est `true`.

Les valeurs valides sont `true` ou `false`. La valeur doit être `true` lorsque SSL est activé.

com.collation.security.enablesslforconsole=true
La valeur par défaut est `true`.

Les valeurs valides sont `true` ou `false`.

com.collation.security.enabledatalevelsecurity=false
La valeur par défaut est `false`.

Les valeurs valides sont `true` ou `false`. Pour limiter l'accès aux collections des objets TADDM par utilisateur ou groupe d'utilisateurs, définissez cette valeur sur `true`.

com.collation.security.enforceSSL=false
La valeur par défaut est `false`.

Les valeurs valides sont `true` ou `false`. Pour désactiver des connexions non sécurisées et forcer l'utilisation de connexions SSL, définissez cet option à `true`.

com.collation.security.usermanagementmodule=file
La valeur par défaut est `file`.

Cette propriété offre trois options :

- `file` pour un registre d'utilisateurs basé sur le fichier TADDM.
- `ldap` pour un registre d'utilisateurs LDAP.
- `vmm` pour un registre d'utilisateurs utilisant les répertoires fédérés de WebSphere Application Server

com.collation.security.auth.sessionTimeout=240
La valeur par défaut est `240`. Il doit s'agir d'un entier.

com.collation.security.auth.searchResultLimit=100
La valeur par défaut est `100`. Il doit s'agir d'un entier.

Utilisez cette propriété si les utilisateurs sont nombreux.

Important : Si vous disposez de plus de 100 utilisateurs dans un référentiel LDAP ou WebSphere Federated, augmentez cette valeur pour prendre en charge le nombre d'utilisateurs attendu. Par exemple, `com.collation.security.auth.searchResultLimit=150`

com.collation.security.auth.websphereHost=localhost
La valeur par défaut est `localhost`.

Entrez le nom de domaine complet du système qui héberge la fonctionnalité des référentiels fédérés de WebSphere Application Server.

com.collation.security.auth.websperePort=2809
La valeur par défaut est `2809`.

Il doit s'agit d'un entier. Cette valeur indique le port du système WebSphere.

com.ibm.cdb.service.SecurityManager.port=9540
Pour les serveurs autres que les serveurs de synchronisation :

La valeur par défaut est 9540.

Indique le port du pare-feu qui est utilisé par le gestionnaire de sécurité.

Pour les serveurs de synchronisation :
La valeur par défaut n'est pas définie.
Les domaines communiquent avec un serveur de synchronisation via un port spécifié dans le paramètre **com.collation.EnterpriseSecurityManager.port**. La valeur par défaut de cette propriété est 19433.

com.collation.cdm.analytics.authorizedRole=

Le panneau Analytics peut être restreint à un rôle spécifique. Par défaut, cette propriété n'est pas définie dans le fichier collation.properties et le panneau Analytics est accessible à tous. La valeur de la propriété doit être le nom du rôle autorisé à accéder au panneau.

L'accès aux zones suivantes du panneau Analytics peut être accordé au rôle spécifié :

- Fix Pack 2 Modèles de regroupement
- Récapitulatif de l'inventaire
- Récapitulatif de l'application
- Récapitulatif du service
- Inventaire du système
- Inventaire des serveurs logiciels
- Rapports BIRT

com.collation.security.discoverOutsideScope=true
La valeur par défaut est true.

Les valeurs valides sont true ou false. Pour désactiver une reconnaissance d'éléments qui ne sont pas à l'intérieur de la portée, définissez cet indicateur à false.

com.ibm.cdb.secure.tomcat=false (TADDM 7.3.0 uniquement)
La valeur par défaut est false.

Les valeurs valides sont true ou false. Pour désactiver le port HTTP non sécurisé, définissez cet indicateur à true.

com.ibm.cdb.http.ssl.protocol=TLS
La valeur par défaut est TLS.

Cette propriété modifie le protocole SSL qui est utilisé par le port SSL Web, à savoir le port HTTPS (9431 par défaut). Vous pouvez définir le port avec la propriété com.ibm.cdb.service.web.secure.port.

Pour obtenir la liste des valeurs prises en charge, voir la documentation IBM Java 7 à http://www-01.ibm.com/support/knowledgecenter/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/jsse2Docs/protocols.html. Si vous utilisez des protocoles plus sécurisés, comme TLS v1.1 ou TLS v1.2, vous devez tout d'abord configurer votre navigateur Web pour leur prise en charge. En outre, des protocoles plus forts pourraient affecter l'intégration à d'autres produits qui se connectent à TADDM via le port SSL Web.

Fix Pack 5 Lorsque com.ibm.cdb.http.ssl.protocol=TLSv1.2 et JAVA7 sont utilisés côté client, les paramètres suivants doivent être mis à jour :

```
<JAVA_HOME>/jre/lib/security/java.security
jdk.tls.disabledAlgorithms=SSLv2, SSLv3, TLSv1, TLSv1.1
```

En outre, TLSv1 et TLSv1.1 doivent être désactivés dans le navigateur.

⌂**com.ibm.cdb.ssl.protocol=TLS**
Cette propriété n'est par défaut pas ajoutée dans le fichier `collation.properties`. Dans ce cas, la valeur par défaut est `TLS`. Pour la modifier, ajoutez manuellement cette propriété dans le fichier `collation.properties` avec la nouvelle valeur.

Cette propriété modifie le protocole SSL qui est utilisé par les ports suivants :

- Le port sur lequel le serveur d'API est en mode écoute pour les demandes SSL (`9531` par défaut). Vous pouvez définir le port avec la propriété `com.ibm.cdb.service.SecureApiServer.secure.port`.
- Le port de données RMI à utiliser avec SSL (`9434` par défaut). Vous pouvez le définir avec la propriété `com.ibm.cdb.service.SecureClientProxyServer.secure.port`.

Pour obtenir la liste des valeurs prises en charge, voir la documentation IBM Java 7 à http://www-01.ibm.com/support/knowledgecenter/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/jsse2Docs/protocols.html. Si vous utilisez des protocoles plus sécurisés, comme `TLS v1.1` ou `TLS v1.2`, vous devez tout d'abord configurer votre navigateur Web pour leur prise en charge. En outre, des protocoles trop forts pourraient affecter l'intégration à d'autres produits qui se connectent à TADDM via les ports répertoriés.

⌂**com.ibm.cdb.http.ssl.ciphers=**
Les chiffrements sont définis sur le serveur LibertyServer et la communication se fait uniquement sur les chiffrements donnés. Autrement, les chiffrements par défaut, susceptibles d'être des algorithmes faibles, sont sélectionnés.

⌂**com.ibm.cdb.rmi.ssl.protocol=**
La propriété `com.ibm.cdb.rmi.ssl.protocol` permet d'activer un protocole spécifique pour la connexion SSL qui a été créée sur `com.ibm.cdb.ssl.protocol`.

`com.ibm.cdb.rmi.ssl.protocol` doit provenir de la liste des protocoles pris en charge sur `com.ibm.cdb.ssl.protocol`.

⌂**com.ibm.cdb.rmi.ssl.ciphers=**
Cette propriété vous permet de définir les algorithmes de chiffrement du port de données RMI et le port de ce serveur API est en mode écoute.

Propriétés des répertoires temporaires

Ces propriétés s'appliquent à l'utilisation des répertoires temporaires.

Les répertoires temporaires sont utilisés par TADDM pour stocker les fichiers temporaires sous certaines conditions. Il peut s'agir par exemple de fichiers d'ancre de journal, de scripts de reconnaissance, de résultats de reconnaissance et d'informations requises par certains détecteurs lors de l'exécution d'une reconnaissance. TADDM utilise trois répertoires temporaires : `ANCHOR_DIR`, `ASD_TEMP_DIR` et `TADDM_TEMP_ROOT`.

com.ibm.cdb.taddm.anchor.root=.
La valeur par défaut est `.\`.

Cette entrée indique l'emplacement du répertoire ANCHOR_DIR dans lequel le serveur d'ancrage est déployé. Cette propriété est une propriété sectorisée. Vous pouvez lui ajouter l'adresse IP et le nom de la portée ou du système d'exploitation. Par exemple : com.ibm.cdb.taddm.anchor.root.SunOS=.

Pour un système Windows, le nom de propriété et la valeur par défaut suivants sont utilisés :

```
com.ibm.cdb.taddm.anchor.root.Windows=%windir%\\temp\\
```

La valeur de propriété utilise des variables résolues sur les hôtes cible. Les variables Linux, AIX et SunOS doivent contenir un préfixe et un signe dollar ($). Les variables Windows doivent être encadrées par des signes pourcentage (%). Par exemple com.ibm.cdb.taddm.anchor.root=$TMP/taddmdirs/anchor et com.ibm.cdb.taddm.anchor.root.Windows=%TEMP%\\taddmdirs\\anchor.

Si la valeur de propriété résolue est un chemin de répertoire relatif, son préfixe est le suivant :

- %windir%\\temp\\ - pour Windows
- Répertoire de base - pour les systèmes AIX, Linux et SunOS

Le chemin porte comme suffixe le répertoire taddmversion/anchor. Par exemple /home/taddmusr/taddm7.2.1/anchor et c:\Windows\Temp\taddm7.2.1\anchor.

com.ibm.cdb.taddm.asd.temp
Cette entrée définit l'emplacement du répertoire ASD_TEMP_DIR, dans lequel les scripts de reconnaissance et les résultats des reconnaissances sont stockés. Cette propriété est une propriété sectorisée. Vous pouvez la personnaliser en lui ajoutant l'adresse IP ou le nom du système d'exploitation.

Le répertoire taddm*version*/asd/ est créé à l'emplacement indiqué. Par exemple : /tmp/taddm7.2.1/asd/. Si vous indiquez un nouvel emplacement, tous les utilisateurs doivent disposer de tous les droits d'accès au nouvel emplacement.

com.ibm.cdb.taddm.file.temp=.
La valeur par défaut est .\.

Cette entrée définit l'emplacement du répertoire taddm_temp_root qui est utilisé par divers détecteurs pour stocker les données temporaires nécessaires à l'exécution d'une reconnaissance. Les répertoires DB2® et WebLogic sont des exemples de détecteurs qui stockent des données temporaires.

Le répertoire TADDM_TEMP_ROOT est créé dans le répertoire de base du répertoire taddm*version*/temp/. Par exemple : /home/taddmusr/taddm7.2.1/temp/.

Propriétés du générateur de topologie

Ces propriétés s'appliquent au générateur de topologie.

com.collation.topobuilder.RuntimeGcUnknownServerRetentionSpan=5
La valeur par défaut est 5.

Cette propriété indique combien de temps (en jours) les processus inconnus doivent être conservés. La valeur maximale est 14. Les processus inconnus déterminent le moment où les modèles de serveur personnalisés sont nécessaires. Toutefois, à défaut de nettoyages réguliers, le nombre de processus inconnus peut s'accumuler au fil du temps. Ceci peut entraîner

des problèmes de performances de la topologie. L'élément d'espace adresse zOS n'est pas supprimé lors de ce traitement.

com.collation.topobuilder.RuntimeGcThreadCount=
La valeur par défaut est `4`.

Cette propriété ajoute du parallélisme à l'agent RuntimeGC qui peut améliorer les performances

com.collation.topobuilder.agent.DerivedAppToAppDependencyAgent.ServiceDependency.enabled
La valeur par défaut est `false`.

Cette propriété indique si l'agent de topologie `DerivedAppToAppDependency` crée une dépendance entre des applications métier quand leurs membres sont liés par une dépendance de service.

Pour permettre à l'agent de créer ce type de dépendance, affectez la valeur `true` à cette propriété.

Propriétés du gestionnaire de topologie

Ces propriétés s'appliquent au gestionnaire de topologie.

com.ibm.JdoQuery.FetchBatchSize=500
La valeur par défaut est `500`.

La taille des lots est une propriété configurable et correspond à la propriété **`kodo.FetchBatchSize`**. Cette propriété représente le nombre de lignes à extraire en une fois de l'ensemble de résultats d'une requête.

com.ibm.cdb.service.TopologyManager.port=9550
La valeur par défaut est `9550`.

Définit le port du pare-feu utilisé par le gestionnaire de topologie.

Propriétés du gestionnaire de vues

Ces propriétés s'appliquent au gestionnaire de vues.

Fix Pack 2 **com.ibm.taddm.hideNetworkConnectionUnusedColumns.enabled**
La valeur par défaut est `false`.

Cette propriété indique si les colonnes suivantes de l'onglet **Connexions réseau** s'affichent dans Data Management Portal :

- **Flux**
- **Paquets**
- **Octets**
- **Premier vu**
- **Dernier vu**

Pour masquer ces colonnes, définissez cette propriété sur `true`.

com.collation.view.maxnodes=500
La valeur par défaut est `500`. Il doit s'agir d'un entier.

Cette propriété indique le nombre maximal de noeuds pouvant être affichés dans un graphique de topologie dans le portail de gestion de données. Si vous définissez la propriété à une valeur supérieure, vous pourrez afficher des topologies de taille supérieure. Cependant, cela peut augmenter les besoins en terme de mémoire.

Vérification de l'intégrité des données

Vous pouvez exécuter la commande **verify-data** pour vérifier l'intégrité des données des éléments de configuration de la base de données TADDM. Vous pouvez vérifier les relations, le mappage des héritages, les doublons et les excès de fusion.

Avant de commencer

N'exécutez pas une reconnaissance, un chargement en bloc ou une synchronisation avec l'option réparation activée. L'outil d'intégrité des données analyse une grande quantité de données et il peut prendre un certain temps pour terminer le processus, en particulier avec l'option réparation activée. Le serveur TADDM doit être actif et en service mais vérifiez qu'il n'effectue aucune tâche.

Pourquoi et quand exécuter cette tâche

L'outil de vérification de l'intégrité des données signale et résout les problèmes d'intégrité des données des éléments de configuration de la base de données TADDM. Le script exécutable se trouve dans le répertoire `$COLLATION_HOME/bin`. L'outil génère des rapports et des journaux dans le fichier `verify-data.log`. Vous pouvez arrêter l'outil et le réexécuter à tout moment.

Vérification des relations

Le processus de vérification des relations interroge et vérifie les clés externes dans toutes les tables de modèle et d'intersection.

Pourquoi et quand exécuter cette tâche

Avec l'option de réparation activée, le processus de vérification des relations supprime les objets enfant si un objet parent ne figure pas dans la base de données et supprime les valeurs de clé externe non valides pour les relations définies comme non contenues. Cette option peut également supprimer un nombre significatif d'éléments de configuration de bas niveau. Cependant, si les éléments ne possèdent pas d'objet parent, ils peuvent être supprimés en toute sécurité.

Procédure

Pour vérifier les relations, exécutez l'une des commandes suivantes :

- **verify-data.sh -v ro [-a repair]**
- **verify-data.bat -v ro [-a repair]**

Vérification du mappage des héritages

Le processus de vérification du mappage des héritages interroge toutes les tables mappant une classe d'élément de configuration et vérifie que toutes les tables contiennent une entrée pour chaque ligne.

Pourquoi et quand exécuter cette tâche

Lorsque l'option réparation est activée, les enregistrements sont recréés.

Procédure

Pour vérifier le mappage des héritages, exécutez l'une des commandes suivantes :

- **verify-data.sh -v io [-a repair]**
- **verify-data.bat -v io [-a repair]**

Vérification des doublons

Le processus de vérification des doublons recherche les éléments de configuration en double en se basant sur les valeurs des zones de règle de nommage de la base de données.

Pourquoi et quand exécuter cette tâche

Si l'option réparation est activée, les objets en double sont fusionnés. Après la fusion, l'objet définitif reste dans la base de données et l'objet transitoire est supprimé.

La fusion est effectuée par plusieurs unités d'exécution en parallèle. Le nombre d'unités d'exécution par défaut est 5. Vous pouvez modifier le nombre d'unités d'exécution dans le fichier `collation.properties` en définissant l'indicateur **`com.ibm.cdb.topomgr.dataverification.generator.ThreadCount`** sur un nombre approprié, comme dans l'exemple suivant :

- **`com.ibm.cdb.topomgr.dataverification.generator.ThreadCount=10`**

Vous devez redémarrer le serveur TADDM après avoir modifié le nombre d'unités d'exécution.

Certaines erreurs peuvent se produire lors de la fusion des objets. La cause des erreurs est contenue dans un fichier journal.

- `ERROR_INVALID_DURABLE_GUID`
- `ERROR_INVALID_TRANSIENT_GUID`

La cause des erreurs correspond à des alias manquants dans la table d'alias ou à un objet non valide. Vous devez attendre que les agents de nettoyage suppriment les objets non valides.

Procédure

Pour vérifier les doublons, exécutez l'une des commandes suivantes :

- **`verify-data.sh -v dup [-a repair]`**
- **`verify-data.bat -v dup [-a repair]`**

Vérification des excès de fusion

Le processus de vérification des excès de fusion utilise les données collectées dans la table ALIASES_JN pour rechercher et signaler des GUID présentant de nombreux changements d'alias maîtres.

Pourquoi et quand exécuter cette tâche

La table ALIASES_JN contient un historique des changements apportés à la table ALIASES. Un excès de fusion se produit lorsque quelques objets changent leur objet parent en objet de même modèle. Les objets enfant sont alors regroupés autour d'un certain nombre d'objets parent. Les excès de fusion qui surviennent avant l'installation de TADDDM 7.2.1 groupe de correctifs 3 sont introuvables car il n'y a aucune donnée obligatoire dans la table ALIASES_JN. Le processus de vérification ne comprend pas l'option réparation car il peut rechercher et signaler de faux résultats positifs.

Par défaut, le suivi détaillé est activé pour les classes ComputerSystem, AppServer et Operating System et toutes les autres classes qui héritent de ces dernières. Si vous souhaitez activer le suivi pour des classes différentes, vous pouvez modifier la propriété suivante dans le fichier `collation.properties` :

```
com.ibm.tivoli.namereconciliation.service.overmergeClasses
```

L'exemple ci-dessous illustre la propriété spécifiée pour la recherche des classes ComputerSystem, AppServer et Operating System :

```
com.ibm.tivoli.namereconciliation.service.overmergeClasses=
ComputerSystem,AppServer,OperatingSystem
```

Signification des actions utilisées pour exécuter la commande :

- s1s2s1 - La vérification recherche les éléments de configuration qui modifient les valeurs de leurs attributs de nommage dans une boucle. Par exemple, un système informatique avec une signature A, puis une signature B, avant que la signature A soit à nouveau détectée.
- s1s2s3 - La vérification recherche les éléments de configuration contenant un certain nombre de modifications pour des attributs de nommage donnés.
- m1m2m1 - La vérification recherche les éléments de configuration pour lesquels les identificateurs globaux uniques ont modifié leur identificateur global unique maître à plusieurs reprises. Par exemple, un alias A avec un identificateur global unique maître B ultérieurement réattribué à l'identificateur global maître C, puis réattribué à l'identificateur global unique maître B, serait détecté.
- m1m2m3 - La vérification recherche les éléments de configuration pour lesquels les identificateurs globaux uniques ont modifié leur identificateur global unique maître à plusieurs reprises.
- WinCSLinCSWinCS - La vérification recherche les éléments de configuration ayant modifié leur type à plusieurs reprises. Par exemple, un système informatique initialement stocké en tant que WindowsComputerSystem, puis mis à jour vers LinuxUnitaryComputerSystem, avant d'être remis à jour vers WindowsComputerSystem serait détecté.

Procédure

Pour vérifier les excès de fusion, exécutez l'une des commandes suivantes :

- **verify-data.sh -v om [-a <action>] [-p <class>] [-from <time stamp>] [-to <time stamp>]**
- **verify-data.bat -v om [-a <action>] [-p <class>] [-from <time stamp>] [-to <time stamp>]**

  où :

  – **<action>**: s1s2s1, s1s2s3, m1m2m1, m1m2m3, WinCSLinCSWinCS
  – **<class>** : n'importe quelle classe du modèle TADDM, par exemple, ComputerSystem.
  – **<time stamp>** : horodatage au format YYYY-MM-DD HH24:MI:SI.

Exemple

```
verify-data.sh -v om -a s1s2s1 m1m2m1 WinCSLinCSWinCS
-p ComputerSystem -from 2012-11-13 14:50:00 -to 2012-11-14 14:50:01
```

Cette commande recherche les fusions de type s1s2s1, m1m2m1 et WinCSLinCSWinCS pour la classe ComputerSystem et toutes les classes qui héritent de cette dernière et créées entre le 2012-11-13 14:50:00 et le 2012-11-14 14:50:01.

Résolution du problème d'excès de fusion :

Un excès de fusion se produit lorsque quelques objets changent leur objet parent en objet de même modèle. Les objets enfant sont alors regroupés autour d'un certain nombre d'objets parent.

Procédure

1. Effectuez la vérification des excès de fusions.
2. Vérifiez les éléments de configuration signalés. La vérification peut les signaler de manière incorrecte sous forme d'excès de fusions.
3. Corrigez la configuration des environnements pouvant être la cause de l'excès de fusion. Les problèmes de configuration peuvent présenter la même signature, le même numéro de série, le même ID de machine virtuelle et d'autres attributs de noms d'EC.
4. Supprimez les objets fusionnés en excès de la base de données TADDM.
5. Exécutez une reconnaissance des objets supprimés et validez les résultats.
6. Supprimez tous les enregistrements de la table ALIASES_JN après avoir résolu les problèmes d'excès de fusion.

Gestion du cache des données d'identification - Utilitaire cachemgr

Vous pouvez utiliser la commande **cachemgr.sh** ou **cachemgr.bat** pour afficher et supprimer le contenu du cache des données d'identification.

Syntaxe de la commande

cachemgr -h | **-u** *utilisateur* **-p** *mot_passe* (**-l** | **-r**) *valid* | *invalid* | *all* [[**-s** *IP* | *scope* | *scope group* | *range* | *subnet*] [**-a** *espaceAdresse*] [**-n** *nomDonnéesIdentificationAccès*] [**-c** *type*] [**-d** *aaaa/mm/jj*] [**-k** *clé*] [**-t** *baliseEmplacement*]]

Paramètres

-a, --addressSpace ***espaceAdresse***
Correspond au nom de l'espace adresse.

-c, --class ***type***
Correspond au type d'une entrée d'accès sélectionnée décrite par le nom de la classe spécifique qui implémente l'entrée d'accès.

-d, --date ***aaaa/mm/jj***
Correspond au seuil de date utilisé pour sélectionner des entrées non modifiées jusqu'à l'heure spécifiée. Le format est aaaa/mm/jj.

-h, --help
Affiche l'aide.

-k, --key ***clé***
Correspond à la clé d'une entrée de cache sélectionnée.

-l, --list ***valid*|*invalid*|*all***
Correspond à l'opération de liste contrôlée par les arguments suivants :

- *valid* - Ne répertorie que les tentatives d'authentification valides conservées en cache.
- *invalid* - Ne répertorie que les tentatives d'authentification non valides conservées en cache.

- *all* - Répertorie les tentatives d'authentification valides et non valides conservées en cache.

-n, --name *nomDonnéesIdentificationAccès*
Correspond au nom des données d'identification d'accès, comme dans la liste d'accès.

-p, --password *mot_passe*
Correspond au mot de passe de l'utilisateur qui se connecte au serveur TADDM.

-r, --remove *valid|invalid|all*
Correspond à l'opération de suppression contrôlée par les arguments suivants :

- *valid* - Ne supprime que les tentatives d'authentification valides conservées en cache.
- *invalid* - Ne supprime que les tentatives d'authentification non valides conservées en cache.
- *all* - Supprime les tentatives d'authentification valides et non valides conservées en cache.

-s, --scope *IP|scope|scope group|range|subnet*
Correspond à la portée d'une entrée d'accès. Contrôlée par les arguments suivants :

- *IP*
- *scope*
- *scope group*
- *range*
- *subnet*

-t, --locationTag *baliseEmplacement*
Correspond à la balise d'emplacement d'une entrée d'accès sélectionnée.

-u, --username *nom_utilisateur*
Correspond à l'utilisateur qui se connecte au serveur TADDM.

Exemples

- La commande suivante répertorie toutes les tentatives d'authentification non valides des ordinateurs dans la portée "ScopeSet" :

```
cachemgr.sh -u utilisateur -p mot_passe -l invalid -s ScopeSet
```

Cette commande génère la sortie suivante :

```
Les entrées suivantes correspondent aux critères indiqués :
CachedAuthEntry
 guid: 3B954CE4CFBF346C8DF538F09F1F7FFD
 keyString: SSH!9.128.109.144!!com.collation.platform.security.auth.HostAuth!null!
 lastModified: Thursday, 5 September 2013 11:00:38
 Autorisation : non valide. Message d'erreur : CTJTP1190E Le serveur n'a pas terminé
le processus d'autorisation.
CachedAuthEntry
 guid: ACC2F35A66D3379BAC13FC606C5A08A3
 keyString: SSH!9.128.109.145!!com.collation.platform.security.auth.HostAuth!null!
 lastModified: Thursday, 5 September 2013 11:00:38
 Autorisation : non valide. Message d'erreur : CTJTP1190E Le serveur n'a pas terminé
le processus d'autorisation.
```

- La commande suivante supprime les tentatives d'authentification non valides dans la plage d'adresses IP comprise entre 9.123.149.10 et 9.123.149.12 et l'entrée d'accès com.collation.platform.security.auth.HostAuth :

```
cachemgr.sh -u utilisateur -p mot_passe -r invalid -s 9.123.149.10-9.123.149.12
-c com.collation.platform.security.auth.HostAuth
```

Cette commande génère la sortie suivante :

```
Entrées d'authentification supprimées du cache (2).
```

Codes retour de l'utilitaire Cachemgr

Si vous écrivez un script cron ou un autre script qui appelle l'utilitaire cachemgr, les codes retour ci-après indiquent le mode de sortie du programme.

0 Le programme s'est correctement déroulé.

1 Un paramètre de ligne de commande non valide a été spécifié. Le paramètre lui-même ou les données fournies avec le paramètre ne sont pas correctes. Corrigez la commande et renouvelez l'opération.

2 Un paramètre de ligne de commande de date n'était pas au format attendu.

3 La définition de portée fournie n'est pas résolue en adresse IP ou l'entrée d'accès fournie n'est pas valide.

4 Une erreur inconnue s'est produite. Accédez au répertoire des journaux et ouvrez le fichier `cachemgr.log` pour rechercher des informations supplémentaires.

5 L'utilisateur spécifié ne dispose pas de privilèges suffisants (reconnaissance) pour effectuer l'opération.

6 Aucune entrée de la base de données ne correspondait aux critères fournis.

Préparation de la reconnaissance

Pour optimiser les informations rassemblées par TADDM de votre environnement lors de reconnaissances, vous devez exécuter des tâches de configuration afin de préparer votre environnement pour une reconnaissance.

Pourquoi et quand exécuter cette tâche

Les tâches de configuration spécifiques dépendent du type et du niveau de reconnaissance que vous devez prendre en charge dans votre environnement.

Que faire ensuite

Outre la configuration de votre environnement pour une reconnaissance, vous devez configurer des détecteurs TADDM selon les besoins. Pour plus d'informations sur la marche à suivre, voir le *Guide de référence des détecteurs* de TADDM.

Pour plus d'informations sur l'exécution d'une reconnaissance, notamment sur la définition d'une portée et d'une planification, voir le *Guide d'utilisation* de TADDM.

Configuration de l'ID de connexion utilisateur

TADDM requiert un utilisateur interactif pour exécuter des reconnaissances. Vous devez donc configurer l'ID de connexion de cet utilisateur.

Un ID de connexion d'utilisateur interactif est utilisé dans un mode non interactif pour toutes les sessions de reconnaissance, y compris pour une session entre un serveur et une passerelle ou l'inverse. L'utilisateur doit être interactif pour exécuter

les commandes. Toutefois, les commandes sont exécutées de manière non interactive, ce qui signifie que l'utilisateur exécute les commandes puis en attend les résultats.

Définissez l'utilisateur dans le fichier `/etc/passwd` comme suit :

taddmusr`:x:100:100::/export/home/`*taddmusr*`:/bin/sh`

où *taddmusr* indique le nom de l'utilisateur de TADDM.

Configuration pour d'autres méthodes de reconnaissance

Vous pouvez utiliser d'autres méthodes de reconnaissance, comme la reconnaissance asynchrone, la reconnaissance basée sur un script ou la reconnaissance à l'aide d'IBM Tivoli Monitoring.

Notes :

1. Une reconnaissance asynchrone ou basée sur un script est uniquement prise en charge si le système informatique cible exécute le système d'exploitation AIX, FreeBSD, HP NonStop, Linux (sur des systèmes x86 uniquement), Solaris ou Windows.
2. Si le système informatique cible exécute le système d'exploitation Solaris, une reconnaissance basée sur un script peut échoue en cas d'utilisation de SunSSH 1.0.

Configuration de la reconnaissance asynchrone

Pour exécuter une reconnaissance asynchrone, vous devez commencer par configurer cette reconnaissance.

Pourquoi et quand exécuter cette tâche

Pour configurer une reconnaissance asynchrone, vous devez générer un package de script de reconnaissance, le copier sur le système cible et exécuter le script sur le système cible. La sortie du script de reconnaissance est un fichier archive contenant les résultats de la reconnaissance. Vous devez ensuite déplacer ce fichier vers le serveur TADDM.

Remarque : Si vous avez configuré la reconnaissance pour qu'elle s'exécute en mode asynchrone puis que vous avez mis TADDM à niveau, vous devez de nouveau générer un package de script de reconnaissance, car l'ID du plug-in de détecteur peut changer.

Procédure

1. Pour générer un package de script de reconnaissance, entrez l'une des commandes suivantes depuis le répertoire `$COLLATION_HOME/bin` :
   - **Méthode classique**

     `makeASDScriptPackage` *`REP_SORTIE UNOM`* `[`*`ADRESSEIP`*`] [`*`METHODE_PACKAGE`*`]`

     REP_SORTIE
     Chemin de répertoire du package de script.

     UNOM
     Système d'exploitation du système cible sur lequel le script doit être exécuté. Les valeurs valides sont `AIX`, `Linux`, `SunOS`, `FreeBSD`, `Windows` ou `NONSTOP_KERNEL`.

     ***ADRESSEIP* (facultatif)**
     Adresse IP du système cible sur lequel le script doit être exécuté.

Les scripts employés pour une reconnaissance asynchrone utilisent des informations des propriétés du serveur TADDM définies dans le fichier `collation.properties` ; il est possible d'appliquer une portée à certaines propriétés.

Propriété sectorisée
Propriété à laquelle vous pouvez ajouter une adresse IP ou le nom d'un ensemble de portées. Une fois cette adresse ou ce nom ajouté, la propriété devient dépendante du système hôte en cours de reconnaissance. Vous pouvez utiliser uniquement des noms d'ensembles de portées qui ne contiennent ni espace, ni apostrophe ('), ni point (.) ni barre oblique (/).

Si vous avez personnalisé l'une des propriétés du serveur TADDM afin qu'elle ait une portée, vous devez inclure l'option *IPADDRESS* dans la commande **makeASDScriptPackage**.

METHODE_PACKAGE **(facultatif)**
Méthode utilisée pour créer le package de fichiers. Les valeurs valides sont `tar` et `zip`.

Si aucune méthode n'est spécifiée, le système d'exploitation en choisit une. La méthode TAR est par exemple utilisée pour les systèmes d'exploitation tels que Linux.

L'utilitaire d'archivage est par défaut recherché dans le chemin de système. Si nécessaire, ajoutez la propriété `com.ibm.cdb.tarpath` au fichier `collation.properties` et indiquez un chemin alternatif pour l'utilitaire d'archivage.

Sur les systèmes d'exploitation Solaris, en raison d'une limitation relative à la longueur des noms de fichier, vous devez utiliser l'utilitaire d'archivage gtar et spécifier le chemin d'accès à cet utilitaire.

L'exemple suivant montre comment indiquer le chemin de la commande **tar** sur le serveur TADDM qui exécute le système d'exploitation AIX :

```
com.ibm.cdb.tarpath=tar
```

Les exemples suivants montrent comment spécifier le chemin de la commande **tar** *sur le système cible*, en fonction du système d'exploitation :

Pour AIX
```
com.ibm.cdb.targettarpath.AIX=tar
```

Pour Solaris
```
com.ibm.cdb.targettarpath.SunOS=/usr/sfw/bin/gtar
```

Par exemple, pour générer un package de script de reconnaissance pour le système d'exploitation AIX, entrez la commande suivante :

```
./makeASDScriptPackage /tmp AIX
```

Cette commande crée le package de script AIX suivants dans le répertoire `tmp` : `/tmp/taddm_AIX.tar`.

- **Méthode étendue**

```
makeASDScriptPackage --outputDir REP_SORTIE --uname UNOM
[--ipAddress IP_ADDRESS] [--packingMethod METHODE_PACKAGE] [--sensors DETECTEUR]
```

--outputDir *REP_SORTIE*
Voir la description du paramètre *REP_SORTIE* de la méthode classique.

--uname *UNOM*
Voir la description du paramètre *UNOM* de la méthode classique.

[--ipAddress *ADRESSE_IP*] (facultatif)
Voir la description du paramètre *ADRESSE_IP* de la méthode classique.

[--packingMethod *METHODE_PACKAGE*] (facultatif)
Voir la description du paramètre *METHODE_PACKAGE* de la méthode classique.

[--sensors *DETECTEUR*] (facultatif)
Nom du détecteur à inclure dans votre package. Le tableau suivant contient les noms de détecteur qui doivent être utilisés dans cette commande.

Tableau 33. Noms de détecteur utilisés dans la commande **makeASDScriptPackage**.

Détecteur	**Nom utilisé dans la commande**
Détecteur Apache	apacheserver
Détecteur Citrix XenServer	xenserver
Détecteur de système informatique FreeBSD	computersystem
Détecteur de serveur générique	genericserver
Détecteur de système informatique HP NonStop	computersystem
Détecteur du système informatique IBM AIX	computersystem
Détecteur IBM DB2	db2
Détecteur de serveur IBM Lotus Domino	dominoserverinitial
Détecteur d'utilisation IBM Tivoli	utilization
Détecteur IBM WebSphere MQ Server	mqserver
Détecteur IBM WebSphere	webspherescript
Détecteur JBoss Application Server 7	jboss7
Détecteur KVM	kvm
Détecteur de système informatique Linux	computersystem
Détecteur Microsoft Exchange	exchange
Détecteur de serveur Microsoft IIS Web Server	iisserver
Détecteur Oracle	oracle
Détecteur de système informatique Solaris	computersystem
Détecteur WebLogic SSH	weblogiclaunchersensor
Détecteur de système informatique Windows	computersystem

Le détecteur de reconnaissance asynchrone est ajouté par défaut à chaque package. Tous les détecteurs de système d'exploitation sont nommés `computersystem`. Ils sont différenciés par le paramètre `--uname`. Par exemple, si vous spécifiez les paramètres suivants :

```
[...] --uname Linux --sensors computersystem
```

Le détecteur de système informatique Linux est ajouté au package.

Par exemple, pour générer un package de script de reconnaissance pour le système d'exploitation AIX, entrez la commande suivante :

```
./makeASDScriptPackage --outputDir /tmp --uname AIX --sensors computersystem
```

Cette commande crée le package de script AIX suivants dans le répertoire `tmp` : `/tmp/taddm_AIX.tar`.

2. Copiez le package de script à partir de *REP_SORTIE* sur le système cible, puis extrayez le package de script.
3. En tant que superutilisateur sur les systèmes UNIX ou qu'administrateur sur un système Windows, accordez des privilèges d'exécution sur tous les fichiers de script. Si le script de reconnaissance est exécuté en tant qu'utilisateur non superutilisateur ou non administrateur, certains scripts de détection risquent de ne pas effectuer une reconnaissance complète ou les données reconnues par le détecteur risquent d'être limitées.
4. Exécutez le script **scriptsRunner.sh** pour les cibles UNIX, ou le fichier **scriptsRunner.bat** pour la cible Windows.
5. Déplacez le fichier archive résultant (par exemple `/tmp/taddm${`*version*`}/asd/taddmasd-${`*nom_hôte*`}-${`*horodatage d'exécution*`}.tar`) vers le serveur TADDM, dans l'emplacement défini par la propriété `com.ibm.cdb.discover.asd.AsyncDiscoveryResultsDirectory` dans le fichier `collation.properties`.
6. Dans le fichier `collation.properties`, définissez la valeur de la propriété `com.ibm.cdb.discover.asd.ProcessUnreachableIPs` sur `TRUE`.
7. Vérifiez que le détecteur de reconnaissance asynchrone (`ASDSensor`) est activé dans votre profil de reconnaissance. Par défaut, le détecteur est activé dans les profils de reconnaissance de niveaux 2 et 3.
8. Créer une portée avec l'adresse IP du système cible.

Que faire ensuite

Exécutez la reconnaissance. Les droits du superutilisateur ne sont pas nécessaires pour exécuter cette reconnaissance.

Au cours de la reconnaissance, si le détecteur Ping, le détecteur de port ou le détecteur de session ne peut pas accéder au système cible, le système cible est considéré comme étant inaccessible. Si la valeur de la propriété `com.ibm.cdb.discover.asd.ProcessUnreachableIPs` est définie sur `true`, le détecteur de reconnaissance asynchrone est exécuté pour traiter le fichier archive de reconnaissance du système cible. Le fichier archive est traité uniquement si l'adresse IP de la portée de reconnaissance correspond à l'adresse IP du système qui a généré le fichier archive. Selon le contenu de ce fichier, les détecteurs sont planifiés en vue du traitement de la sortie du script. Une fois le fichier archive traité, il est renommé en *nom_fichier_tar*`.tar_done` de sorte à ne pas faire l'objet d'un second traitement.

Le fichier archive de reconnaissance est traité une seule fois. Si un détecteur n'est pas activé pour traiter la sortie du script lors du traitement du fichier archive, l'activation de ce détecteur, puis l'exécution d'une seconde reconnaissance ne permettent pas de traiter un fichier archive précédemment traité, à moins que vous ne procédiez comme suit :

1. Redonnez au fichier archive son nom d'origine. Par exemple, supprimez `_DONE` du nom de fichier.

2. Le fichier `.processed` du répertoire `$COLLATION_HOME/var/asdd` contient une liste des fichiers archive traités. Supprimez le nom du fichier archive du fichier `.processed`.

Plusieurs fichiers archive de systèmes différents peuvent être traités en une seule exécution de la reconnaissance, mais un seul fichier archive pour chaque système cible est traité. Si un système cible contient plusieurs fichiers archive, seul le plus récent est traité.

Pour reconnaître plusieurs fichiers archive à partir de différents systèmes lors d'une seule exécution de la reconnaissance, copiez chaque fichier archive à l'emplacement défini par la propriété `com.ibm.cdb.discover.asd.AsyncDiscoveryResultsDirectory`. Incluez l'adresse IP de chaque système cible dans la portée de la reconnaissance.

Etant donné que le script de reconnaissance utilise la commande **tar** pour créer le fichier archive de reconnaissance, vous devez installer un programme TAR tiers qui sera utilisé par TADDM pour extraire les fichiers du fichier archive si vous utilisez un serveur TADDM sur lequel le système d'exploitation Windows s'exécute. L'emplacement du programme TAR est défini par la propriété `com.ibm.cdb.tarpath`.

Restriction : Votre programme d'archivage sur bande doit prendre en charge les longs chemins d'accès au fichier. L'archivage sur bande GNU 1.13 n'est pas pris en charge car il risque de tronquer les noms de fichier longs.

Configuration de la reconnaissance basée sur un script

Pour exécuter une reconnaissance basée sur un script, vous devez commencer par configurer cette reconnaissance.

Pourquoi et quand exécuter cette tâche

Par rapport aux détecteurs ordinaires, les détecteurs qui sont exécutés dans le mode basé sur un script sont plus apparents. Cela signifie que toutes les commandes utilisées par le détecteur se trouvent dans un seul script, que vous pouvez afficher. Pour obtenir la liste des détecteurs qui prennent en charge le mode basé sur un script, ainsi que les restrictions qui s'appliquent à certains d'entre eux, voir la rubrique *Détecteurs prenant en charge une reconnaissance asynchrone et basée sur un script* dans le *Guide de référence des détecteurs* de TADDM.

Procédure

Configurez le détecteur de l'une des façons suivantes :

- **Activation de tous les détecteurs prenant en charge la reconnaissance basée sur un script**

  Pour activer globalement tous les détecteurs prenant en charge la reconnaissance basée sur un script, ouvrez le fichier `collation.properties`, puis définissez la valeur de la propriété `com.ibm.cdb.discover.PreferScriptDiscovery` sur `TRUE`.

-

Activation de tous les détecteurs prenant en charge la reconnaissance basée sur un script dans un profil de reconnaissance spécifique

Pour activer tous les détecteurs prenant en charge la reconnaissance basée sur un script pour un profil de reconnaissance spécifique, procédez comme suit :

1. Dans le portail de gestion de reconnaissance, sélectionnez le profil de reconnaissance pour lequel vous voulez activer le mode basé sur un script.
2. Sous l'onglet **Propriétés de plateforme**, définissez la valeur de la propriété `com.ibm.cdb.discover.PreferScriptDiscovery` sur `true`.

•

Activation d'un détecteur prenant en charge la reconnaissance basée sur un script dans un profil de reconnaissance

Pour activer un détecteur donné prenant en charge la reconnaissance basée sur un script pour un profil de reconnaissance, mettez à jour la configuration de ce détecteur dans le profil de reconnaissance concerné. Procédez comme suit :

1. Dans le portail de gestion de reconnaissance, accédez au profil de reconnaissance qui contient le détecteur que vous voulez activer.
2. Sous l'onglet **Configuration du détecteur**, sélectionnez le détecteur et cliquez sur **Nouveau**.
3. Dans la fenêtre Créer une configuration, indiquez le nom de la configuration et sélectionnez l'option **Exécuter une reconnaissance basée sur un script**.
4. Cliquez sur **OK** pour sauvegarder la configuration.

Que faire ensuite

Configuration de TADDM en vue de la sélection d'utilisateurs non par défaut pour la reconnaissance

Par défaut, seul l'utilisateur demandé par le script est utilisé pour la reconnaissance. Si vous rencontrez des problèmes lors de l'exécution d'une reconnaissance avec l'utilisateur par défaut et qu'il existe un autre utilisateur possédant toutes les autorisations requises, vous pouvez configurer TADDM de sorte que cet utilisateur soit sélectionné pour la reconnaissance.

Remarque : Utilisez la configuration suivante avec précaution. Si un utilisateur ne possédant pas toutes les autorisations requises est utilisé pour une reconnaissance, l'opération peut échouer ou certaines des cibles ne seront pas reconnues.

Dans le fichier `plugin.xml` qui se trouve dans le package de chaque détecteur dans le répertoire `COLLATION_HOME/osgi/plugins`, éditez la définition du noeud `script`, comme dans le fragment `plugin.xml` du détecteur IBM WebSphere MQ Server présenté ci-dessous :

```
<scriptset>
   <ostype>AIX</ostype>
   <mainScript name="sensorCommon.sh" />
   <script name="script.sh" authClassName="com.collation.platform.security.
auth.MQServerAuth" authMode="preferred" hostAuthFallback="true"/>
</scriptset>
```

Vous pouvez définir les propriétés suivantes :

authMode

Définit la façon dont TADDM traite les entrées de la liste d'accès pour le type spécifié par `authClassName`. Les valeurs suivantes sont disponibles :

- `single` - seul un utilisateur demandé par le script est utilisé. Il s'agit de la valeur par défaut.
- `preferred` - tout d'abord un utilisateur préféré par le script est utilisé, mais s'il n'est pas disponible ou est défaillant, les entrées restantes de la liste d'accès du type défini sont utilisées.
- `regular` - les entrées de la liste d'accès dont utilisées dans leur ordre spécifié sans vérification de la préférence utilisateur.

hostAuthFallback

Détermine si, en cas de problèmes avec la connexion établie avec la cible pour un `authClassName` spécifique ou pour l'utilisateur préféré, ou pour les deux, TADDM a recours à la session établie par l'utilisateur générique qui est utilisé pour la connexion à la cible. Les valeurs suivantes sont disponibles :

- `false` - la valeur par défaut.
- `true`.

Configuration de la reconnaissance à l'aide d'IBM Tivoli Monitoring (ancienne méthode)

TADDM peut effectuer des reconnaissances de niveaux 1 et 2 et certaines reconnaissances de niveau 3 en utilisant une infrastructure IBM Tivoli Monitoring 6.2.1 ou ultérieure.

Ancienne méthode d'intégration

Cette section s'applique à une méthode obsolète d'intégration de TADDM à IBM Tivoli Monitoring. A partir de TADDM version 7.3.0, il est recommandé d'effectuer l'intégration à IBM Tivoli Monitoring 6.3 via une automatisation OSLC. L'ancienne méthode d'intégration à l'aide d'un détecteur IBM Tivoli Monitoring Scope est obsolète et sera retirée des prochaines éditions. Pour plus d'informations sur la configuration de la reconnaissance via une automatisation OSLC, voir «Configuration pour reconnaissance sur une session d'automatisation OSLC», à la page 117.

Si vous utilisez IBM Tivoli Monitoring 6.2.1-TIV-ITM-FP0001, 6.2.2-TIV-ITM-FP0002 ou un niveau supérieur, vous pouvez reconnaître les noeuds finaux Tivoli Monitoring via Tivoli Enterprise Portal Server. Ces groupes de correctifs résolvent l'APAR IZ63983, qui améliore les performances de Tivoli Monitoring lors des reconnaissances TADDM. L'utilisation d'éditions ou de niveaux plus récents d'IBM Tivoli Monitoring pour exécuter des reconnaissances TADDM via Tivoli Enterprise Portal Server peut entraîner une charge excessive du processeur et du réseau, particulièrement sur les composants Tivoli Monitoring.

Remarque : Une reconnaissance à l'aide de IBM Tivoli Monitoring n'est possible que si la base de données de Tivoli Enterprise Portal Server est sur Microsoft SQL Server et DB2. Elle n'est pas possible si la base de données Apache Derby est utilisée comme base de données de Tivoli Enterprise Portal Server.

Propriétés du serveur TADDM spécifiques à la reconnaissance avec Tivoli Monitoring

Pour des informations sur les propriétés du serveur TADDM spécifiques à la reconnaissance avec IBM Tivoli Monitoring, y compris les propriétés affectant la

façon dont TADDM reconnaît des noeuds finaux Tivoli Monitoring, voir «Propriétés de la reconnaissance à l'aide d'IBM Tivoli Monitoring (ancienne méthode)», à la page 84.

Dans un profil de reconnaissance, vous pouvez configurer les propriétés du serveur TADDM affectant la façon dont TADDM reconnaît les noeuds finaux Tivoli Monitoring. Pour ce faire, procédez comme suit, selon si vous utilisez un profil personnalisé ou le profil par défaut :

Configuration des propriétés pour un profil personnalisé

1. Démarrez la console de gestion de reconnaissance.
2. Ouvrez **Profils de reconnaissance**.
3. Cliquez sur le profil de reconnaissance que vous voulez configurer.
4. Cliquez sur l'onglet **Propriétés de la plateforme**.
5. Changez la valeur de la propriété que vous voulez mettre à jour et cochez la case **Inclus** correspondante.
6. Sauvegardez les changements.

Configuration des propriétés pour le profil par défaut

Dans le fichier `$COLLATION_HOME/etc/collation.properties`, ajoutez (ou modifiez) la propriété correspondante, comme indiqué dans l'exemple suivant, où *profil_reconnaissance* correspond au nom du profil de reconnaissance :

```
com.ibm.cdb.session.allow.ITM.profil_reconnaissance=true
```

Par exemple, la propriété suivante indique que TADDM utilise le profil de reconnaissance «Utilization Discovery» et IBM Tivoli Monitoring pour reconnaître les noeuds finaux Tivoli Monitoring :

```
com.ibm.cdb.session.allow.ITM.Utilization_Discovery=true
```

Remarque : Dans le fichier `collation.properties`, vous devez remplacer le caractère espace entre «Utilization» et «Discovery» dans le nom du profil par un caractère de soulignement.

Autres propriétés du serveur TADDM éventuellement à configurer

Les conseils suivants décrivent d'autres propriétés du serveur TADDM devant éventuellement être configurées :

- La valeur de la propriété suivante, spécifique aux systèmes Windows, doit être définie à `true` (la valeur par défaut) pour permettre la reconnaissance des systèmes cible Windows à l'aide d'IBM Tivoli Monitoring. Si la valeur est définie à `false`, TADDM ne peut pas établir une session IBM Tivoli Monitoring sur les systèmes cible Windows.

  ```
  com.collation.AllowPrivateGateways=true
  ```

- Le processeur de Tivoli Enterprise Portal Server risque d'être très sollicité lors de la reconnaissance. Pour réduire la charge pesant sur ce processeur, vous pouvez limiter le nombre d'unités d'exécution s'exécutant lors de la reconnaissance. Définissez la propriété suivante sur le serveur TADDM :

  ```
  com.collation.discover.dwcount=16
  ```

- Dans un environnement IBM Tivoli Monitoring de grande taille, le détecteur de portée IBM Tivoli Monitoring peut dépasser le délai d'attente avant la fin de son exécution. Pour autoriser un temps de traitement plus long, définissez les propriétés du serveur suivantes :

```
com.collation.platform.session.ITMSessionNumProgressChecks=3600
com.collation.discover.agent.ITMScopeSensor.timeout=3600000
```

Configuration pour reconnaissance sur une session d'automatisation OSLC

TADDM peut exécuter des reconnaissances de niveau 2 (L2) et certaines de niveau 3 (L3) via OSLC.

Avant de commencer

Pour configurer la reconnaissance sur des ensembles de portées fournis par des fournisseurs de services d'automatisation d'exécution OSLC, vous devez satisfaire aux exigences suivantes :

- Vous devez avoir au moins un fournisseur de services d'automatisation d'exécution OSLC installé et en fonctionnement.
- TADDM doit être connecté au fournisseur de services d'automatisation d'exécution OSLC.

Procédure

Pour exécuter une reconnaissance sur une session d'automatisation OSLC, procédez comme suit :

1. Ajoutez des données d'identification d'accès du produit que vous intégrez à la liste d'accès. Pour cela, créez une nouvelle entrée de liste d'accès du type `"Integration">"OSLC Automation"`. Si vous intégrez TADDM à ITM, fournissez des données d'identification ITM TEPS. Pendant la reconnaissance, des entrées de liste d'accès à l'automatisation OSLC et un type d'entrée de liste d'accès ITM sont utilisés pour assurer la compatibilité avec des versions antérieures.
2. Vérifiez la portée de reconnaissance. L'agent OSLCAutomationAgent crée périodiquement les ensembles de portées. Les nouveaux ensembles de portées sont répertoriés sous l'onglet **Ensembles de portées**. Si vous intégrez TADDM à ITM, un ensemble de portées est créé pour chaque ITM TEMS. Vous pouvez exécuter l'agent OSLCAutomationAgent manuellement à l'aide de la commande suivante :

   ```
   /taddm/dist/support/bin/runtopobuild.sh -a OSLCAutomationAgent
   ```
3. Configurez les propriétés de reconnaissance qui permettent l'utilisation d'une session d'automatisation OSLC. Vous pouvez définir les propriétés dans le fichier `collation.properties` ou dans un nouveau profil de reconnaissance personnalisée.
   - Le fichier `collation.properties` :

     ```
     com.ibm.cdb.session.prefer.OSLCAutomation=true
     com.ibm.cdb.session.allow.OSLCAutomation=true
     ```

     Les exemples de propriétés sectorisées :

     ```
     com.ibm.cdb.session.prefer.OSLCAutomation.9.222.222.124=false
     com.ibm.cdb.session.prefer.OSLCAutomation.Level_3_Discovery=false
     ```
   - Profil de reconnaissance personnalisé. Dans la console de gestion de reconnaissance, créez un profil de reconnaissance et configurez l'onglet **Propriétés de plateforme** de la manière suivante :

     ```
     com.ibm.cdb.session.allow.OSLCAutomation=true
     com.ibm.cdb.session.prefer.OSLCAutomation=true
     ```
4. Exécutez une reconnaissance de portée régulière créée par l'agent OSLCAutomationAgent en sélectionnant l'une des méthodes suivantes :

- Le profil L2 ou L3 par défaut, lorsque le fichier `collation.properties` est configuré pour prendre en charge une session d'automatisation OSLC.
- Le nouveau profil dont l'onglet **Propriétés de plateforme** est correctement configuré.

Référence associée:

«Propriétés pour une reconnaissance via une session d'automatisation OSLC», à la page 86
Ces propriétés s'appliquent à une reconnaissance via une session d'automatisation OSLC.

«Interface de ligne de commande pour OSLCAutomationAgent», à la page 216
OSLCAutomationAgent permet de collecter des données provenant des fournisseurs de services d'automatisation d'exécution OSLC. Vous pouvez utiliser des commandes pour exécuter l'agent manuellement et pour actualiser ou mettre à jour les ensembles de portées qu'il crée.

Configuration du niveau de reconnaissance

Vous devez configurer le niveau de reconnaissance.

Configuration pour la reconnaissance de niveau 1

Une configuration minimale est obligatoire pour la reconnaissance de niveau 1 (sans droits d'accès), qui analyse la pile TCP/IP pour rassembler des informations de base sur les systèmes informatiques actifs.

Pourquoi et quand exécuter cette tâche

Pour la reconnaissance de niveau 1, vous devez configurer les périphériques réseau dans l'environnement que le serveur TADDM doit reconnaître.

Procédure

Pour ce faire, procédez comme suit :

1. En fonction de votre version SNMP, enregistrez les informations suivantes pour utilisation avec le serveur TADDM :
   - Pour SNMP V1 et V2, enregistrez la chaîne SNMP MIB2 GET COMMUNITY.
   - Pour SNMP V3, enregistrez le nom d'utilisateur et le mot de passe SNMP.
2. Attribuez des droits pour les interfaces étendues, les interfaces, le protocole IP et le système MIB2.

Configuration pour la reconnaissance de niveau 2

Outre les conditions requises pour la reconnaissance de niveau 1, la reconnaissance de niveau 2 requiert une configuration permettant de prendre en charge la reconnaissance d'informations de configuration détaillées sur les hôtes.

Avant de commencer

Si les systèmes cible sont des noeuds finaux IBM Tivoli Monitoring reconnus par le détecteur IBM Tivoli Monitoring Scope, les autorisations d'accès pour ces systèmes ne sont pas obligatoires pour la reconnaissance de niveau 2. Pour plus d'informations, voir les sources suivantes :

- «Intégration de TADDM à IBM Tivoli Monitoring (ancienne méthode)», à la page 217
- «Configuration de la reconnaissance à l'aide d'IBM Tivoli Monitoring (ancienne méthode)», à la page 115

- *Guide de référence des détecteurs* de TADDM pour en savoir plus sur le détecteur IBM Tivoli Monitoring Scope

Pourquoi et quand exécuter cette tâche

Sur les systèmes d'exploitation cible (systèmes informatiques) que TADDM doit reconnaître, vous devez au moins configurer le logiciel suivant :

Secure Shell (SSH)
Vous pouvez utiliser OpenSSH ou la version fournisseur du service SSH proposée avec le système d'exploitation. Pour plus d'informations sur les systèmes d'exploitation Windows, voir «Dépendance de Windows Management Instrumentation (WMI)», à la page 133.

SUNWscpu (environnement Solaris uniquement)
Pour fournir des informations complètes sur les processus, installez le module SUNWscpu (compatibilité source).

Fichiers ouverts LiSt (lsof)
Pour fournir des informations complètes sur les dépendances, installez le programme LiSt Open Files (lsof) selon les *exigences lsof* dans le Wiki TADDM à l'adresse https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Application%20Dependency%20Discovery%20Manager/page/TADDM%20lsof%20requirements.

Création du compte de service :

Vous devez créer un compte de service sur tous les systèmes informatiques reconnus à l'aide des connexions SSH à base de clés et de mots de passe. Il s'agit de la méthode principale de reconnaissance des systèmes informatiques (serveurs) dans votre réseau.

Pourquoi et quand exécuter cette tâche

Pour simplifier la configuration de la reconnaissance, créez le même compte de service sur chaque système informatique cible à reconnaître. Le compte de service doit autoriser l'accès à toutes les ressources du système informatique cible que TADDM doit reconnaître. Ce compte doit disposer des droits d'accès en écriture au répertoire de base de chaque système informatique cible. Ce répertoire requiert environ 20 Mo d'espace disponible. Au cours d'une reconnaissance, les scripts et les fichiers de résultats temporaires peuvent être stockées dans ce répertoire. Une fois la reconnaissance exécutée, les fichiers sont supprimés.

Vous pouvez utiliser un compte de service sans droits administrateur. Toutefois, pour exécuter le système informatique cible, certaines commandes du système d'exploitation utilisées lors de la reconnaissance peuvent demander un privilège élevé (comme root ou superutilisateur).

Procédure

Effectuez l'une des procédures suivantes pour créer un compte de service sur le système informatique cible :

1. Pour un système d'exploitation Linux, Solaris, AIX et Linux pour System z, supposez que le nom du compte de service est `coll` et utilisez les commandes suivantes pour créer un compte de service :

```
# mkdir -p /export/home/coll
# useradd -d /export/home/coll -s /bin/sh \
   -c "Service Account" -m coll
# chown -R coll /export/home/coll
```

2. Pour un système informatique Windows, créez un compte de service qui est membre du groupe de l'administrateur local. Ce compte peut être un compte local ou un compte de domaine. Etant donné que TADDM compte sur WMI pour la reconnaissance, le compte doit avoir accès à tous les objets WMI de l'ordinateur local. Le compte de service doit être créé sur la passerelle Windows et sur tous les systèmes informatiques cibles Windows.

   Remarque : Le compte de service doit disposer d'un accès en lecture/écriture au répertoire `\WINDOWS\system32` ou `\WINDOWS\system64` et aux sous-répertoires qu'il contient. Sur les systèmes Windows Server 2008, les nouveaux utilisateurs ne disposent pas de l'accès requis par défaut. Vous devez donc l'accorder explicitement pour le compte de service.

Configuration de la reconnaissance avec Secure Shell (SSH) :

Le serveur TADDM peut se connecter à OpenSSH (version 1 ou 2) ou à la version de SSH offerte par le fournisseur du système d'exploitation.

Le serveur TADDM prend en charge les méthodes d'authentification suivantes :

- Connexion par clé SSH2 (clés RSA ou DSA) et connexion par clé SSH1 (RSA uniquement)
- Nom d'utilisateur et mot de passe à l'aide de SSH2, et nom d'utilisateur et mot de passe à l'aide de SSH1

Bien que vous puissiez utiliser l'une ou l'autre de ces méthodes d'authentification, il est conseillé d'utiliser la connexion à base de clés SSH2. Le serveur essaye automatiquement chaque méthode dans l'ordre indiqué ici et utilise la première qui fonctionne correctement. Le serveur TADDM utilise alors la même méthode avec cet hôte pour l'exécution complète de la reconnaissance.

Remarque : Pour une connexion par clé SSH2, le serveur TADDM tente de se connecter uniquement avec une clé (RSA ou DSA) disponible sur le serveur TADDM. Si les deux clés existent, seule la clé RSA est utilisée.

Création de paires de clés pour la connexion par clé avec le serveur TADDM :

Vous pouvez créer une paire de clés publique/privée à l'aide du protocole SSH (Secure Shell) pour les connexions par clé avec le serveur TADDM.

Pourquoi et quand exécuter cette tâche

Selon la version du service SSH employée, la connexion par clé SSH utilise les clés répertoriées dans le tableau 34.

Tableau 34. Clés SSH

Version SSH/Algorithme	Clé privée	Clé publique
Openssh/SSH2/RSA	$HOME/.ssh/id_rsa	$HOME/.ssh/id_rsa.pub
Openssh/SSH2/DSA	$HOME/.ssh/id_dsa	$HOME/.ssh/id_dsa.pub
Openssh/SSH1/RSA	$HOME/.ssh/identity	$HOME/.ssh/identity.pub

Tableau 34. Clés SSH (suite)

Version SSH/Algorithme	Clé privée	Clé publique
Commercial/SSH2/RSA	$HOME/.ssh2/id_dss_1024_a	$HOME/.ssh2/id_dss_1024_a .pub

Vous pouvez également générer une paire de clés publique/privée à l'aide d'OpenSSH, version 2. Pour générer une paire de clés publique/privée à l'aide d'un programme SSH autre que OpenSSH ou une autre version de OpenSSH, consultez la documentation SSH.

Procédure

Pour générer une paire de clés publique/privée à l'aide de OpenSSH, version 2, procédez comme suit :

1. Connectez-vous en tant que propriétaire du serveur TADDM.
2. Pour générer la clé SSH, entrez la commande suivante :

   ```
   $ ssh-keygen -t rsa
   ```

   Acceptez les valeurs par défaut de la commande. TADDM prend en charge les paires de clés avec ou sans phrase passe.
3. Sur chaque ordinateur hôte sur lequel vous souhaitez autoriser la connexion par clé, insérez le contenu du fichier `id_rsa.pub` dans le fichier*$HOME*`/.ssh/authorized_keys` correspondant au compte de service. Certaines implémentations SSH2 génèrent des clés dans un répertoire autre que `$HOME/.ssh`. Si votre implémentation SSH génère des clés dans un autre répertoire ou sous un autre nom, vous devez copier, lier ou déplacer le fichier de clés privées vers le répertoire *$HOME*`/.ssh/id_rsa` ou *$HOME*`/.ssh/id_dsa`, en fonction de l'algorithme.

Ajout d'une entrée de liste d'accès pour le compte de service du système informatique :

Pour configurer l'authentification par mot de passe avec Secure Shell (SSH), vous devez ajouter une entrée de liste d'accès pour le compte de service du système informatique créé sur le système cible.

Pour ajouter une entrée de liste d'accès pour le compte de service du système informatique, procédez comme suit :

1. Dans la page de démarrage de TADDM, vérifiez que tous les services dans la console d'administration ont été démarrés.
2. Démarrez la console de gestion de reconnaissance.
3. Cochez la case **Etablir une session sécurisée (SSL)** pour utiliser l'option de sécurité SSL. Cette option chiffre toutes les données, y compris les noms d'utilisateur et les mots de passe des listes d'accès, avant leur envoi entre la console de gestion de reconnaissance et le serveur TADDM.
4. Ajoutez une entrée de liste d'accès de système informatique pour le compte de service et précisez le nom et le mot de passe de connexion.

Configuration de System p et System i :

La reconnaissance d'un système basé sur la technologie IBM Power5 (System p ou System i) et ses partitions logiques est réalisée via une console de gestion. TADDM prend en charge deux types de console de gestion : la console HMC (Hardware Management Console) et la console IVM (Integrated Virtualization Manager).

TADDM reconnaît la console de gestion avec SSH. La portée de la reconnaissance doit inclure l'adresse IP de la console de gestion et la liste d'accès doit contenir une entrée de type Système informatique avec les autorisations d'accès appropriées (nom d'utilisateur et mot de passe).

Outre les données d'identification de l'utilisateur, l'utilisateur de la reconnaissance doit être défini sur la console de gestion avec les autorisations minimales suivantes :

- Console HMC (Hardware Management Console)
  - Pour une console de gestion HMC, un utilisateur basé sur le rôle **hmcoperator** est requis. Par exemple, créez un rôle appelé *taddmViewOnly* à partir du rôle hmcoperator. De plus, les tâches de la ligne de commande suivantes doivent être attribuées au nouveau rôle :

    Système géré
    Nécessaire pour utiliser les commandes **lshwres** et **lssyscfg**.

    Partition logique
    Nécessaire pour utiliser les commandes **lshwres**, **lssyscfg** et **viosvrcmd**.

    Configuration HMC
    Nécessaire pour utiliser la commande **lshmc**.
- Integrated Virtualization Manager (IVM).

  Pour une console de gestion IVM, un utilisateur avec le rôle **Affichage uniquement** est requis.

Configuration pour la reconnaissance de niveau 3

Outre les conditions requises pour la reconnaissance de niveau 2, la reconnaissance de niveau 3 requiert une configuration afin de prendre en charge la reconnaissance des données d'hôte et de configuration d'applications.

Configuration des serveurs Web et d'applications pour la reconnaissance :

Vous devez configurer les serveurs Web et les serveurs d'applications dans l'environnement que vous souhaitez que le serveur TADDM reconnaisse.

Cette section présente les étapes de configuration des serveurs Web et d'applications.

Le serveur Microsoft IIS ne nécessite pas de configuration. Il n'existe aucune condition d'accès. Le compte utilisateur déjà établi sur le système hôte est suffisant.

Pour le serveur Web Apache, le compte de service TADDM du système hôte doit disposer des droits en lecture sur les fichiers de configuration Apache tels que le fichier `httpd.conf`.

Pour le serveur Web Oracle iPlanet, le compte de service TADDM pour le système hôte doit disposer des droits en lecture sur les fichiers de configuration iPlanet.

Pour les serveurs Lotus Domino, vérifiez que vous remplissez les conditions requises décrites à la rubrique *Détecteur de serveur IBM Lotus Domino* de la *Référence de détecteurs* de TADDM.

Configuration d'un serveur d'applications Oracle :

La reconnaissance d'un serveur d'applications Oracle utilise des fichiers JAR fournis avec ce serveur. Ces fichiers JAR ne sont pas inclus dans l'installation du serveur TADDM.

Pourquoi et quand exécuter cette tâche

Une des propriétés du fichier `$COLLATION_HOME/etc/collation.properties` permet de pointer vers une installation existante du serveur d'applications Oracle. Le texte suivant se trouve dans le fichier `$COLLATION_HOME/etc/collation.properties` :

```
# Emplacement du répertoire
principal du serveur d'applications Oracle sur
Tivoli Application Dependency Discovery Manager
# 1. Voici un exemple /home/oracle/product/10.1.3/OracleAS_1
# 2. Un répertoire relatif est un parent de com.collation.home
# 3. Ce répertoire (et ses sous-répertoires) doit être accessible
     à l'utilisateur sous lequel fonctionne le serveur, en règle générale l'utilisateur
     collation.
# 4. Ignorez si vous n'envisagez pas d'effectuer une reconnaissance de serveur
     d'applications Oracle.
```

Pour pointer vers une installation existante du serveur d'applications Oracle, modifiez la ligne suivante du fichier `$COLLATION_HOME /etc/collation.properties` :

```
com.collation.oracleapp.root.dir=lib/oracleapp
```

Au sein d'une installation du serveur d'applications Oracle, les répertoires qui contiennent les fichiers JAR requis appartiennent à l'utilisateur `oracle` disposant des droits suivants : `rwx------`. Cela signifie qu'aucun utilisateur à l'exception du propriétaire (une application Oracle, en règle générale) ne peut accéder à ces répertoires. Si le serveur TADDM est exécuté à l'aide de l'utilisateur `oracle`, ces répertoires sont accessibles. Toutefois, si tel n'est pas le cas, vous devez modifier les droits d'accès aux répertoires suivants en indiquant `711` afin que tous les utilisateurs puissent y accéder :

- *OracleAppServerHome*
- *OracleAppServerHome*`/j2ee`
- *OracleAppServerHome*`/j2ee/home`
- *OracleAppServerHome*`/opmn`
- *OracleAppServerHome*`/opmn/lib`, où *OracleAppServerHome* peut par exemple prendre la valeur `/home/oracle/product/10.1.3/OracleAS_1`

Pour la reconnaissance d'un serveur d'applications Oracle, la propriété com.collation.platform.os.ignoreLoopbackProcesses du fichier `$COLLATION_HOME/etc/collation.properties` doit être définie sur `true`:

```
com.collation.platform.os.ignoreLoopbackProcesses=true
```

Procédure

Pour configurer cette liste d'accès, procédez comme suit :

1. Dans la console de gestion de reconnaissance, créez un ensemble de portées de reconnaissance contenant votre serveur d'applications Oracle ou utilisez une portée existante contenant ce serveur.
2. Pour créer une liste d'accès, cliquez sur l'icône **Liste d'accès**.
3. Dans la fenêtre Liste d'accès, cliquez sur **Ajouter**.

4. Dans la zone **Type de composant** de la fenêtre Caractéristiques de l'accès, cliquez sur **Serveurs d'applications**.
5. Dans la zone **Fournisseur**, cliquez sur **Serveur d'applications Oracle**.
6. Entrez les autorisations d'accès au serveur d'applications Oracle.

Configuration du serveur Microsoft Exchange :

Vous devez configurer le serveur Microsoft Exchange que le serveur TADDM doit reconnaître.

Pourquoi et quand exécuter cette tâche

Pour reconnaître le serveur Microsoft Exchange, le service de gestion Microsoft Exchange doit être en cours d'exécution sur le systèmeWindows. L'ID de service Windows du compte de service TADDM doit être créé sur le système Windows sur lequel le serveur Microsoft Exchange s'exécute. L'ID de service Windows doit posséder des droits d'accès complets (Execute Methods, Full Write, Partial Write, Provider Write, Enable Account, Remote Enable, Read Security et Edit Security) aux espaces de nom WMI suivants :

- Root\CIMV2
- Root\CIMV2\Applications\Exchange
- Root\MicrosoftExchangeV2

Si l'ID de service Windows du compte de service TADDM possède les droits suffisants pour reconnaître un serveur Microsoft Exchange, le détecteur utilise l'ID de service Windows et une entrée distincte dans la liste d'accès au serveur Microsoft n'est pas nécessaire.

Si l'ID de service Windows du compte de service TADDM ne dispose pas des droits suffisants pour reconnaître un serveur Microsoft Exchange, vous devez créer une liste d'accès au serveur Microsoft Exchange distincte.

Procédure

Pour configurer cette liste d'accès, procédez comme suit :

1. Dans la console de gestion de reconnaissance, créez un ensemble de portées de reconnaissance contenant votre serveur Microsoft Exchange ou utilisez une portée existante contenant votre serveur Microsoft Exchange.
2. Pour créer une liste d'accès, cliquez sur l'icône **Liste d'accès**.
3. Dans la fenêtre Liste d'accès, cliquez sur **Ajouter**.
4. Dans la zone **Type de composant** de la fenêtre Caractéristiques de l'accès, cliquez sur **Serveurs de messagerie**.
5. Dans la zone **Fournisseur**, cliquez sur **Microsoft Exchange Server**.
6. Entrez les autorisations d'accès pour le serveur Microsoft Exchange.

Configuration de serveurs VMware :

Une fois correctement configuré, le processus de reconnaissance TADDM renvoie des informations sur les serveurs VMware.

Pourquoi et quand exécuter cette tâche

Pour configurer les serveurs VMware en vue de la reconnaissance, attribuez un droit d'accès en lecture seule au compte de service TADDM ne disposant pas des privilèges d'un superutilisateur dans la console VMware ESX. Vous pouvez sinon utiliser le superutilisateur dans le cadre de la reconnaissance. Pour plus d'informations sur les serveurs VMware, vous pouvez faire des recherches dans les rubriques de la communauté VMware à l'adresse https://communities.vmware.com/welcome.

Base de données configurée pour la reconnaissance :

Pour prendre en charge la reconnaissance de vos bases de données, vous devez créer des utilisateurs de base de données DB2, Oracle ou Sybase pour le serveur TADDM. Celui-ci utilise ces utilisateurs pour collecter des informations sur les bases de données qui sont exécutées sur les hôtes distants.

Création d'un utilisateur DB2 :

Pour effectuer une reconnaissance plus complète d'instances DB2 sur les hôtes informatiques distants, créez un utilisateur DB2.

Procédure

Pour créer un utilisateur DB2, procédez comme suit :

1. Créez un utilisateur ayant accès aux éléments suivants :
   - Serveur TADDM de base de données DB2
   - Totalité des instances du serveur TADDM de base de données DB2 qui doivent être reconnues
2. Configurez cet utilisateur DB2 pour qu'il dispose d'un accès SSH au système qui héberge le serveur de base de données DB2.
3. Dans la liste d'accès au serveur TADDM, procédez comme suit pour ajouter le nom d'utilisateur et le mot de passe de l'utilisateur de DB2 :
   a. Dans la barre d'outils de la console de gestion de reconnaissance, cliquez sur **Reconnaissance** > **Liste d'accès**. La sous-fenêtre Liste d'accès s'affiche.
   b. Cliquez sur **Ajouter**. La fenêtre Caractéristiques de l'accès s'affiche.
   c. Dans la fenêtre Caractéristiques de l'accès, entrez les informations suivantes :
      1) Dans la liste **Type de composant**, sélectionnez **Base de données**.
      2) Dans la liste **Fournisseur**, sélectionnez **DB2**.
      3) Entrez le nom, le nom d'utilisateur et le mot de passe pour l'utilisateur DB2.
   d. Cliquez sur **OK** pour enregistrer vos informations. Les nouvelles informations s'affichent dans le panneau Liste d'accès.

Création d'un utilisateur Microsoft SQL Server :

Pour reconnaître de façon plus complète des instances Microsoft SQL Server sur des hôtes distants, créez un utilisateur Microsoft SQL Server.

Procédure

Pour créer un utilisateur Microsoft SQL Server, procédez comme suit :

1. Créez un utilisateur Microsoft SQL Server avec les privilèges du rôle `db_datareader` et le droit d'accès `VIEW_ANY_DEFINITION`. Cela doit éventuellement être complété par l'administrateur Microsoft SQL Server.
2. Dans la console de gestion de reconnaissance, procédez comme suit pour ajouter le nom d'utilisateur et le mot de passe de l'utilisateur du serveur Microsoft SQL dans la liste d'accès au serveur TADDM :
   a. Dans la barre d'outils, cliquez sur **Reconnaissance** > **Liste d'accès**. La sous-fenêtre Liste d'accès s'affiche.
   b. Cliquez sur **Ajouter**. La fenêtre Caractéristiques de l'accès s'affiche.
   c. Dans la fenêtre Caractéristiques de l'accès, entrez les informations suivantes :
      1) Dans la liste **Type de composant**, sélectionnez **Base de données**.
      2) Dans la liste **Fournisseur**, sélectionnez **Microsoft SQL Server**.
      3) Entrez le **nom**, le **nom d'utilisateur** et le **mot de passe**.
   d. Cliquez sur **OK** pour enregistrer vos informations. Les nouvelles informations s'affichent dans le panneau Liste d'accès.

Création d'un utilisateur Oracle :

Pour effectuer une reconnaissance plus complète d'instances Oracle sur des hôtes informatiques distants, créez un utilisateur Oracle.

Procédure

Pour créer un utilisateur Oracle, procédez comme suit :

1. Créez un utilisateur Oracle avec des privilèges SELECT_CATALOG_ROLE. Cette opération devra probablement être effectuée par l'administrateur Oracle.

   Par exemple, utilisez la commande suivante pour créer l'utilisateur Oracle IBM :

   ```
   create user collation identified by collpassword;
   grant connect, select_catalog_role to collation;
   ```
2. Dans la console de gestion de reconnaissance, procédez comme suit pour ajouter le nom d'utilisateur et le mot de passe de l'utilisateur Oracle dans la liste d'accès au serveur TADDM :
   a. Dans la barre d'outils, cliquez sur **Reconnaissance** > **Liste d'accès**. La sous-fenêtre Liste d'accès s'affiche.
   b. Cliquez sur **Ajouter**. La fenêtre Caractéristiques de l'accès s'affiche.
   c. Dans la fenêtre Caractéristiques de l'accès, entrez les informations suivantes :
      1) Dans la liste **Type de composant**, sélectionnez **Base de données**.
      2) Dans la liste **Fournisseur**, sélectionnez **Oracle**.
      3) Entrez le nom, le nom d'utilisateur et le mot de passe pour l'ordinateur.
   d. Cliquez sur **OK** pour enregistrer vos informations. Les nouvelles informations s'affichent dans le panneau Liste d'accès.

Création d'un utilisateur Sybase :

Pour effectuer une reconnaissance complète de Sybase ASE sur des hôtes informatiques distants, créez un utilisateur Sybase affecté à un rôle approprié.

Procédure

Pour créer un utilisateur de Sybase, procédez comme suit :

1. Utilisez la commande suivante pour créer un utilisateur Sybase membre du rôle sa.

   ```
   sp_role "grant",sa_role,IBM
   ```

   Vérifiez que l'utilisateur Sybase IQ est un membre administrateur de base de données. Dans le cas contraire, les informations spécifiques à la base de données Sybase IQ sont introuvables.
2. Dans la console de gestion de reconnaissance, procédez comme suit pour ajouter le nom d'utilisateur et le mot de passe de l'utilisateur Oracle dans la liste d'accès au serveur TADDM :
   a. Pour créer une liste d'accès, cliquez sur l'icône **Liste d'accès**.
   b. Dans la fenêtre Liste d'accès, cliquez sur **Ajouter**.
   c. Dans la zone **Type de composant** de la fenêtre Caractéristiques de l'accès, cliquez sur **Base de données**.
   d. Dans la zone **Fournisseur**, cliquez sur**Base de données**.
   e. Entrez les donnée d'identification (nom d'utilisateur et mot de passe) pour établir la connectivité JDBC (Java Database Connectivity) au serveur Sybase.

Configuration pour la reconnaissance de systèmes Windows

Pour la reconnaissance de systèmes informatiques Windows, TADDM prend en charge la reconnaissance par passerelle et la reconnaissance SSH, ainsi que la reconnaissance asynchrone et basée sur un script.

Pour plus d'informations sur la reconnaissance asynchrone, voir «Configuration de la reconnaissance asynchrone», à la page 109. Pour plus d'informations sur la reconnaissance basée sur un script, voir «Configuration de la reconnaissance basée sur un script», à la page 113.

La reconnaissance par passerelle nécessite un système informatique Windows, accessible via SSH, pour servir de passerelle. Les requêtes de reconnaissance traversent la passerelle. La passerelle utilise Windows Management Instrumentation (WMI) pour reconnaître les systèmes informatiques Windows cible.

Fix Pack 2 Si vous utilisez TADDM version 7.3.0.2 ou ultérieure, vous pouvez utiliser une session PowerShell au lieu de WMI pour reconnaître les systèmes informatiques Windows cible. Vous pouvez configurer TADDM pour qu'il autorise uniquement la communication via la session PowerShell. Pour plus d'informations, voir la rubrique *Configuration pour la reconnaissance via un pare-feu sans ancrage* dans le *Guide d'utilisation* de TADDM.

La reconnaissance SSH ne requiert pas de système informatique de passerelle dédiée. La reconnaissance se sert d'une connexion SSH directe au système informatique Windows cible.

En général, la reconnaissance par passerelle est préférée à la reconnaissance SSH, car il est plus simple de configurer la passerelle et WMI ou PowerShell que de configurer SSH. WMI est disponible par défaut sur tous les systèmes cible Windows pris en charge par TADDM. PowerShell est pris en charge uniquement pour les cibles exécutant Windows Server 2008 ou ultérieur. PowerShell version 2, ou une version ultérieure, doit être installé sur la passerelle et les systèmes cible. A

part l'ordinateur passerelle, qui requiert un serveur SSH, aucun autre logiciel n'est requis pour les cibles Windows. Toutefois, la reconnaissance SSH peut s'avérer plus rapide car aucune passerelle n'est impliquée dans le flux de reconnaissance et aucun fournisseur WMI n'est déployé.

L'exécution d'une reconnaissance directe nécessite un serveur SSH sur chaque système Windows cible. De plus, pour la reconnaissance directe à l'aide de SSH, vous devez installer Microsoft .NET Framework version 2 ou 3 sur chaque système Windows cible. Notez que .NET Framework n'est pas installé par défaut sur Windows Server 2000.

Remarque : Fix Pack 2 Si vous utilisez TADDM version 7.3.0.2 ou ultérieure, vous pouvez également installer .NET Framework version 4 ou 4.5.

Les deux types de reconnaissance utilisent le programme de reconnaissance Windows TADDM (le fichier TaddmTool.exe). La reconnaissance par passerelle déploie le programme TaddmTool dans la passerelle lors de l'initialisation de la reconnaissance. La reconnaissance SSH déploie le programme TaddmTool sur chaque système informatique Windows cible. Le programme TaddmTool est une application .NET.

Par défaut, TADDM est configuré pour utiliser uniquement une reconnaissance par passerelle. Cette configuration est contrôlée par les deux propriétés de serveur TADDM suivantes, décrites dans le *Guide de référence des détecteurs* de TADDM pour le détecteur du système informatique Windows :

- `com.collation.AllowPrivateGateways=true`
- `com.collation.PreferWindowsSshOverGateway=false`

Par défaut, TADDM est configuré pour utiliser la session WMI. Pour savoir dans quels cas utiliser la session PowerShell et comment l'activer, voir «Session PowerShell», à la page 133.

Que vous utilisiez une passerelle Windows avec WMI ou vous connectiez directement avec SSH, les informations récupérées sont identiques. La liste suivante indique les conditions prérequises pour la reconnaissance par passerelle et la SSH :

Conditions prérequises pour la reconnaissance par passerelle avec WMI

1. Un système informatique Windows Server dédié est requis en tant que passerelle. Les exigences pour le système d'exploitation concernant les serveur de passerelle sont identiques à celle du système d'exploitation Windows pour les serveurs TADDM. Pour plus d'informations sur les systèmes d'exploitation Windows pris en charge, voir la rubrique *Configuration logicielle requise du serveur TADDMT* dans le *Guide d'installation* de TADDM.
2. La passerelle doit se trouver dans la même zone de pare-feu que les ordinateurs Windows pour être reconnue.
3. Vous devez installer une version de serveur SSH prise en charge sur le système informatique de la passerelle.
4. La passerelle utilise WMI à distance pour reconnaître chaque ordinateur cible Windows. En outre, un fournisseur WMI est automatiquement déployé sur chaque système informatique Windows cible lors de l'initialisation de la reconnaissance. Le fournisseur WMI est utilisé pour reconnaître les données qui ne sont pas incluses dans le WMI central.

Activez WMI sur le système informatique Windows cible à reconnaître. Par défaut, WMI est activé sur la plupart des systèmes Windows 2000 et ultérieurs.

Fix Pack 2 **Conditions prérequises pour la reconnaissance par passerelle avec PowerShell**

1. Un système informatique Windows Server dédié est requis en tant que passerelle. Les exigences pour le système d'exploitation concernant les serveur de passerelle sont identiques à celle du système d'exploitation Windows pour les serveurs TADDM. Pour plus d'informations sur les systèmes d'exploitation Windows pris en charge, voir la rubrique *Configuration logicielle requise du serveur TADDMT* dans le *Guide d'installation* de TADDM.
2. PowerShell version 2, ou une version ultérieure, doit être installé sur la passerelle et les systèmes cible. Seules les cibles exécutant Windows Server 2008 ou ultérieur sont prises en charge.
3. La passerelle doit être configurée via la commande suivante :

   ```
   Set-Item WSMan:\localhost\Client\TrustedHosts * -Force
   ```

   Cette commande définit la liste **trustedHosts**. Par défaut, la liste existe mais elle est vide ; ainsi, elle doit être définie avant que la session à distance ne soit ouverte. Le paramètre `-Force` force PowerShell à exécuter la commande sans que vous ayez besoin de confirmer chaque étape.
4. Les systèmes cible doivent être configurés via la commande suivante :

   ```
   Enable-PSRemoting -Force
   ```

   Cette commande démarre le service WinRM, le configure de sorte qu'il démarre automatiquement avec votre système et crée une règle de pare-feu afin d'autoriser les connexions entrantes. Le paramètre `-Force` force PowerShell à exécuter ces actions sans que vous ayez besoin de confirmer chaque étape.

Conditions prérequises pour la reconnaissance SSH

1. Vous devez installer une version de serveur SSH prise en charge sur chaque système Windows cible.
2. Vous devez installer Microsoft .NET Framework version 2 ou 3 sur chaque système Windows Server cible.

   Remarque : Fix Pack 2 Si vous utilisez TADDM version 7.3.0.2 ou ultérieure, vous pouvez également installer .NET Framework version 4 ou 4.5.

Voir également la rubrique *Configuration pour une reconnaissance Windows non administrateur* dans le *Guide de référence des détecteurs* de TADDM.

Configuration de Bitvise WinSSHD

Vous pouvez utiliser Bitvise WinSSHD pour fournir un accès SSH aux systèmes Windows.

Avant de commencer

Pour une reconnaissance basée sur une passerelle, Bitvise WinSSHD doit être installé sur le système de passerelle. Pour une reconnaissance SSH directe, Bitvise WinSSHD doit être installé sur chaque système Windows.

Pour plus d'informations sur les versions de Bitvise WinSSHD prises en charge, reportez-vous à la rubrique *Passerelles Windows* dans le *Guide d'installation* de TADDM.

Bitvise WinSSHD est disponible sur le site http://www.bitvise.com/.

Pourquoi et quand exécuter cette tâche

La procédure ci-dessous explique comment configurer Bitvise WinSSHD 5.22. Les étapes spécifiques peuvent varier selon l'édition de Bitvise WinSSHD que vous possédez.

Procédure

1. Pour limiter l'accès hôte SSH au serveur TADDM, procédez comme suit :
   a. Dans le Panneau de configuration WinSSHD, cliquez sur **Open easy settings**.
   b. Dans l'onglet **Server settings**, pour la zone **Open Windows Firewall**, sélectionnez **As set in Advanced WinSSHD settings**.
   c. Cliquez sur **Save Changes**.
   d. Dans le Panneau de configuration WinSSHD, cliquez sur **Edit advanced settings**. La fenêtre Advanced WinSSDH Settings s'affiche.
   e. Cliquez sur **Settings** > **Session**.
   f. Paramétrez la valeur des éléments suivants sur `0`:
      - Blocage IP - durée de la fenêtre
      - Blocage IP - heure de blocage
   g. Cliquez sur **OK**.
   h. Dans le Panneau de configuration WinSSHD, cliquez sur **Edit advanced settings**. La fenêtre Advanced WinSSDH Settings s'affiche.
   i. Cliquez sur **Settings** > **Access Control**.
   j. Dans le panneau de droite, cliquez sur **IP Rules**.
   k. Cliquez sur **Add**.
   l. Entrez l'adresse IP du serveur TADDM.
   m. Dans la zone **Number of significant bits**, tapez `32`.
   n. Dans la zone **Description**, tapez `TADDM server`.
   o. Assurez-vous que la case **Allow connect** est cochée.
   p. Cliquez sur **OK**.
   q. Supprimez l'entrée `0.0.0.0/0` de la liste.
2. Pour créer et configurer un groupe virtuel et des utilisateurs, procédez comme suit :
   a. Dans le Panneau de configuration WinSSHD, cliquez sur **Edit advanced settings**. La fenêtre Advanced WinSSDH Settings s'affiche.
   b. Cliquez sur **Settings** > **Virtual Groups**.
   c. Pour ajouter un nouveau groupe, cliquez sur **Add**.
   d. Dans les zones **Group** et **Windows Account Name**, entrez un nom.
   e. Cliquez sur **OK**.
   f. Cliquez sur **Settings** > **Virtual Accounts**.
   g. Pour ajouter un nouveau compte, cliquez sur **Add**.
   h. Dans la zone **Virtual account name**, entrez un nom.

i. Définissez un mot de passe à l'aide du lien relatif au mot de passe de compte virtuel.
j. Dans la liste déroulante, sélectionnez le groupe virtuel que vous avez créé à l'étape précédente, puis assurez-vous que la case **Use group default Windows account** est cochée.
k. Cliquez sur **OK**.

3. Dans le Panneau de configuration WinSSHD, cliquez sur **Start WinSSHD**.

Que faire ensuite

Si vous faites la reconnaissance de plusieurs serveurs Windows, vous pouvez obtenir le message suivant :

```
A Working gateway cannot be found
```

Pour plus d'informations sur les opérations de configuration supplémentaires qui peuvent vous aider, voir la rubrique *Problèmes de passerelle* dans le *Guide d'identification et de résolution des problèmes* de TADDM.

Configuration du démon SSH Cygwin

Vous pouvez utiliser le démon SSH Cygwin (sshd) pour fournir un accès SSH aux systèmes Windows.

Pourquoi et quand exécuter cette tâche

Pour une reconnaissance basée sur une passerelle, le démon SSH Cygwin doit être installé sur le système de passerelle. Pour une reconnaissance SSH directe, le démon doit être installé sur chaque système Windows.

Pour plus d'informations sur les versions de du démon Cygwin SSH prises en charge, reportez-vous à la rubrique *Passerelles Windows* dans le *Guide d'installation* de TADDM.

Important : Les conditions suivantes doivent être remplies pour que la reconnaissance à l'aide de SSH Cygwin aboutisse :

- Les ancrages et les passerelles doivent être pris en charge sous Cygwin édition 64 bits sur Windows Server 2012 x64 et Windows Server 2008 x64.
- L'utilisateur de reconnaissance et l'utilisateur qui démarre le service doivent être les mêmes. L'utilisateur de reconnaissance doit appartenir au groupe des administrateurs.

Cygwin est disponible sur le site http://www.cygwin.com/.

Procédure

Pour configurer le démon SSH Cygwin :

1. Démarrez l'interpréteur de commandes cygwin bash.
2. A partir des informations système et de l'utilitaire **`cygwin mkpasswd`**, créez un fichier `/etc/passwd` initial. Vous pouvez également vous servir de l'utilitaire **`mkgroup`** pour créer un groupe `/etc/` initial. Pour plus de détails, voir le manuel *Cygwin User's Guide*.

   Par exemple, la commande suivante définit le fichier de mots de passe, `passwd`, à partir des comptes en local de votre système :

   ```
   mkpasswd -l > /etc/passwd
   ```

3. Exécutez le programme de configuration ssh-host-config.
4. Configurez SSH. Répondez `Oui` à toutes les questions.
5. Démarrez le serveur SSH à l'aide de la commande suivante :

   ```
   net start sshd
   ```

Que faire ensuite

Le service Cygwin (sshd) doit utiliser un compte utilisateur du domaine lors de l'accès au serveur de passerelle. Ce compte utilisateur est requis pour certains détecteurs, par exemple le détecteur de Microsoft Exchange. Procédez comme suit :

1. Configurez le compte utilisateur du domaine en exécutant les commandes suivantes :

   ```
   mkpasswd -u [domain_user] -d [domain] >> /etc/passwd
   mkgroup -d [domain] >> /etc/group
   ```

2. Démarrez le programme services.msc. Vérifiez les propriétés de connexion du service Cygwin (sshd) créé. Vérifiez que ce service est configuré pour être exécuté par un compte utilisateur de domaine d'administration.
3. La configuration Cygwin (sshd) et les fichiers journaux doivent être détenus par le même compte utilisateur de domaine que celui utilisé par le service Cygwin (sshd) pour accéder à la passerelle. Exécutez les commandes suivantes :

   ```
   $ chown [utilisateur_domaine] /var/log/sshd.log
   $ chown -R [domain_user] /var/empty
   $ chown [utilisateur_domaine] /etc/ssh*
   ```

4. Le compte utilisateur de domaine doit disposer des droits suivants sur le serveur de passerelle :
   - Réglage des quotas de mémoire des processus
   - Création d'un objet jeton
   - Connexion en tant que service
   - Remplacement d'un jeton de niveau processus

Si vous faites la reconnaissance de plusieurs serveurs Windows, vous pouvez obtenir le message suivant :

```
A Working gateway cannot be found
```

Pour plus d'informations sur les opérations de configuration supplémentaires qui peuvent vous aider, voir la rubrique *Problèmes de passerelle* dans le *Guide d'identification et de résolution des problèmes* de TADDM.

Configuration de Remotely Anywhere

Vous pouvez utiliser Remotely Anywhere pour fournir un accès SSH aux systèmes Windows.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur les versions de Remotely Anywhere prises en charge, reportez-vous à la rubrique *Passerelles Windows* dans le *Guide d'installation* de TADDM.

Pour une reconnaissance basée sur une passerelle, Remotely Anywhere doit être installé sur le système de passerelle.

Pour une reconnaissance SSH directe, Remotely Anywhere doit être installé sur chaque système Windows.

Vous pouvez utiliser les valeurs de configuration par défaut dans Remotely Anywhere. Pour plus d'informations, voir http://remotelyanywhere.com/.

Configuration du serveur Tectia SSH

Vous pouvez utiliser le serveur Tectia SSH pour fournir un accès SSH aux systèmes Windows.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur les versions du serveur Tectia SSH prises en charge, voir la rubrique *Passerelle Windows* dans le *Guide d'installation* de TADDM.

Pour une reconnaissance basée sur une passerelle, vous devez installer le serveur Tectia SSH sur un système de passerelle.

Pour une reconnaissance SSH directe, vous devez installer le serveur Tectia SSH sur chaque système Windows.

Vous pouvez utiliser les valeurs de configuration par défaut du serveur Tectia SSH. Pour plus d'informations, voir http://www.ssh.com.

Dépendance de Windows Management Instrumentation (WMI)

TADDM s'appuie sur Windows Management Instrumentation (WMI) pour reconnaître les systèmes informatiques Windows. TADDM peut être configuré pour redémarrer le service WMI en cas de problème avec WMI. Si le service WMI est redémarré, tous les services qui en dépendent et qui s'exécutaient avant le redémarrage sont également redémarrés.

Les propriétés suivantes du serveur TADDM contrôlent le redémarrage de WMI.

Remarque : La valeur par défaut pour le redémarrage de WMI est `false`. La définition des propriétés suivantes à `true` peuvent offrir une reconnaissance Windows fiable, mais vous devez aussi prendre en compte l'impact négatif potentiel du service WMI temporairement arrêté et redémarré.

- `com.collation.RestartWmiOnAutoDeploy=false`
- `com.collation.RestartWmiOnAutoDeploy.1.2.3.4=false`
- `com.collation.RestartWmiOnFailure=false`
- `com.collation.RestartWmiOnFailure.1.2.3.4=false`

Pour plus d'informations sur les propriétés du serveur TADDM utilisé par le détecteur de système informatique Windows, voir la rubrique *Configuration du fichier collation.properties* dans la section relative aux détecteurs de système informatique Windows de la *Référence des détecteurs* de TADDM.

Session PowerShell

Fix Pack 2

Pour reconnaître des systèmes informatiques Windows, vous pouvez utiliser la session WMI ou la session PowerShell. Comparée à la session WMI, la session PowerShell permet à TADDM d'envoyer moins de demandes d'accès aux systèmes cible, ce qui réduit le nombre d'événements consignés. La session PowerShell peut

être utilisée uniquement avec les détecteurs basés sur un script. Si vous voulez commencer à utiliser la session PowerShell, vous devez l'activer. En effet, elle est désactivée par défaut.

Vous pouvez utiliser les deux sessions en même temps. Si vous exécutez des reconnaissances standard et basées sur un script, vous ne pouvez pas désactiver la session WMI. Sans elle, la reconnaissance standard échoue. Toutefois, vous pouvez définir les priorités vis-à-vis de l'utilisation de la session PowerShell.

Important : Si vous exécutez uniquement des reconnaissances standard, la session PowerShell n'est pas prise en charge.

Vous pouvez contrôler l'utilisation et la définition des priorités de la session PowerShell à l'aide des propriétés suivantes :

- `com.collation.PowerShellAccessEnabled=false`
- `com.collation.WmiAccessEnabled=true`
- `com.collation.PreferPowerShellOverWMI=true`
- `com.collation.PowerShellPorts=5985,5986`
- `com.ibm.cdb.session.ps.useSSL=false`
- `com.ibm.cdb.session.ps.allowDNS=true`
- `com.ibm.cdb.session.ps.fallbackToIP=true`
- `com.collation.PowerShellTimeoutFudge=10000`
- Fix Pack 3 `com.ibm.cdb.session.ps.urlPrefix=wsman`

Pour activer la session PowerShell, définissez la propriété `com.collation.PowerShellAccessEnabled` sur `true`. La session PowerShell est préférée à la session WMI par défaut.

Pour plus d'informations sur ces propriétés, voir la rubrique relative à la *configuration des entrées de fichier `collation.properties`* pour le détecteur de système informatique Windows dans le *Guide de référence des détecteurs* de TADDM.

Remarque : Dans un cas très particulier, lorsque vous avez configuré votre pare-feu pour permettre la communication via la session PowerShell seulement, vous devez ouvrir des ports PowerShell et configurer la propriété du détecteur Ping. Pour plus d'informations, voir la rubrique *Configuration pour la reconnaissance via un pare-feu sans ancrage* dans le *Guide d'utilisation* de TADDM.

Exemples de scénarios

Selon la méthode utilisée pour reconnaître vos systèmes cible Windows, vous pouvez configurer les propriétés précédentes des manières suivantes.

- Vous utilisez uniquement les détecteurs prenant en charge la reconnaissance basée sur un script. Dans ce cas, vous pouvez activer la session PowerShell en définissant la propriété `com.collation.PowerShellAccessEnabled` sur `true` et désactiver la session WMI en définissant la propriété `com.collation.WmiAccessEnabled` sur `false`. Toutefois, lorsque PowerShell est indisponible, la session et la reconnaissance échouent.
- Vous utilisez des détecteurs prenant en charge la reconnaissance basée sur un script et la reconnaissance standard. Dans ce cas, ne désactivez pas la session WMI ; cela entraînerait l'échec de la reconnaissance standard. Activez la session PowerShell en définissant la propriété `com.collation.PowerShellAccessEnabled` sur `true`. Pour établir la session PowerShell dès que possible, ne modifiez pas la

valeur par défaut de la propriété `com.collation.PreferPowerShellOverWMI`. Dans ce cas, TADDM crée une session hybride capable d'utiliser les fonctions PowerShell et WMI. La session WMI est utilisée uniquement lorsque la session PowerShell n'est pas en mesure d'exécuter les tâches demandées par les détecteurs standard.

Configuration pour la reconnaissance des marques de réservation

Fix Pack 3

Vous pouvez configurer TADDM afin qu'il crée des marques de réservation pour les dépendances non reconnues dans votre infrastructure.

Une marque de réservation est un objet qui fait partie de votre infrastructure mais qui n'est pas représenté dans TADDM avec les paramètres par défaut. Les raisons pour lesquelles l'objet n'est pas représenté peuvent être qu'un côté de la connexion n'est pas reconnu, qu'aucun détecteur ne prend en charge son type ou qu'aucun modèle de serveur personnalisé n'est créé pour lui.

Les marques de réservation appartiennent à la classe SSoftwareServer. Elles possèdent le jeu d'attributs `hierarchyDomain` et `hierarchyType`. Le tableau suivant indique les valeurs des attributs :

Tableau 35. Valeurs des attributs `hierarchyDomain` et `hierarchyType`.

Côté de la connexion	Valeur de l'attribut `hierachyDomain`	Valeur de l'attribut `hierarchyType`
Local	`app.placeholder.client.local`	Nom de la commande qui lance la connexion, par exemple, `Java`
Distant	`app.placeholder.server.remote`	`Inconnu`

A l'aide de ces valeurs, vous pouvez filtrer les relations indésirables dans la configuration de traversée des applications métier. Pour plus d'informations, voir la rubrique *Configuration de traversée* dans le *Guide d'utilisation* de TADDM.

Lorsqu'une marque de réservation est créée, puis que le serveur d'applications équivalent est créé par un détecteur ou un modèle de serveur personnalisé, PlaceholderCleanupAgent fusionne la marque de réservation avec le serveur d'applications reconnu.

Remarque : Vous pouvez créer des marques de réservation dans TADDM 7.3.0.2, mais la fonction est limitée. C'est pourquoi il est conseillé d'utiliser des marques de réservation dans TADDM version 7.3.0.3 et ultérieures. La migration des marques de réservation créées dans FP2 et FP3 n'est pas prise en charge.

Activation de la création des marques de réservation

Pour activer la création des marques de réservation, ajoutez la propriété suivante dans le fichier `collation.properties` :

```
com.ibm.cdb.topomgr.topobuilder.agents.ConnectionDependencyAgent2
dependencyPlaceholders=true
```

La valeur par défaut est `false`.

Lorsque vous définissez la première fois cette propriété sur `true`, vous devez redémarrer TADDM afin d'activer les attributs étendus des classes LogicalConnection et SoftwareServer. Ces attributs étendus sont nécessaires au bon fonctionnement de cette fonction.

Si la propriété ci-dessus est définie sur `true`, il n'est pas nécessaire de définir explicitement les propriétés ci-dessous du fichier `collation.properties`, car leurs valeurs codées par défaut seront utilisées.

```
com.ibm.taddm.dependencyPlaceholders.create.localClient.to.remoteServer
=true
```

La valeur par défaut est `true`.

```
com.ibm.taddm.dependencyPlaceholders.create.remoteClient.to.localServer
=false
```

La valeur par défaut est `false`.

Remarque : Vous pouvez modifier le comportement des marques de réservation en définissant ces propriétés dans le fichier `collation.properties`.

Important : Lorsque vous activez la création des marques de réservation, vos applications métier peuvent croître de manière significative et la construction peut prendre plus de temps. Pour éviter cette situation, vous pouvez filtrer les relations indésirables dans la configuration de traversée des applications métier.

Affichage des marques de réservation

Vous pouvez afficher les marques de réservation dans la sous-fenêtre Récapitulatif de l'inventaire après avoir défini le filtre sur `Marques de réservation`. Les marques de réservation des dépendances non reconnues se trouvent dans l'onglet **Serveurs logiciels**.

Création de modèles de serveur personnalisé

Les marques de réservation permettent de créer des modèles de serveur personnalisé des manières suivantes :

- En utilisant les informations concernant les marques de réservation qui sont générées par l'outil `bizappscli`. Pour plus d'informations, voir *Actions pour l'analyse du contenu des applications métier* dans le *Guide d'utilisation* de TADDM.
- En utilisant les informations de ligne de commande qui sont affichées sous l'onglet **Exécution** dans la sous-fenêtre Détails pour les marques de réservation de type `app.placeholder.*.local`.

Pour plus d'informations sur les modèles de serveur personnalisé, voir dans la rubrique *Création et gestion de modèles de serveur personnalisé* du *Guide d'utilisation* de TADDM.

Création de serveurs d'applications de niveau 3 sans données d'identification

Fix Pack 2

Si vous souhaitez reconnaître les informations de base de niveau 3 concernant vos éléments d'infrastructure, vous n'avez pas besoin de fournir de données d'identification dans la liste d'accès. Vous pouvez créer des serveurs d'applications à l'aide des modèles internes de détecteurs. Ces modèles peuvent être traités par

CustomAppServerTopoAgent ou pendant une exécution de la reconnaissance par le détecteur de modèle de serveur personnalisé.

Pourquoi et quand exécuter cette tâche

Si vous créez des serveurs d'applications sans données d'identification, vous pouvez reconnaître uniquement les informations de base concernant votre infrastructure, par exemple les types de logiciels installés. Sélectionnez ce mode si vous ne voulez pas fournir de données d'identification pour la reconnaissance de niveau 3 mais que vous souhaitez reconnaître les informations de base concernant votre infrastructure.

Il existe deux méthodes pour créer des serveurs d'applications de niveau 3. Vous pouvez exécuter le détecteur de modèle de serveur personnalisé ou activer CustomAppServerTopoAgent.

Procédure

- Exécution d'une reconnaissance avec le détecteur de modèle de serveur personnalisé
  Procédez comme suit :
  1. Dans le fichier `collation.properties`, définissez la propriété `com.collation.internaltemplatesenabled` sur `true`. Cette propriété active les modèles internes des détecteurs de niveau 3. La valeur par défaut est `false`.
  2. Exécutez la reconnaissance à l'aide d'un profil ne contenant pas le détecteur qui reconnaîtrait normalement les informations souhaitées avec un détecteur de modèle de serveur personnalisé. Par exemple, pour reconnaître les données de base concernant le serveur DB2, sélectionnez la reconnaissance de profil de niveau 2 ou votre profil personnalisé ne contenant pas le détecteur IBM DB2. Si le détecteur IBM DB2 est mentionné dans le profil, il est exécuté à la place du détecteur de modèle de serveur personnalisé.
- Exécution de CustomAppServerTopoAgent
  CustomAppServerTopoAgent utilise les processus d'exécution précédemment reconnus par le détecteur de serveur générique. Vous pouvez exécuter l'agent manuellement ou le configurer pour qu'il s'exécute automatiquement. Procédez comme suit :
  1. Pour les modes automatique et manuel de l'agent, dans le fichier `collation.properties`, définissez la propriété `com.collation.internaltemplatesenabled` sur `true`. Cette propriété active les modèles internes des détecteurs de niveau 3. La valeur par défaut est `false`.
  2. Pour démarrer manuellement CustomAppServerTopoAgent, exécutez la commande suivante :
     ```
     COLLATION_HOME/support/bin/runtopobuild.sh -a CustomAppServerTopoAgent
     ```
  3. Pour configurer les exécutions automatiques de l'agent, définissez la propriété `com.ibm.cdb.topobuilder.groupinterval.discovery=` dans le fichier `collation.properties`.
     Cette propriété spécifie la fréquence d'exécution de l'agent. Par défaut, aucune valeur n'est fournie, ce qui signifie que l'agent est désactivé. Pour l'activer, indiquez la valeur en heures, par exemple `com.ibm.cdb.topobuilder.groupinterval.discovery=4`.
- Facultatif : Sélection des modèles à exclure du traitement
  Si vous voulez activer seulement certains des modèles internes de détecteurs de niveau 3, utilisez la propriété suivante :
  ```
  com.collation.discovery.ignoreTemplateList
  ```

Cette propriété indique la liste des modèles internes à ne pas traiter. La valeur de cette propriété est une liste de noms de modèle séparés par un point-virgule, par exemple `com.collation.discovery.ignoreTemplateList=DB2Unix;MSSQL`. Pour trouver le nom d'un modèle interne, consultez le portail de gestion de données dans la zone **Nom d'objet**, qui se trouve sous l'onglet **Général** dans la sous-fenêtre **Détails** de la zone **Autres serveurs de base de données**.

Configuration du balisage d'emplacement

Le balisage d'emplacement indique l'endroit où chaque élément de configuration (EC) a été créé. Il permet le filtrage en fonction de l'emplacement des éléments de configuration dans les rapports BIRT et les requêtes API.

Si vous activez le balisage d'emplacement, chaque objet stocké dans la base de données de reconnaissance contient l'attribut **`locationTag`** (chaîne). Les objets tels que les relations, des objets d'agrégation et les objets d'héritage créés par les agents de topologie contiennent des données de balise d'emplacement dans certaines conditions :

- Une relation un à un (telle que Dependency ou NetworkConnection) contient une balise d'emplacement si l'emplacement est le même pour les deux objets connectés.
- Un objet d'agrégation (tel qu'un cluster) contient une balise d'emplacement si l'emplacement est le même pour tous les objets agrégés.

  Remarque : Dans le cas de collections personnalisées, l'attribut **`locationTag`** est défini uniquement si la *valeur* de la balise d'emplacement de tous les éléments de configuration clé de la collection personnalisée est la même. Si une collection personnalisée est étendue avec un élément de configuration clé dont la balise d'emplacement est différente, l'attribut **`locationTag`** relatif à une telle collection personnalisée est supprimé.
- Un objet simple contient la balise d'emplacement de l'objet sur lequel il est basé.

Dans tous les autres cas, les objets créés par les agents de topologie ne contiennent pas de valeur de balise d'emplacement.

Pour activer le balisage d'emplacement, définissez la propriété suivante dans le fichier `collation.properties` :

```
com.ibm.cdb.locationTaggingEnabled=true
```

Les valeurs de balise d'emplacement peuvent être soit statiques (définies pour un serveur ou un ancrage précis), soit dynamiques (définies pour une reconnaissance ou une importation de manuel IdML précise). Une valeur de balise d'emplacement est limitée à 192 caractères. Si la balise d'emplacement précise dépasse les 192 caractères, elle est coupée à la longueur obligatoire.

Limitations

Lorsque vous exécutez une reconnaissance de niveau 1, les éléments de configuration déjà présents dans la base de données ne sont pas mis à jour. Ainsi, les balises d'emplacement ne sont affectées qu'aux nouveaux objets détectés.

Balisage d'emplacement statique

Le balisage d'emplacement statique affecte l'attribut **`locationTag`** à tous les objets reconnus ou chargés à l'aide de l'importation de manuel IdML en fonction de la configuration statique de TADDM ou du serveur d'ancrage.

Serveur TADDM

Pour configurer la valeur de balise d'emplacement des EC créés sur un serveur TADDM, définissez la propriété suivante dans le fichier `collation.properties` :

```
com.ibm.cdb.locationTag=location
```

où **`location`** correspond à la valeur de balise d'emplacement à utiliser.

Ancrage

Pour configurer la valeur de balise d'emplacement des EC créés sur un ancrage, configurez l'attribut **anchor_location_n** dans le fichier `$COLLATION_HOME/etc/anchor.properties`. Les exemples d'entrées suivants du fichier `anchor.properties` indiquent la façon dont les informations d'emplacement des ancrages sont définies :

```
anchor_host_1=192.168.1.13
anchor_scope_1=FIRST_SCOPE
anchor_zone_1=FIRST_ZONE
anchor_location_1=FIRST_LOCATION
anchor_host_2=192.168.2.22
anchor_scope_2=SECOND_SCOPE
anchor_location_2=SECOND_LOCATION
Port=8497
```

Si une balise d'emplacement n'est pas définie pour un ancrage, l'emplacement de chacun des EC créés sur l'ancrage est paramétré sur l'emplacement défini pour le serveur TADDM auquel les EC sont connectés.

Si la valeur de balise d'emplacement n'est pas définie pour l'ancrage ou le serveur TADDM, aucune information d'emplacement n'est définie pour cet EC.

Balisage d'emplacement dynamique

Le balisage d'emplacement dynamique définit l'attribut **`locationTag`** à l'aide d'une valeur spécifiée pour une reconnaissance dynamique ou une importation de manuels IdML.

Reconnaissance

Pour définir une valeur de balise d'emplacement au cours d'une reconnaissance, lancez la reconnaissance à partir de la ligne de commande et indiquez la balise d'emplacement à l'aide de l'option facultative **`-l`** or **`-myLocation`**, comme dans l'exemple suivant :

```
api.sh -u administrator -p collation discover start -n discovery1 -p myProfile -l myLocation myScope
```

où **`locationTag`** correspond à la valeur de balise d'emplacement à utiliser. La valeur que vous définissez remplace la valeur de balise d'emplacement statique des objets créés au cours de cette reconnaissance précise.

Remarque : Si le balisage d'emplacement n'est pas activé dans le fichier `collation.properties`, le fait de définir une balise d'emplacement lors de la demande de reconnaissance génère une exception de reconnaissance.

Importation du manuel IdML

Pour définir une valeur de balise d'emplacement au cours d'une importation d'un manuel IdML, définissez la balise d'emplacement à l'aide de l'option facultative -l, comme dans l'exemple suivant :

```
loadidml.sh -f idml_book.xml -l locationTag
```

où **locationTag** correspond à la valeur de balise d'emplacement à utiliser. Si vous souhaitez importer plusieurs manuels IdML avec différentes balises d'emplacement, chaque manuel doit être chargé séparément.

Liste d'accès

Vous pouvez créer des entrées de liste d'accès assorties d'une balise d'emplacement.

L'attribut de balise d'emplacement est obligatoire, mais peut être modifié ultérieurement. Les données d'identification sont filtrées par emplacement, c'est pourquoi seules les entrées d'accès des emplacements spécifiques sont utilisées. Cela limite le risque de piratage du mot de passe des autres clients ou emplacements. Si vous exécutez la reconnaissance sans balise d'emplacement, aucune des données d'identification balisées n'est utilisée.

Si vous ajoutez une entrée d'accès dont la balise d'emplacement a pour valeur le signe astérisque (*), elle est utilisée comme dernière entrée d'accès tentée au cours d'une reconnaissance lors de l'établissement d'une session avec le noeud final.

L'astérisque (*) correspond à la valeur par défaut. Vous pouvez modifier cette valeur en définissant le paramètre suivant :

```
com.ibm.cdb.locationTag.global=GLOBAL
```

Dans ce cas, l'entrée d'accès ayant la balise `GLOBAL` est la dernière à être tentée pendant l'exécution d'une reconnaissance. La balise d'emplacement précédente est uniquement utilisée pour la liste d'accès et n'a pas d'influence sur les balises d'emplacement qui sont affectées aux éléments de configuration qui sont découverts au cours d'une reconnaissance.

Rapports BIRT

Les rapports Business Intelligence and Reporting Tools (BIRT) peuvent être filtrés pour générer les données liées à l'emplacement client spécifique.

Si le balisage d'emplacement est activé, la zone de texte se trouve sur la sous-fenêtre des rapports BIRT, sous la liste de rapports. Vous pouvez exécuter un rapport BIRT en fonction d'une balise d'emplacement de manière à afficher les données figurant uniquement dans cet emplacement.

Aucun des rapports prêts à l'emploi ne peut gérer les balises d'emplacement. Si vous devez utiliser les rapports BIRT, ils doivent être mis à jour manuellement afin de prendre en charge le filtrage par balise d'emplacement.

Maintenance et optimisation

Pour augmenter les performances de TADDM, vous pouvez éventuellement suivre d'autres tâches de configuration et de maintenance continue.

Optimisation des paramètres de chargement en bloc

Vous pouvez personnaliser le comportement du chargeur en bloc en spécifiant des paramètres au moment de l'exécution ou en configurant le fichier `bulkload.properties`.

Il existe trois phases distinctes de chargement de données à l'aide du programme de chargement en bloc :

1. Analyser les objets et les relations pour déterminer les graphiques dans les données.

   En général, 1 - 5% du temps d'exécution.
2. Construire des objets de modèle et générer des graphiques.

   En général, 2 - 5% du temps d'exécution.
3. Transférer les données au serveur d'API (interface de programme d'application).

   En général, 90 - 99% du temps d'exécution.

Il existe deux options pour charger des données :

- Les données peuvent être chargées avec un enregistrement à la fois. Il s'agit du mode par défaut. Vous devez charger un seul enregistrement à la fois pour les fichiers suivants :
  - Fichiers comportant des erreurs.
  - Fichiers comportant des attributs étendus.
- Les données peuvent être chargées en bloc. Cela est désigné par écriture graphique car la totalité d'un graphique est chargée, et non un seul enregistrement.

  Le chargement en bloc à l'aide de l'option d'écriture graphique est plus rapide que le chargement d'un enregistrement à la fois. (Pour plus de détails, reportez-vous aux mesures du chargement en bloc). L'exemple suivant présente l'option d'écriture graphique, où -g=buffer et des blocs de données sont transmis au serveur d'API :

  ```
  ./loadidml.sh –g –f /home/configia/testfiles/sample.xml
  ```

  Les paramètres suivants de `bulkload.properties` peuvent être utilisés pour améliorer les performances lors du chargement en bloc des données :

  ```
  com.ibm.cdb.bulk.cachesize=2000
  ```

  Le paramètre `cachesize` détermine le nombre d'objets traités dans une même opération d'écriture lors du chargement en bloc à l'aide de l'option d'écriture graphique. L'augmentation de la valeur de taille du cache améliore les performances au risque de réduire la mémoire, que ce soit au niveau du client ou du serveur. Modifiez-le uniquement lorsque des informations spécifiques sont disponibles pour indiquer que le traitement d'un fichier avec un cache plus volumineux permet d'améliorer les performances. La valeur par défaut et la valeur maximale de la taille du cache sont respectivement de 2 000 et de 40 000.

  ```
  com.ibm.cdb.bulk.allocpoolsize=1024
  ```

  Cette valeur spécifie la quantité maximale de mémoire qui peut être allouée au programme de chargement en bloc. Il s'agit d'une valeur Xmx qui est transmise à la classe Java principale du programme de chargement en bloc. Spécifiez la valeur en mégaoctets.

  Vérifiez qu'une machine virtuelle Java ne possède pas une mémoire insuffisante. Pour ce faire, collectez les clichés de l'unité d'exécution des processus TADDM et étudiez-les. Si nécessaire, augmentez la taille de la mémoire.

  Conseil : Des tests effectués dans le cadre du livre ITNMIP indiquent que les performances sont optimales lorsque vous définissez les propriétés et paramètres du processus de chargement en bloc sur les valeurs suivantes :

```
com.ibm.cdb.bulk.cachesize=4000
com.ibm.cdb.bulk.allocpoolsize=4096
value-Xms768M|-Xmx1512M|-DTaddm.xmx64=6g|
```

Il est également important que vous exécutiez la commande **RUNSTATS** régulièrement au cours du processus de chargement en bloc.

Maintenance de la base de données

Pour garantir des performances de haut niveau sur votre système, vous devez planifier et exécuter régulièrement des opérations de maintenance et d'optimisation de la base de données TADDM.

Configurations de la base de données par défaut

Les configurations de base de données par défaut fournies avec TADDM sont suffisantes pour appliquer le concept, la technologie et de petites implémentations pilotes de TADDM.

Instructions d'optimisation pour les bases de données DB2 et Oracle

Les instructions d'optimisation suivantes s'appliquent aux bases de données DB2 et Oracle :

1. Ne tentez pas de limiter le nombre de disques physiques disponibles pour votre base de données en fonction de la capacité de stockage uniquement.
2. Les composants suivants doivent idéalement être situés sur des disques/tableaux distincts :
   - Données d'application (comme des tables et des indexe)
   - Journaux de base de données
   - Espace temporaire de base de données : utilisé pour les opérations de tri et de fusion
3. Utilisez les disques disponibles les plus rapides pour vos fichiers journaux.
4. Activez les E-S asynchrones au niveau du système d'exploitation.

Pour plus d'informations sur l'optimisation des bases de données DB2 et Oracle, consultez le manuel *Database Performance Tuning on AIX* à l'adresse http://www.redbooks.ibm.com/redbooks/pdfs/sg245511.pdf.

Pour plus d'informations sur l'optimisation de la base de données DB2, voir également *Relational Database Design and Performance Tuning for DB2 Database Servers* à l'adresse http://www-01.ibm.com/support/docview.wss?uid=tss1wp100764 et les manuels *DB2 UDB Version 8 Product Manuals* à l'adresse http://www.ibm.com/support/docview.wss?rs=71&uid=swg27009554.

Suppression d'anciens enregistrements de base de données

Le nombre d'enregistrements de données des tables évolue dans le temps et, selon l'espace disponible, vous pouvez être périodiquement amené à supprimer manuellement des données des tables afin d'en limiter la taille. Une fois que vous avez effacé CHANGE_HISTORY_TABLE, vous pouvez supprimer les entrées correspondantes de CHANGE_CAUSE_TABLE. Vous pouvez également améliorer les performances et la convivialité de l'outil d'intégrité des données en supprimant les anciens enregistrements de la table ALIASES_JN.

Suppression des enregistrements de CHANGE_HISTORY_TABLE et CHANGE_CAUSE_TABLE :

Vous pouvez supprimer les anciens enregistrements pour améliorer les performances et conserver une taille plus petite pour les tables. Une fois que vous avez supprimé les enregistrements de CHANGE_HISTORY_TABLE, vous pouvez supprimer en toute sécurité les entrées correspondantes de CHANGE_CAUSE_TABLE.

Pour libérer de la mémoire dans les bases de données TADDM, utilisez des requêtes SQL afin de supprimer manuellement les anciennes données de la table CHANGE_HISTORY_TABLE. La commande suivante est un exemple de requête SQL, où l'entier 1225515600000 correspond à la date (1er novembre 2008) exprimée dans le même format que celui renvoyé par la méthode Java System.currentTimeMillis() ou un nombre égal à la différence, mesurée en millisecondes, entre l'heure actuelle et minuit, le 1er janvier 1970 (temps universel coordonné) :

```
DELETE FROM CHANGE_HISTORY_TABLE
HERE PERSIST_TIME < 1225515600000 (il s'agit de l'horodatage Java)
```

Pour convertir une date en horodatage Java, utilisez le code suivant :

```
import java.util.*;
import java.text.*;
import java.sql.Timestamp;

public class DateToString {

  public static void main(String args[]) {
  try {
     String str = args[0];
     SimpleDateFormat formatter = new SimpleDateFormat("dd/MM/yyyy");
     Date date = formatter.parse(str);

    long msec = date.getTime();

    System.out.println("Date is " +date);
    System.out.println("MillSeconds is " +msec);

    } catch (ParseException e)
    {System.out.println("Exception :"+e);    }

  }
}
```

Exécutez le code comme suit :

```
java DateToString 1/11/2008
Date is Sat Nov 01 00:00:00 EST 2008
MillSeconds is 1225515600000
```

Utilisez l'horodatage Java obtenu dans la requête SQL.

Si la table CHANGE_HISTORY_TABLE contient un nombre exceptionnel d'enregistrements, des suppressions incrémentielles (suppression d'un sous-ensemble d'enregistrements à la fois) peuvent être nécessaires pour éviter que les journaux de transaction de la base de données se remplissent.

Une fois que vous avez effacé CHANGE_HISTORY_TABLE, vous pouvez supprimer en toute sécurité les entrées correspondantes de CHANGE_CAUSE_TABLE. La table CHANGE_CAUSE_TABLE est une table de

liens utilisées pour la propagation des changements. Par exemple, si vous ajoutez un composant logiciel au système d'exploitation, la table relie ce changement au système informatique sur lequel le système d'exploitation fonctionne. Vous pouvez supprimer les enregistrements dans la table CHANGE_CAUSE_TABLE à l'aide de la commande suivante :

```
delete from change_cause_table where cause_id not in (select id from change_history_table)
```

Intervalles de suppression de données

Pour limiter la croissance de la base de données au fil du temps, vous pouvez gérer la taille des données de l'historique des modifications stockées par TADDM. Lorsque vous souhaitez déterminer à quelle fréquence vous souhaitez supprimer des données de la table de l'historique des modifications, tenez compte de l'utilisation que vous faites de cet historique et demandez-vous si ces informations sont utilisées par d'autres applications.

Si les informations de l'historique des modifications sont utilisées par une autre application, vérifiez que la fréquence de synchronisation est supérieure à la fréquence de suppression de ces données dans la table CHANGE_HISTORY_TABLE.

Les exemples suivants illustrent quelques scénarios classiques :

- Si vous utilisez les données d'historique des modifications dans le cadre de la détermination des problèmes et que vous souhaitiez rechercher les problèmes survenus il y a cinq semaines, vous devez conserver les données de la table CHANGE_HISTORY_TABLE pendant au moins cinq semaines.
- Si vous synchronisez TBSM (Tivoli Business Service Manager) une fois par semaine, vous devez conserver les données d'historique des modifications pendant plus d'une semaine dans la table d'historique des modifications TADDM.

Il est important de noter que lors de déploiements de serveur de synchronisation, une grande quantité de données d'historique des modifications augmente la durée nécessaire à une synchronisation complète.

Maintenance des données dans un déploiement de serveur de synchronisation

Dans un déploiement de serveur de domaine, vous pouvez prendre vos décisions en matière de maintenance des données en vous fondant uniquement sur les données nécessaires au domaine. Dans un déploiement de serveur de synchronisation, vous devez coordonner la suppression des données d'historique des modifications entre chaque base de données du serveur de domaine et la base de données du serveur de synchronisation et vous devez supprimer les données de toutes les bases de données.

Dans un déploiement de serveur de synchronisation, utilisez les instructions suivantes pour la maintenance des données :

- Conservez les données d'historique des modifications au niveau du domaine pendant une période plus longue que la période qui s'écoule entre chaque synchronisation planifiée des bases de données du serveur de domaine avec la base de données du serveur de synchronisation. Si, par exemple, la synchronisation est planifiée pour avoir lieu une fois par semaine, conservez les données d'historique des modifications pendant au moins deux semaines dans chaque base de données du serveur de domaine.

- Commencez par supprimer les données d'une base de données du serveur de domaine. Supprimez ensuite les données de la base de données du serveur de synchronisation.
- La meilleure pratique consiste à conserver le même nombre de semaines de données d'historique des modifications dans toutes les bases de données TADDM. Toutefois, la durée de conservation des données d'historique dans la base de données du serveur de synchronisation peut différer de la durée de conservation de ces données dans les bases de données du serveur de domaine.
- Après avoir identifié une fréquence de suppression des données correspondant aux besoins spécifiques de votre environnement, la meilleure pratique consiste à supprimer les données juste après une synchronisation entre les bases de données de serveur de domaine et la base de données du serveur de synchronisation.

Suppression des enregistrements de la table ALIASES_JN :

Lorsque d'anciens enregistrements sont supprimés de la table ALIASES_JN, les performances et la convivialité de l'outil d'intégrité des données sont améliorées et de l'espace supplémentaire est libéré dans la base de données.

Pourquoi et quand exécuter cette tâche

La table ALIASES_JN contient l'historique des changements apportés à la table ALIASES. L'outil d'intégrité des données a besoin des données collectées pour rechercher les éventuels excès de fusion des éléments de configuration dans la base de données. Au fil du temps, le nombre d'enregistrements de données contenus dans la table ALIASES_JN passe à une taille significative. La taille de cette table affecte à la fois les performances et la convivialité de l'outil d'intégrité des données et accroît le besoin en espace de stockage de la base de données TADDM.

L'agent de topologie `AliasesJnTableCleanup` effectue le nettoyage de la table ALIASES_JN.

Par défaut, il supprime toutes les lignes datant de plus de 30 jours. Vous pouvez changer l'âge auquel les enregistrements sont supprimés en configurant la propriété suivante dans le fichier `collation.properties` :

```
com.ibm.cdb.topomgr.topobuilder.agents.AliasesJnTableCleanupAgent.removeOlderThanDays=30
```

Si vous définissez la propriété sur la valeur -1, l'agent est désactivé. Si vous définissez l'âge à une valeur trop faible, l'outil de vérification des données avec l'option de fusion peut ne pas donner des résultats complets.

Par défaut, l'agent s'exécute pendant plus de 1 800 secondes (30 minutes). Si cette durée ne suffit pas à supprimer toutes les lignes d'âge, une nouvelle tentative a lieu à la prochaine exécution de l'agent. Vous pouvez définir la valeur de délai d'attente de l'agent en configurant la propriété suivante dans le fichier `collation.properties` :

```
com.ibm.cdb.topomgr.topobuilder.agents.AliasesJnTableCleanupAgent.timeout=1800
```

Maintenance de la base de données DB2

Vous devez faire régulièrement la maintenance de la base de données DB2 de TADDM pour assurer des performances optimales.

Pourquoi et quand exécuter cette tâche

Les utilitaires DB2 disponibles sont les suivants :

REORG

Après de nombreuses modifications apportées aux données des tables suite à l'insertion, la suppression et la mise à jour des données des colonnes de longueur variable, des données séquentielles peuvent se trouver dans des pages de données physiques non séquentielles. Le gestionnaire de base de données doit donc effectuer d'autres opérations de lecture pour accéder aux données. Réorganisez les tables DB2 pour éliminer la fragmentation et obtenir de l'espace à l'aide de l'utilitaire **REORG**. Utilisez l'utilitaire **REORG** si **RUNSTATS** demande plus de temps que d'ordinaire pour s'exécuter ou que la commande DB2 **REORGCHK** le demande. Arrêtez le serveur TADDM avant d'exécuter l'utilitaire **REORG**, car pendant une réorganisation d'index ou de tables hors ligne (défragmentation des données), les applications peuvent accéder aux données des tables mais pas les mettre à jour. Comme TopologyBuilder s'exécute fréquemment, même sans reconnaissance, ce type de verrouillage peut causer des effets inattendus dans l'application.

RUNSTATS (collecte de statistiques manuelle)

L'optimiseur DB2 utilise des informations et des statistiques du catalogue DB2 pour identifier le meilleur mode d'accès à la base de données, en fonction de la requête fournie. Des informations statistiques sont collectées pour des tables et des index spécifiques dans la base de données locale lorsque vous exécutez l'utilitaire **RUNSTATS**. Lorsqu'un nombre important de lignes est ajouté ou supprimé dans les tables, ou que les données des colonnes pour lesquelles vous collectez des statistiques sont mises à jour, vous devez utiliser la commande **RUNSTATS** pour mettre à jour les statistiques. Pour optimiser les performances, exécutez la tâche **RUNSTATS** chaque semaine, ou chaque jour si la base de données connaît une forte activité. Si les statistiques ne sont pas suffisamment mises à jour, les performances de TADDM peuvent se dégrader fortement. L'utilitaire **RUNSTATS** peut être exécuté même quand le serveur TADDM est en cours d'exécution. TADDM requiert un format spécifique pour **RUNSTATS** (décrit plus loin) et l'option DB2 **AUTO_RUNSTATS** doit être désactivée.

AUTO_RUNSTATS (collecte de statistiques automatique)

Vous pouvez activer la collecte automatique de statistiques, également connue comme **auto-runstats**, pour permettre à DB2 de décider si les statistiques de base de données TADDM doivent être mises à jour. L'utilitaire **RUNSTATS** est exécuté en arrière-plan et les statistiques de base de données sont toujours à jour.

Pour activer la collecte de statistiques automatique, vous devez définir les paramètres `AUTO_MAINT`, `AUTO_TBL_MAINT` et `AUTO_RUNSTATS` sur `ON`. Exécutez la commande suivante :

```
CONNECT TO <alias_bd>
UPDATE DB CONFIG USING AUTO_MAINT ON AUTO_TBL_MAINT ON AUTO_RUNSTATS ON
```

où *alias_bd* est le nom de votre base de données.

Restriction : Vous ne pouvez utiliser cet utilitaire que si l'APAR IT05733 DB2 est installé et que le paramètre `DB2_SELECTIVITY=DSCC` est défini. L'APAR IT05733 DB2 est inclus dans les éditions suivantes et ultérieures de DB2 :

- 9.7 Groupe de correctifs 11

- 10.1 Groupe de correctifs 6
- 10.5 Groupe de correctifs 7

Pour définir le paramètre DB2_SELECTIVITY=DSCC sur DB2 version 10.*x*, exécutez la commande suivante :

```
db2set -immediate DB2_SELECTIVITY=DSCC
```

Remarque : DB2 9.7 ne prend pas en charge le paramètre `-immediate`. Pour définir le paramètre DB2_SELECTIVITY=DSCC dans cette version, exécutez la commande **db2set DB2_SELECTIVITY=DSCC** et redémarrez DB2.

Remarque : Si l'utilisateur TADDM met à niveau la version DB2 dans l'installation TADDM, la version compatible du pilote doit également être mise à jour. Vous pouvez demander à votre administrateur de base de données le fichier `db2jcc.jar` du serveur TADDM DB2 ou vous pouvez télécharger le fichier approprié pour votre version DB2 ici :http://www-01.ibm.com/support/docview.wss?uid=swg21363866 Une fois que vous l'avez, arrêtez TADDM, copiez-le dans `dist/lib/jdbc/`, confirmez que les droits sont corrects afin que l'utilisateur TADDM puisse lire le fichier, puis démarrez TADDM. Répétez cette étape sur tous les serveurs TADDM de votre environnement.

DB2 HEALTH MONITOR

Il est recommandé d'exécuter le moniteur d'état DB2 sur la base de données TADDM de manière à surveiller préventivement si des conditions ont changé et nécessitent une commande **RUNSTATS** ou **REORG** ou toute autre optimisation. Le moniteur d'état peut alerter un administrateur de base de données sur d'éventuels problèmes de santé du système. Le moniteur d'état détecte préventivement les incidents pouvant induire des pannes matérielles ou des problèmes liés aux fonctionnalités ou aux performances du système. Grâce à cette surveillance préventive de l'état de santé, vous pouvez résoudre un problème avant qu'il n'affecte les performances du système.

DB2 PERFORMANCE ANALYSIS SUITE

En cas de suspicion d'un incident dans DB2, l'outil Performance Analyst peut analyser rapidement un instantané DB2 réalisé pendant la période concernée et proposer des actions. Vous pouvez télécharger cet outil à l'emplacement https://www.ibm.com/developerworks/community/groups/community/perfanalyst.

Pour réaliser un instantané DB2 pour TADDM, procédez comme suit :

1. Connectez-vous à la base de données TADDM depuis le serveur DB2 et exécutez la commande suivante :

   ```
   db2 -tf updmon.sql
   ```

   où le fichier `updmon.sql` contient les entrées suivantes :

   ```
   UPDATE MONITOR SWITCHES USING BUFFERPOOL ON ;
   UPDATE MONITOR SWITCHES USING LOCK       ON ;
   UPDATE MONITOR SWITCHES USING SORT       ON ;
   UPDATE MONITOR SWITCHES USING STATEMENT  ON ;
   UPDATE MONITOR SWITCHES USING TABLE      ON ;
   UPDATE MONITOR SWITCHES USING UOW        ON ;
   UPDATE MONITOR SWITCHES USING TIMESTAMP  ON ;
   RESET MONITOR ALL
   ```

2. Une fois l'étape 1 terminée, exécutez la commande «DB2 get monitor switches» pour voir les valeurs définies pour ces paramètres. Ils doivent tous avoir l'état `ON`.

3. Exécutez le processus ayant des problèmes de performances.
4. En respectant des intervalles appropriés, exécutez la commande suivante à partir de DB2 pendant que le processus lent s'exécute :

   ```
   db2 get snapshot for all on <dbname> > <dbname>-dbsnap.out
   ```

   Exécutez cette commande dans la fenêtre que vous avez utilisée pour la commande exécutée à l'étape 1. Cette commande ne peut pas être exécutée avec un script.
5. Exécutez les instantanés à l'aide d'un fichier de sortie horodaté différent à chaque fois. Exécutez-les avec des intervalles permettant d'obtenir trois ou quatre instantanés pendant le processus sans dépasser un délai d'une heure entre chaque exécution.

Une fois l'instantané collecté, analysez-le avec Performance Analyst en commençant par le dernier instantané. Par exemple, si l'onglet des instructions montre un temps d'exécution moyen et une consommation d'UC élevés pour une requête exécutée plusieurs fois, cela indique un problème d'optimisation que vous pouvez résoudre à l'aide de l'utilitaire **RUNSTATS**. Un pourcentage de dépassement de capacité élevé indiqué dans l'onglet des tables peut nécessiter d'utiliser **REORG**. Vérifiez l'onglet du pool de mémoire tampon pour vous assurer qu'il n'y a pas d'alertes. Un pool de mémoire tampon trop petit peut induire une dégradation des performances.

Avant de commencer

Après toute opération de maintenance importante entraînant une modification du schéma, par exemple, après l'application d'un groupe de correctifs, vous devez générer le fichier `TADDM_table_statistics.sql` sur le serveur de stockage TADDM. Ce fichier est nécessaire pour les tâches de maintenance de base de données **RUNSTATS** que vous devez effectuer périodiquement. TADDM demande un format spécial pour mettre à jour les statistiques de la base de données en raison d'une limitation de DB2 liée au traitement des colonnes comportant des préfixes communs longs, tels que les noms de classe, qui sont largement utilisés dans TADDM. Pour cette raison, n'utilisez pas l'option de DB2 **AUTO_RUNSTATS** mais utilisez plutôt la syntaxe de **RUNSTATS** que vous obtenez en procédant comme indiqué ci-après. Toutefois, si l'APAR IT05733 DB2 est installé et que le paramètre `DB2_SELECTIVITY=DSCC` est défini, vous pouvez utiliser l'option **AUTO_RUNSTATS**.

Remarque : Les instructions suivantes concernent les systèmes d'exploitation Linux et UNIX. Pour une maintenance de la base de données sur le système d'exploitation Windows, utilisez le script `.bat` correspondant au lieu du script `.sh`.

Pour générer le fichier `TADDM_table_stats.sql`, procédez comme suit :

1. Exécutez la commande suivante :

   ```
   cd $COLLATION_HOME/bin
   ```
2. Exécutez la commande suivante, où *tmpdir* est un répertoire où ce fichier peut être créé :

   ```
   ./gen_db_stats.jy > tmpdir/TADDM_table_stats.sql
   ```

   Dans un déploiement de serveur de diffusion en continu, exécutez cette commande sur le serveur de stockage principal.
3. Copiez le fichier sur le serveur de base de données ou communiquez-le à l'administrateur de base de données (dba) pour l'exécuter sur la base

de données TADDM comme indiqué à l'étape 2 de la procédure. Mettez à jour les statistiques de la base de données au moins une fois par semaine, ou plus souvent si les tables sont considérablement modifiées.

Procédure

Pour effectuer la maintenance dans une base de données DB2, procédez comme suit :

1. Pour vous servir de l'utilitaire **REORG**, procédez comme suit :
   a. Sur le serveur de base de données, entrez la requête SQL suivante pour générer les commandes **REORG TABLE** dans un fichier :

      ```
      select  'reorg table '||CAST(RTRIM(creator) AS VARCHAR(40))||'.
       "'||substr(name,1,60)||'" ; ' from sysibm.systables where creator
       = 'utilisateur_bd' and type = 'T' and name not in ('CHANGE_SEQ_ID')
       order by 1;
      ```

      où *utilisateur_bd* est la valeur dans `com.collation.db.user=`.

      Remarque : Assurez-vous que la casse de *dbuser* est celle utilisée dans la table `sysibm.systables` de la base de données, dans la colonne `creator`.
   b. Arrêtez le serveur TADDM.
   c. A une ligne de commande DB2, connectez-vous à la base de données et exécutez les commandes suivantes :

      ```
      db2 –x –tf temp.sql > cmdbreorg.sql
      db2 –tvf cmdbreorg.sql > cmdbreorg.out
      ```
   d. Vérifiez que l'exécution de l'utilitaire **REORG** a abouti en regardant si le fichier `cmdbreorg.out` signale des erreurs.
   e. Démarrez le serveur TADDM.
2. Pour utiliser l'utilitaire **RUNSTATS**, effectuez les étapes ci-après. Automatisez le processus pour qu'il s'exécute au moins une fois par semaine.
   a. Sur le serveur de base de données, exécutez la version TADDM de la commande **RUNSTATS** en reprenant la sortie générée plus tôt :

      ```
      db2 -tvf rép_tmp/TADDM_table_stats.sql  > table_stats.out
      ```
   b. Vérifiez que l'exécution de l'utilitaire **RUNSTATS** a abouti en regardant si le fichier `table_stats.out` signale des erreurs.

Maintenance de la base de données DB2 for z/OS

Ces instructions de maintenance et d'optimisation s'appliquent aux bases de données IBM DB2 for z/OS.

Procédure

Ces instructions supposent que *DB_USER* correspond à l'ID utilisateur de base de données DB2 principal et que *ARCHIVE_USER* correspond à l'ID utilisateur de base de données DB2 secondaire.

1. Utilisez la console de gestion de reconnaissance pour exécuter une reconnaissance. Cette méthode permet de remplir de données la base de données du domaine.
2. Arrêtez le serveur TADDM.
3. Générez et exécutez l'instruction de contrôle REORG pour chaque espace de table utilisé par TADDM.

   ```
   SELECT 'REORG TABLESPACE '||DBNAME||'.'||NAME FROM SYSIBM.SYSTABLESPACE
    WHERE CREATOR IN ('DB_USER', 'ARCHIVE_USER') ORDER BY 1;
   ```

4. Générez et exécutez l'instruction de contrôle REORG pour chaque index utilisé par TADDM.

```
SELECT 'REORG INDEX '||CREATOR||'.'||NAME FROM SYSIBM.SYSINDEXES
 WHERE CREATOR IN ('DB_USER', 'ARCHIVE_USER');
```

5. Générez et exécutez l'instruction de contrôle RUNSTATS pour chaque espace de table utilisé par TADDM.

```
SELECT 'RUNSTATS TABLESPACE '||DBNAME||'.'||NAME||' INDEX(ALL)
SHRLEVEL REFERENCE' FROM SYSIBM.SYSTABLESPACE
WHERE CREATOR IN ('DB_USER', 'ARCHIVE_USER') ORDER BY 1;
```

6. Générez et exécutez à nouveau les instructions de statistiques d'index UPDATE pour chaque utilisateur de la base de données TADDM.

```
SELECT 'UPDATE SYSIBM.SYSINDEXES SET FIRSTKEYCARDF=FULLKEYCARDF
WHERE NAME = '||''''||CAST(RTRIM(name) AS VARCHAR(40))||''''||'
AND CREATOR = '||''''||CAST(RTRIM(creator) AS VARCHAR(40))||''''||'
AND TBNAME = '||''''||CAST(RTRIM(tbname) AS VARCHAR(40))||''''||'
AND TBCREATOR = '||''''||CAST(RTRIM(tbcreator) AS VARCHAR(40))||''''||';'
from sysibm.sysindexes a
where tbcreator in ('DB_USER', 'ARCHIVE_USER')
AND   NAME IN
(SELECT IXNAME
FROM SYSIBM.SYSKEYS B
WHERE A.CREATOR = B.IXCREATOR
AND A.NAME    = B.IXNAME
AND COLNAME = 'PK__JDOIDX')
AND TBNAME IN
(SELECT NAME
FROM SYSIBM.SYSTABLES C
WHERE A.TBCREATOR = C.CREATOR
AND A.TBNAME = C.NAME
AND CARDF > 0);
```

où DB_USER correspond à l'ID utilisateur de base de données DB2 principal et ARCHIVE_USER correspond à l'ID utilisateur de base de données DB2 secondaire.

7. Générez et exécutez à nouveau les instructions de statistiques de colonne UPDATE pour chaque utilisateur de la base de données TADDM.

```
SELECT 'UPDATE SYSIBM.SYSCOLUMNS SET COLCARDF=(SELECT FULLKEYCARDF FROM
SYSIBM.SYSINDEXES WHERE NAME = '||''''||CAST(RTRIM(name)
AS VARCHAR(40))||''''||'
AND CREATOR = '||''''||CAST(RTRIM(creator) AS VARCHAR(40))||''''||'
AND TBNAME = '||''''||CAST(RTRIM(tbname) AS VARCHAR(40))||''''||'
AND TBCREATOR = '||''''||CAST(RTRIM(tbcreator) AS VARCHAR(40))||''''||')
WHERE NAME = '||''''||'PK__JDOIDX'||''''||' AND TBNAME = '||''''||
CAST(RTRIM(tbname) AS VARCHAR(40))||''''||'
AND TBCREATOR = '||''''||CAST(RTRIM(tbcreator) AS VARCHAR(40))||''''||';'
from sysibm.sysindexes a
where tbcreator in ('DB_USER', 'ARCHIVE_USER')
AND   NAME IN
(SELECT IXNAME
FROM SYSIBM.SYSKEYS B
WHERE A.CREATOR = B.IXCREATOR
AND A.NAME    = B.IXNAME
AND COLNAME = 'PK__JDOIDX')
AND TBNAME IN
(SELECT NAME
FROM SYSIBM.SYSTABLES C
WHERE A.TBCREATOR = C.CREATOR
AND A.TBNAME = C.NAME
AND CARDF > 0);
```

8. Contrôlez régulièrement vos tables les plus volumineuses en fonction de votre utilisation de TADDM et, si nécessaire, ajustez leurs paramètres de stockage. Surveillez en particulier la taille des tables suivantes de la base de données, qui peuvent grandir énormément :
   - ALIASES
   - CHANGE_CAUSE_TABLE
   - CHANGE_HISTORY_TABLE
   - MSSOBJLINK_REL
   - PERSOBJ
   - SUPERIORS

   Utilisez les instructions ALTER pour modifier les attributs *PRIQTY* et *SECQTY* en fonction des besoins de votre environnement. Si cela est approprié, envisagez de déplacer les tables dans des espaces de table distincts.
9. Utilisez la commande REBIND sur les packages suivants avec l'option KEEPDYNAMIC(YES) :
   - SYSLH200
   - SYSLH201
   - SYSLH202

Maintenance de la base de données Oracle

Ces instructions de maintenance et d'optimisation s'appliquent aux bases de données Oracle.

1. Exécutez le package dbms_stats dans les tables de base de données. Oracle utilise un optimiseur basé sur les coûts. Cet optimiseur requiert des données pour choisir un plan d'accès. Ces données sont générées par le package dbms_stats. Les bases de données Oracle dépendent des données sur les tables et les index. Sans ces données, l'optimiseur doit faire des estimations.

   La régénération des index et l'exécution du package dbms_stats sont déterminantes pour optimiser les performances en cas d'utilisation d'une base de données Oracle. Une fois la base de données remplie, l'opération doit être exécutée régulièrement (par exemple, chaque semaine).

   - **REBUILD INDEX** : après de nombreuses modifications apportées aux données des tables suit à l'insertion, la suppression et la mise à jour de l'activité, les données séquentielles peuvent se trouver dans des pages de données physiques non séquentielles ; dans ce cas, le gestionnaire de la base de données doit effectuer des opérations de lecture supplémentaires pour accéder aux données. Régénérez les index pour améliorer les performances SQL.

     a. Générez les commandes **REBUILD INDEX** en exécutant l'instruction SQL suivante sur la base de données Oracle, où *utilisateurbd* est la valeur provenant de `com.collation.db.user=` :

        ```
        select 'alter index utilisateurbd.'||index_name||' rebuild tablespace '
        ||tablespace_name||';' from dba_indexes where owner = 'dbuser'
        and index_type not in ('LOB');
        ```

        Ceci génère toutes les commandes **ALTER INDEX** que vous devez exécuter.

     b. Exécutez les commandes dans SQLPLUS ou une fonction comparable. La régénération des index sur un base de données importante prend entre 15 et 20 minutes.
2. **DBMS_STATS** : utilisez le système de gestion de base de données relationnelle Oracle pour collecter divers types de statistiques en vue d'améliorer les performances. L'optimiseur utilise les informations et les statistiques dans le dictionnaire pour déterminer le meilleur accès à la base de données en fonction de la requête fournie. Les informations statistiques sont collectées pour des tables et des index spécifiques dans la base de données locale lorsque vous

exécutez la commande **DBMS_STATS**. Lorsqu'un nombre important de lignes dans les tables est ajouté ou supprimé, ou si les données dans les colonnes dont vous collectez des statistiques sont mises à jour, exécutez à nouveau la commande **DBMS_STATS** pour mettre à jour les statistiques.

- Le programme `gen_db_stats.jy` du répertoire `$COLLATION_HOME/bin` émet les commandes destinées aux bases de données Oracle ou DB2 pour mettre à jour les statistiques sur les tables TADDM. L'exemple suivant montre comment fonctionne le programme :
  a. `cd $COLLATION_HOME/bin`
  b. Exécutez cette instruction SQL, où *réptemp* est le répertoire dans lequel ce fichier a été créé :

     `./gen_db_stats.jy > tmpdir/TADDM_table_stats.sql`

     Dans un déploiement de serveur de diffusion en continu, exécutez cette instruction sur le serveur de stockage principal.
  c. Après cela, copiez le fichier sur le serveur de la base de données et exécutez la commande suivante :
     – Pour exécuter un fichier script dans SQLPlus, entrez @ et le nom du fichier : `SQL > @{file}`
  d. Exécutez les commandes dans SQLPLUS ou une fonction comparable.

3. Un pool de mémoire tampon (ou cache) est une structure de mémoire dans la zone mémoire commune du système (SGA) Oracle pour chaque instance. Ce cache sert à mettre des blocs de données en mémoire. L'accès aux données depuis la mémoire est nettement plus rapide que l'accès depuis le disque. L'objectif de l'optimisation du tampon de blocs est de mettre en cache de façon efficace et régulière des blocs de données utilisateur et d'offrir un accès plus rapide aux données. Cette optimisation est une tâche clé dans toute initiative d'optimisation d'Oracle et fait partie de l'optimisation et de la surveillance continues des bases de données de production. Le produit Oracle conserve son propre cache dans la zone SGA pour chaque instance. Un cache de taille correcte peut donner un taux de présence en mémoire cache de plus de 90 %, ce qui signifie que neuf demandes sur dix sont satisfaites sans passer par le disque. Si un cache est insuffisant, le taux de présence en mémoire cache est faible et il y a plus d'entrées-sorties sur le disque physique. Si sa taille est trop élevée en revanche, certaines parties sont sous-utilisées et des ressources mémoire sont gâchées.

Tableau 36. Instructions relatives à la taille du pool de mémoire tampon (`db_cache_size`)

Nombre d'éléments de configuration	Instruction sur la taille du pool de mémoire tampon
< 500 000	38 000
500 000 - 1 000 000	60 000
> 1 000 000	95 000

4. Vous pouvez doubler le nombre maximum de curseurs ouverts si la reconnaissance ou le chargement en bloc est trop lent(e) et que NRS contient l'erreur suivante :

```
com.ibm.tivoli.namereconciliation.service.NrsService
getAliases(masterGuid)
SEVERE: NOTE ⌂*** SQL State = 60000.   SQL Code  = 604.   SQL Message =
ORA-00604: error occurred at recursive SQL level 1
ORA-01000: maximum open cursors exceeded
ORA-01000: maximum open cursors exceeded
```

5. Vérifiez que la version de votre pilote JDBC Oracle et celle de votre serveur Oracle correspondent. Si nécessaire, remplacez le fichier du pilote JDBC Oracle dans les emplacements suivants.

   Remarque : Ceci s'applique uniquement si le visualiseur de rapports BIRT est activé.

   - TADDM 7.3.0 - `$COLLATION_HOME/deploy-tomcat/birt-viewer/WEB-INF/platform/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.1.r22x_v20070919/drivers/`
   - TADDM versions 7.3.0.1 et ultérieures - `$COLLATION_HOME/apps/birt-viewer/WEB-INF/platform/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.1.r22x_v20070919/drivers/`
   - `$COLLATION_HOME/lib/jdbc/`

Communications avec la base de données

Si la base de données est non disponible, le serveur de stockage tente d'établir à nouveau la connexion.

Lorsqu'il n'y a aucune connexion entre la base de données et le serveur de stockage, le serveur de stockage attend aussi longtemps que ce qui est spécifié dans la propriété `com.ibm.cdb.db.timeout`, puis fait une tentative de connexion à la base de données. Le nombre de nouvelles tentatives d'établissement de la connexion est indiqué dans la propriété `com.ibm.cdb.db.max.retries`.

Pour plus d'informations sur les propriétés de la base de données, accédez à la section Propriétés de base de données.

Réglage des performances de reconnaissance

Vous pouvez mettre à jour les propriétés `com.collation.discover.dwcount` et `com.collation.discover.observer.topopumpcount` dans le fichier `collation.properties` pour influencer le taux de reconnaissance et le taux auquel les résultats de la reconnaissance sont stockés dans la base de données TADDM.

Pour des informations sur ces propriétés, voir «Propriétés des performances», à la page 95.

Si vous augmentez les valeurs des propriétés `com.collation.discover.dwcount` ou `com.collation.discover.observer.topopumpcount`, vous devez également avoir augmenté la quantité de mémoire installée en augmentant le paramètre de la taille de segment maximale pour les machines virtuelles Java suivantes :

Pour la propriété `dwcount` :

- Dans un déploiement de serveur de diffusion en continu :
  - Reconnaissance
  - DiscoverService
- Dans un déploiement de serveur de domaine :
  - Reconnaissance

Pour la propriété `topopumpcount` :

- Dans un déploiement de serveur de diffusion en continu :
  - StorageService
- Dans un déploiement de serveur de domaine :
  - Topologie

Pour plus d'informations, voir «Machine virtuelle Java : optimisation des paramètres IBM», à la page 156.

Pour plus d'informations sur le réglage des performances de reconnaissance, reportez-vous au document intitulé *Optimisation des performances de reconnaissance* à l'adresse http://www.ibm.com/software/brandcatalog/ismlibrary/.

Optimisation du taux de reconnaissance

La zone de l'attribut du taux de reconnaissance est celle permettant le plus d'optimisation. La propriété avec le plus d'impact sur les performances est le nombre d'unités d'exécution de tâche de reconnaissance. Vous pouvez également utiliser les détecteurs actifs pour contrôler les performances ou les améliorer en spécifiant les tailles de groupement de sessions.

Une unité d'exécution de tâche reconnaissance est une unité d'exécution qui exécute des détecteurs. La propriété suivante spécifie le nombre maximum d'unités d'exécution de tâche de reconnaissance :

```
com.collation.discover.dwcount=32
```

Si le serveur contient suffisamment d'espace, vous pouvez augmenter ce nombre et permettre à plusieurs détecteurs de s'exécuter en parallèle.

Détecteurs actifs

Pour contrôler les performances, surveillez les détecteurs actifs. Un détecteur actif peut se trouver dans l'une des trois étapes d'exécution suivantes :

démarré
: Un détecteur dans cet état découvre un ou plusieurs éléments de configuration.

reconnu
: Un détecteur dans cet état a terminé la reconnaissance d'un ou plusieurs éléments de configuration à enregistrer dans le magasin de données.

En cours de stockage
: Un détecteur dans cet état enregistre les résultats de sa reconnaissance dans la base de données.

Pour classer les capteurs actifs par étape d'exécution, cliquez sur la colonne Description.

En observant une exécution de reconnaissance et en comparant le nombre de détecteurs actifs à l'état démarré au nombre de détecteurs actifs à l'état reconnu ou en cours de stockage, il est possible d'évaluer si la reconnaissance d'attributs est plus rapide ou plus lente que le stockage d'attributs pour un environnement déterminé. Comme pour toutes les modifications apportées au fichier `collation.properties`, vous devez redémarrer le serveur pour que les changements s'appliquent.

Exemples :

Détecteurs actifs : STARTED (démarré), DISCOVERED (reconnu), STORING (en cours de stockage).

Si le nombre de détecteurs (DISCOVERED + STORING) est inférieur au nombre de détecteurs STARTED, cela peut indiquer que la reconnaissance correspond au goulot d'étranglement des performances.

Si le nombre de détecteurs (DISCOVERED + STORING) dépasse le nombre de détecteurs STARTED, cela peut indiquer que le stockage correspond au goulot d'étranglement des performances.

Tailles de pool de session et de passerelle

Pour détecter les attributs d'un élément de configuration particulier, un capteur requiert une session SSH ou WMI avec son ordinateur hôte. Pour améliorer les performances, ces sessions sont regroupées en pool et mises en cache. Dans la plupart des cas, les tailles de pool par défaut sont suffisantes, toutefois, lorsque ce n'est pas le cas, elles peuvent limiter le taux de reconnaissance. Pour contrôler cette condition, vous pouvez modifier la propriété suivante sur `true` :

```
com.collation.platform.session.ExtraDebugging=false
```

Vous devez redémarrer le serveur de reconnaissance pour appliquer la modification. Après avoir exécuté une reconnaissance, recherchez les éventuels problèmes de délai d'attente liés aux groupements de sessions dans les journaux DiscoverManager. Pour cela, recherchez les journaux contenant `pool lock`. L'exemple suivant relate une dégradation des performances causée par un conflit de pool de sessions :

```
2006-08-04 16:11:50,733 DiscoverManager [DiscoverWorker-34]
WindowsComputerSystemAgent(192.168.16.181)
INFO session.SessionClientPool -
Session client [3x ssh2:/admlxz@151.179.84.85]#9612508
waited 158.682 seconds for pool lock
```

Il est possible d'augmenter la taille de pool si le délai d'attente est trop long pour une session. Pour cela, deux méthodes existent. Vous pouvez modifier la taille de pool globale pour les sessions par hôte en modifiant la propriété suivante dans le fichier `collation.properties` :

```
com.collation.platform.session.PoolSize=3
```

Il est néanmoins peu probable que le conflit concerne les sessions dans la plupart, voire tous les hôtes de l'environnement. Le conflit est probablement restreint à un plus petit nombre d'hôtes plus volumineux utilisés par de nombreux détecteurs. Le serveur de reconnaissance utilise une propriété sectorisée, ce qui signifie que de nombreuses propriétés du fichier `collation.properties` utilisent une valeur pour les cibles générales et une autre pour les cibles spécifiques. Vous pouvez régler cette propriété en ajoutant une adresse IP ou un nom de portée de serveur de reconnaissance, comme dans l'exemple suivant :

```
com.collation.platform.session.PoolSize.10.10.250.1=20
```

Dans ce cas, la taille de pool est 20 pour 10.10.250.1 mais 3 pour tous les autres hôtes. Vous pouvez consulter les messages de journal dans les fichiers journaux DiscoverManager et déterminer pour quels hôtes la taille de pool de session par défaut est insuffisante, puis apporter les modifications appropriées dans le fichier `collation.properties`.

Un paramètre relatif est la taille de pool de passerelle. Il définit le nombre de sessions autorisées entre le serveur de reconnaissance et la passerelle Windows. Vous pouvez le spécifier en modifiant la propriété suivante :

```
com.collation.platform.session.GatewayPoolSize=10
```

Si votre environnement contient principalement des systèmes informatiques Windows, augmentez la valeur de cette propriété afin qu'elle soit égale au nombre d'unités d'exécution de tâche de reconnaissance.

Optimisation du stockage

Le stockage est la deuxième zone d'optimisation principale. Si le nombre de détecteurs en cours de stockage équivaut plus ou moins à la valeur de la propriété qui spécifie le nombre d'unités d'exécution de stockage parallèles, le stockage des résultats de la reconnaissance correspond au goulot d'étranglement des performances. Pour améliorer les performances, vous pouvez également limiter le nombre d'unités d'exécution qui stockent les données.

La propriété suivante spécifie le nombre d'unités d'exécution de stockage parallèles. Il s'agit de l'un des principaux paramètres permettant de contrôler les performances de stockage de reconnaissance :

`com.collation.discover.observer.topopumpcount`

Pour améliorer les performances de stockage lors de l'exécution des agents de topologie, vous pouvez limiter le nombre d'unités d'exécution qui stockent les données pendant une détection. Ainsi les détections sont plus rapides. Pour spécifier le nombre d'unités d'exécution qui s'exécutent, modifiez les propriétés suivantes dans le fichier `collation.properties` :

com.ibm.cdb.discover.observer.topopump.threshold
Cette propriété spécifie le nombre d'unités d'exécution de stockage.

com.ibm.cdb.discover.observer.topopump.threshold.<nom_groupe_agent>
Cette propriété spécifie le nombre d'unités d'exécution de stockage lors de l'exécution du groupe d'agent spécifié.

Le tableau suivant démontre à quel point la propriété`com.ibm.cdb.discover.observer.topopump.threshold` peut améliorer les performances de détection. Les calculs concernent une base de données avec 76 000 éléments de configuration.

Valeur de propriété seuil	Amélioration de l'heure de pourcentage
0,2	55
0,5	33
0,7	13
1	0

Machine virtuelle Java : optimisation des paramètres IBM

Vous pouvez définir les paramètres de la machine virtuelle Java (JVM) permettant de réduire la fragmentation du segment de mémoire Java et d'améliorer les performances.

La fragmentation du segment de mémoire Java peut se produire quand le nombre d'objets traités augmente. Vous pouvez définir plusieurs paramètres pour réduire la fragmentation du segment de mémoire.

- La zone de stockage kCluster est exclusivement utilisée pour les blocs de classe. Elle est suffisamment grande pour contenir 1 280 entrées. La longueur de chaque bloc de classe est de 256 octets. Cette valeur par défaut est normalement trop petite et peut entraîner la fragmentation du segment de mémoire. Définissez le paramètre kCluster **-Xk** comme suit pour réduire la fragmentation du segment

de mémoire. Il s'agit de valeurs de départ qui doivent éventuellement être ajustées dans votre environnement. Une analyse du cliché de tas serait préférable pour connaître la taille idéale.

  – Topology: -Xk8300
  – EventsCore: -Xk3500
  – DiscoverAdmin: -Xk3200
  – Proxy: -Xk5700
  – Discover: -Xk3700

  Implémentez ces changements dans le fichier `collation.properties` en ajoutant des entrées dans la section des paramètres spécifiques au fournisseur de la machine virtuelle Java. Par exemple, pour implémenter ces changements pour le serveur de topologie, ajoutez la ligne suivante :

  ```
  com.collation.Topology.jvmargs.ibm=-Xk8300
  ```

- Une autre option pour les problèmes de fragmentation consiste à allouer de l'espace spécialement aux objets LOB supérieurs > 64 Ko. Prenez dans ce cas le paramètre **-Xloratio**. Par exemple :

  – **-Xloratio0.2**

  Cette commande réserve x% du segment de mémoire Java actif (non pas x% de -Xmx, mais x% de la taille actuelle du segment de mémoire Java) pour l'allocation d'objets LOB (≥ 64 Ko) uniquement. -Xmx doit être modifié de façon à ne pas réduire la taille de la zone des petits objets. Une analyse du cliché de tas serait préférable pour connaître la valeur idéale pour ce paramètre.

D'autres paramètres pouvant être définis affectent les performances Java. Pour modifier la valeur d'une option existante de la machine virtuelle Java, éditez l'un des fichiers suivants :

- Pour un serveur de domaine dans TADDM 7.3.0, le fichier `$COLLATION_HOME/deploy-tomcat/ROOT/WEB-INF/cmdb-context.xml`.
- Pour un serveur de domaine dans TADDM versions 7.3.0.1 et ultérieures, le fichier `$COLLATION_HOME/apps/ROOT/WEB-INF/cmdb-context.xml`.
- Pour un serveur de synchronisation dans TADDM 7.3.0, le fichier `$COLLATION_HOME/deploy-tomcat/ROOT/WEB-INF/ecmdb-context.xml`.
- Pour un serveur de synchronisation dans TADDM versions 7.3.0.1 et ultérieures, le fichier `$COLLATION_HOME/apps/ROOT/WEB-INF/ecmdb-context.xml`.
- Pour un serveur de reconnaissance dans TADDM 7.3.0, le fichier `$COLLATION_HOME/deploy-tomcat/ROOT/WEB-INF/discovery-server-context.xml`.
- Pour un serveur de reconnaissance dans TADDM versions 7.3.0.1 et ultérieures, le fichier `$COLLATION_HOME/apps/ROOT/WEB-INF/discovery-server-context.xml`.
- Pour un serveur de stockage dans TADDM 7.3.0, le fichier `$COLLATION_HOME/deploy-tomcat/ROOT/WEB-INF/storage-server-context.xml`.
- Pour un serveur de stockage dans TADDM versions 7.3.0.1 et ultérieures, le fichier `$COLLATION_HOME/apps/ROOT/WEB-INF/storage-server-context.xml`.

Pour éditer l'un de ces fichiers et modifier les paramètres de l'un des service TADDM, recherchez d'abord ce service dans le fichier. L'exemple suivant présente le début d'une définition de service dans le fichier XML :

```
<bean id="Discover"
 class="com.collation.platform.service.ServiceLifecycle" init-method="start"
 destroy-method="stop">
```

```
<property name="serviceName">
 <value>Discover</value>
</property>
```

Dans la définition, des éléments et des attributs contrôlent les arguments JVM. Par exemple :

```
<property name="jvmArgs">
 <value>-Xms8M;-Xmx512M;
 -Djava.nio.channels.spi.SelectorProvider=sun.nio.ch.PollSelectorProvider
 </value>
</property>
```

Les arguments de la machine virtuelle Java peuvent être placés dans une liste et séparés par des points-virgules dans l'élément suivant :

```
<property name="jvmArgs"><value>
```

Vous pouvez également modifier les propriétés JVM du fichier `collation.properties`. Ces propriétés peuvent avoir les formats suivants :

com.collation.JVM.jvmargs.FOURNISSEUR
: Les propriétés présentant ce format sont ajoutées aux valeurs lues depuis le fichier `*-config.xml`.

com.collation.jvmargs.FOURNISSEUR
: Les propriétés présentant ce format sont ajoutées à toutes les JVM TADDM.

com.collation.JVM.jvmargs
: Les propriétés présentant ce format remplacent toutes les valeurs spécifiées dans le fichier `*-config.xml`.

où

- La JVM peut être `Proxy`, `Topology`, `EventsCore`, `ExcmdbCore`, `DiscoverAdmin`, `StorageService`, `DiscoveryService`
- Le `FOURNISSEUR` peut être `ibm` ou `sun`

Optimisation des propriétés de la machine virtuelle Java

Dans le fichier `collation.properties`, les valeurs par défaut des propriétés de la machine virtuelle Java qui s'appliquent à la console de gestion de reconnaissance de TADDM dépendent du nombre d'équivalents serveur présents dans votre environnement.

Valeurs par défaut des propriétés JVM qui s'appliquent à la console de gestion de reconnaissance

- Petit environnement (moins de 1 000 équivalents serveur) :
  - com.collation.gui.initial.heap.size=128m
  - com.collation.gui.max.heap.size=512m
- Environnement moyen (1 000–2 500 équivalents serveur) :
  - com.collation.gui.initial.heap.size=256m
  - com.collation.gui.max.heap.size=768m
- Grand environnement (2 500–5 000 équivalents serveur) :
  - com.collation.gui.initial.heap.size=512m
  - com.collation.gui.max.heap.size=1024m

Optimisation du réseau

Une fois le système implémenté, le réseau doit être surveillé pour que l'utilisation de sa bande passante ne dépasse pas 50 %.

Le réseau peut influer sur les performances globales de votre application et il constitue généralement un facteur de performances lorsqu'un délai existe dans les situations suivantes:

- Délai entre l'envoi d'une demande par un système client au serveur et la réception de cette demande par le serveur.
- Délai entre le renvoi des données par le serveur au système client et la réception de ces données par le système client.

Optimisation du serveur DNS

TADDM est sensible aux performances de l'infrastructure DNS déployée. Même si les performances DNS sont adaptées à certaines applications, des configurations peuvent être requises pour optimiser les performances de TADDM.

TADDM exécute de nombreuses requêtes de recherche DNS afin de résoudre les noms affichés de composants et d'événements. A la différence de la plupart des autres applications, TADDM utilise principalement des recherches inversées (mappage des adresses IP aux noms) au lieu de recherches directes (mappage des noms aux adresses IP).

A cause de cela, les problèmes de performances DNS peuvent affecter davantage les performances de TADDM que celles des autres applications. Par exemple, un temps de réponse DNS de 500 millisecondes affecte peu une application standard, mais peut poser des problèmes de performances importants pour TADDM en raison du nombre élevé de requêtes DNS que l'application exécute. De plus, comme d'autres applications exécutent uniquement des recherches directes, les problèmes de performances des recherches inversées n'affectent pas la plupart des applications, mais affectent TADDM.

De manière générale, les problèmes de performances de l'infrastructure DNS doivent être résolus afin de profiter à tous les consommateurs de services DNS. Si cela n'est pas possible, il existe plusieurs moyens de réduire l'impact des problèmes de performance DNS sur TADDM :

- Vérifiez que la délégation in-addr.arpa des recherches inversées est correctement configurée. Les problèmes de délégation peuvent entraîner de longues interruptions pendant les recherches inversées car le serveur TADDM tente de joindre des serveurs qui n'existent pas. Ce type de problème de configuration affecte uniquement les applications qui, comme TADDM, exécutent des recherches inversées.
- Configurez au moins un serveur DNS de cache/réacheminement sur un système de serveurs TADDM et configurez les serveurs TADDM pour qu'ils utilisent ce serveur DNS pour les recherches. Cela permet de mettre en cache les recherches DNS dans l'environnement TADDM local, en fonction des règles TTL des zones. Ce type de serveur ne comporte pas d'état et requiert ainsi peu de maintenance et entraîne des frais minimes.
- Configurez au moins un serveur DNS esclave sur un système de serveurs TADDM, et configurez les serveurs TADDM pour qu'ils utilisent ce serveur DNS pour les recherches. Cela permet d'exécuter les recherches DNS dans l'environnement TADDM local sans communication avec l'infrastructure DNS générale. Les serveurs DNS esclaves mettent à jour leur état automatiquement et requièrent ainsi peu de maintenance et entraîne des frais minimes.

- Utilisez une autre méthode de recherche, comme le fichier `hosts`, au lieu du serveur DNS. Cette méthode peut requérir davantage de maintenance.

Remarque : Ne modifiez pas les paramètres de cache DNS dans le fichier `java.security`. Bien que les paramètres de cache puissent affecter les performances DNS, les modifications apportées à ce fichier de configuration ne sont pas conservées lors de l'application des correctifs de maintenance TADDM. Utilisez l'une des méthodes décrites dans cette rubrique pour optimiser les performances DNS.

Optimisation du serveur de synchronisation

Les performances du serveur de synchronisation sont très dépendantes du traitement de la base de données et, par conséquent, de la maintenance et de l'optimisation de celle-ci. En cas de problèmes liés aux performances lors du traitement de la synchronisation, consultez les informations relatives à l'optimisation de la base de données et notez notamment les paramètres du pool de mémoire tampon pour les bases de données DB2, les paramètres du cache de la mémoire tampon pour les bases de données Oracle et les informations relatives à la maintenance de la base de données.

Mettez à jour la configuration de la base de données DB2 pour le serveur de synchronisation en entrant la commande suivante :

```
UPDATE DATABASE CONFIG FOR TADDM USING
   UTIL_HEAP_SZ 5000
   LOGBUFSZ 1024
   LOCKLIST 20000
   SORTHEAP 2048
   PCKCACHESZ AUTOMATIC
;
```

Optimisation du système Windows

Pour attribuer davantage de mémoire aux services TADDM, réglez les systèmes Windows.

Procédez comme suit :

- Le fichier de pagination du système ne doit pas se trouver sur la même unité que le système d'exploitation. Si possible, placez le fichier de pagination système sur une autre unité de disque.
- Configurez la base de données et le serveur d'applications de sorte à optimiser les données des applications réseau.

Génération de rapport

Vous pouvez créer et ajouter des rapports personnalisés au portail de gestion de données à l'aide de visualiseurs de rapports externes ou JSP ou du système de génération de rapports BIRT.

Visualiseurs de rapport externes

Un visualiseur de rapport externe permet d'exécuter un programme externe qui génère un rapport. Le programme externe accède aux données à l'aide l'API TADDM, à partir de la ligne de commande. Le rapport s'affiche alors dans l'interface utilisateur.

Création de la logique du visualiseur de rapport externe

Un rapport externe peut être implémenté au sein d'un programme exécutable quelconque. Les exemples sont un script Perl, un script de shell ou un programme Java. Le programme externe doit sortir un fichier html valide via une sortie standard pour que le rapport obtenu puisse apparaître dans le portail de gestion de données.

Pourquoi et quand exécuter cette tâche

L'implémentation typique d'un visualiseur de rapport externe utilise un script de shell pour interroger l'API de TADDM et générer les résultats XML de la requête dans un fichier temporaire. Le script de shell démarre ensuite un processeur XSLT pour transformer les résultats de la requête en sortie HTML, qui à son tour est renvoyée en sortie standard.

Important : Les visualiseurs de rapport externe utilisant l'API TADDM doivent fournir des droits d'accès au programme de ligne de commande du script `api.sh` sous Linux et UNIX et dans le fichier `api.bat` sous Windows. Les droits d'accès étant des arguments de ligne de commande dans le script `api.sh` et `api.bat`, ils risquent d'être visibles pour les autres utilisateurs du système à travers des listes de processus. Pour éviter la divulgation de mots de passe confidentiels, envisagez de définir un compte factice avec accès en lecture aux objets devant apparaître dans des rapports générés en externe.

L'exemple suivant est une simple implémentation de script d'interpréteur de commandes Bourne de rapport externe. Copiez le contenu suivant dans un nouveau fichier, `$COLLATION_HOME/sdk/bin/appservers.sh` et rendez le fichier lisible et exécutable par l'utilisateur sous lequel le serveur TADDM s'exécute :

```
#!/bin/sh
# Set environment variables for called scripts
export COLLATION_HOME=/opt/ibm/taddm/dist

# Invoke the query via API and output to $COLLATION_HOME/sdk/bin/appServers.xml
# NOTE: Change 'restrictedUser' and 'restrictedPassword' to your dummy account
#       credentials.
sh $COLLATION_HOME/sdk/bin/api.sh -l log -H localhost -u restrictedUser -p
restrictedPassword \ find AppServer > $COLLATION_HOME/sdk/bin/appServers.xml

# Invoke the XSLT processor
sh $COLLATION_HOME/sdk/bin/xslt.sh -XSL $COLLATION_HOME/sdk/bin/appServers.xsl
```

L'exemple suivant est de la feuille de style `appservers.xsl` utilisée pour transformer le fichier `appservers.xml` généré par le script de shell. Le rapport affiche des noms de serveur d'applications et les versions de produit. Copiez le contenu dans un nouveau fichier, `$COLLATION_HOME/sdk/bin/appservers.xsl` et rendez le fichier lisible par l'utilisateur sous lequel s'exécute le serveur TADDM.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet version = '1.0' xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
xmlns:coll="urn:www-collation-com:1.0" xmlns:xhtml="http://www.w3.org/1999/xhtml">
        <xsl:variable name="nl">
        <xsl:text>
        </xsl:text>
        </xsl:variable>

        <xsl:variable name="pageheadertext">
                Simple Application Server report
        </xsl:variable>

        <xsl:variable name="pagefootertext">
```

```
                End Simple Application Server report
        </xsl:variable>


        <xsl:template match="/">
        <html>
                <head>
                <link rel="stylesheet" type="text/css" media="all"
       href="styles.css" />
                </head>
        <body>
                <h3>
                        <xsl:value-of select="$pageheadertext"/>
                </h3>
    <table border="1" width="100%">
                 <tr>
                     <th>Product Version/th>
                     <th>Name/th>
                        </tr>

      <xsl:apply-templates select="document('appServers.xml')/coll:results"/>
    </table>
                <xsl:value-of select="$nl"/>
        </body></html>
        </xsl:template>

        <xsl:template match="coll:AppServer">
                        <tr>
                          <td>xsl:value-of select="coll:productVersion"/></td>
                          <td>xsl:value-of select="coll:displayName"/></td>
                        </tr>
        </xsl:template>
</xsl:stylesheet>
```

Pour vérifier la logique du rapport, exécutez le script `appServer.sh` à partir d'une ligne de commande. Une sortie HTML s'affiche.

Ajout d'un visualiseur de rapport externe au portail de gestion de données

Les rapports sont ajoutés au portail de gestion de données en modifiant le fichier `reports.xml`. Le fichier `reports.xml` se trouve dans le répertoire `$COLLATION_HOME/etc/ xml/ / CDM`.

Procédure

Pour ajouter un visualiseur de rapport externe au portail de gestion de données, procédez comme suit :

1. A l'aide d'un éditeur de texte, ouvrez le fichier `$COLLATION_HOME/etc/CDM/xml/reports.xml`.
2. Dans le fichier `reports.xml`, spécifiez le descripteur du rapport, le groupe, le nom et le script externe pour la définition du rapport. L'exemple suivant indique comment créer un rapport externe, intitulé `Serveurs d'application`, dans le groupe `Rapports d'inventaire` et spécifie le fichier `sdk/bin/appServers.sh` :

   ```
   <bean class="com.collation.cdm.reports.viewer.ExternalReportViewer" id="AppServers1">
    <property name="reportGroup"><value>Inventory Reports</value></property>
    <property name="reportName"><value>Application Servers</value></property>
    <property name="script"><value>sdk/bin/appServers.sh</value></property>
   </bean>
   ```
3. Sauvegardez le fichier `$COLLATION_HOME/etc/CDM/xml/reports.xml`.
4. Le rapport est maintenant affiché dans le portail de gestion de données.

Visualiseurs de rapport JSP

Un visualiseur de rapport JSP fournit davantage de flexibilité et de sécurité aux utilisateurs ayant des connaissances de création de pages JSP (Java Server Pages). La logique de génération de rapport, notamment tout accès API, est placée dans une page JSP qui est ensuite rendue par le portail de gestion de données. Lorsque vous utilisez des visualiseurs de rapport JSP, les droits d'accès de sécurité sont extraits automatiquement de l'utilisateur qui est connecté.

Création de la logique du visualiseur de rapport JSP

La logique d'un visualiseur de rapport JSP est contenue dans un JSP qui est appelé par le portail de gestion de données. L'implémentation typique d'un rapport JSP utilise une classe auxiliaire Java, appelée TMSDataHelper pour interroger l'API de TADDM. Les résultats de la requête sont des objets qui peuvent être manipulés à l'aide de méthodes Java. Pour plus d'informations sur les API de TADDM et le modèle, consultez la documentation SDK dans `$COLLATION_HOME/sdk/doc`.

Pourquoi et quand exécuter cette tâche

L'exemple suivant est une simple implémentation du visualiseur de rapport JSP. Copiez le contenu suivant dans un nouveau fichier, `$COLLATION_HOME/deploy-tomcat/reports.war/WEB-INF/view/custom.jsp` si vous utilisez TADDM 7.3.0 ou `$COLLATION_HOME/apps/reports.war/WEB-INF/view/custom.jsp` si vous utilisez TADDM version 7.3.0.1 ou ultérieure, et rendez ce fichier lisible et exécutable par l'utilisateur qui exécute le serveur TADDM.

L'exemple suivant montre la feuille de style `appservers.xsl` utilisé pour transformer le fichier `appservers.xml` généré par le script de shell. Le rapport affiche des noms de serveur d'applications et les versions de produit. Copiez le contenu dans un nouveau fichier, `$COLLATION_HOME/sdk/bin/appservers.xsl` et rendez le fichier lisible par l'utilisateur qui exécute le serveur TADDM.

```
<%@ page language="java" %>
<%@ page import="com.collation.cdm.common.util.TMSDataHelper" %>
<%@ page import="java.lang.StringBuffer" %>
<%@ page import="com.collation.cdm.reports.util.ReportsParser" %>
<%@ page import="com.collation.cdm.common.util.TMSReportingTransformer" %>
<%@ page import="com.collation.platform.model.AttributeNotSetException" %>
<%@ page import="com.collation.platform.model.ModelObject" %>
<%@ page import="com.collation.platform.model.topology.sys.ComputerSystem" %>
<%@ page import="com.collation.platform.model.topology.process.BusinessProcess" %>
<%@ page import="com.collation.platform.model.topology.process.Activity" %>
<%@ taglib prefix="x" uri="http://java.sun.com/jstl/xml" %>
<%@ taglib prefix="c" uri="http://java.sun.com/jsp/jstl/core" %>
<%@ page import="com.collation.platform.util.Props" %>
<%@ page import="java.util.ArrayList"%>
<%@ page import="com.collation.cdm.common.messages.CdmLocalizedMessages"%>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%
java.util.Locale locale =
com.collation.cdm.common.util.CDMUtil.checkLocale(request.getLocale());
    if (null == session.getAttribute(org.apache.struts.Globals.LOCALE_KEY)) {
session.setAttribute(org.apache.struts.Globals.LOCALE_KEY, locale);
    }
%>
<%
//TMSDataHelper is a utility class for running MQL queries against the DB
TMSDataHelper tms = new TMSDataHelper(locale);

//Perform a query for all ComputerSystems
ModelObject dataIn[] = tms.doModelObjectQuery("SELECT * FROM ComputerSystem",null);
```

```
  //Build an HTML report based on the API output
  StringBuffer output = new StringBuffer();
  output.append("<p>");
  output.append("<table border=\"1\">");
               int c = 0;
               int s = dataIn.length;
               while (cs) {
                       ComputerSystem tmo = (ComputerSystem)dataIn[c];
                       String csName = null;
                       String csLabel = null;
                       if (tmo.hasName()) {
                               try {
                                       csName = tmo.getName();
                               } catch (AttributeNotSetException e) {
                                       csName = "unknown";
                               }
                       }
                       if (tmo.hasSignature()) {
                               try {
                                       csLabel = tmo.getSignature();
                               } catch (AttributeNotSetException e) {
                                       csLabel = "";
                               }
                       }
                       output.append("<tr><td colspan=\"2\" bgcolor=\"#9999FF\">");
                       output.append("ComputerSystem" + "<br>");
                       output.append(" Name: " + csName + "<br>");
                       output.append("</td><td>");
                       output.append("Signature: " + csLabel);
                       output.append("</td></tr>");
                       c++;
               }
output.append("</table>");
String bpstring = output.toString();
%>
<html>
<body>
<h1>Sample JSP Report/h1>
<%=bpstring%>
</body>
</html>
```

Ajout du visualiseur de rapport JSP au portail de gestion de données

Les rapports sont ajoutés au portail de gestion de données en modifiant le fichier `reports.xml`. Le fichier `reports.xml` se trouve dans le répertoire `$COLLATION_HOME/etc/ xml/ / CDM`.

Procédure

Pour ajouter un visualiseur de rapport JSP au portail de gestion de données, procédez comme suit :

1. A l'aide d'un éditeur de texte, ouvrez le fichier `$COLLATION_HOME/etc/CDM/xml/reports.xml`.
2. Dans le fichier `reports.xml`, spécifiez le descripteur du rapport, le groupe, le nom et le script externe pour la définition du rapport. L'exemple suivant indique comment créer un rapport externe, intitulé `Rapport personnalisé` dans le groupe `Rapports d'inventaire` et spécifie le script `/WEB-INF/view/custom.jsp` :

```
<bean class="com.collation.cdm.reports.viewer.JSPReportViewer" id="CustomReport">
 <property name="reportGroup"><value>Inventory Reports</value></property>
 <property name="reportName"><value>Custom Report</value></property>
 <property name="script"><value>/WEB-INF/view/custom.jsp</value></property>
</bean>
```

3. Sauvegardez le fichier `$COLLATION_HOME/etc/CDM/xml/reports.xml`.
4. Le rapport doit maintenant apparaître dans le portail de gestion de données.

Rapports avec Tivoli Common Reporting

Puisque la visualisation de rapports BIRT dans le visualiseur de rapports BIRT n'est pas sécurisée et est désactivée par défaut, vous pouvez importer des rapports BIRT pour TADDM dans Tivoli Common Reporting. Cette facilité permet d'établir des rapports croisés avec les données de TADDM. Vous pouvez également utiliser des fonctions de Tivoli Common Reporting comme la planification de rapports ou utiliser Tivoli Common Reporting comme référentiel central pour des rapports.

Pour certaines tâches, le déroulement des étapes à réaliser diffère selon la version de Tivoli Common Reporting ou la base de données que vous utilisez.

Fix Pack 1 Si vous disposez de TADDM 7.3 groupe de correctifs 1 ou version ultérieure, voir aussi la rubrique The enhanced Cognos model in TADDM 7.3 FP*x* du document Best Practices Guide.

Présentation de Tivoli Common Reporting

L'outil Tivoli Common Reporting est une fonction de génération de rapports incluse dans certains produits Tivoli qui offre une approche centralisée permettant de visualiser et d'administrer des rapports pour leur donner un format cohérent sur plusieurs produits.

Tivoli Common Reporting comprend un magasin de données pour le stockage et l'organisation de rapports, et des interfaces permettant de gérer, d'exécuter, de planifier et de visualiser des rapports. Tivoli Common Reporting utilise à la fois les moteurs d'exécution Cognos et BIRT.

Important : Tivoli Common Reporting est disponible sur le disque d'installation d'IBM Jazz for Service Management. Si vous n'envisagez pas d'installer IBM Jazz for Service Management, vous pouvez utiliser la fonction de génération de rapports BIRT intégrée.

Si Tivoli Common Reporting est déjà installé sur votre système, vous pouvez importer en option les rapports TADDM prédéfinis, qui sont compatibles avec Tivoli Common Reporting. Vous pouvez ensuite utiliser Tivoli Common Reporting comme référentiel central pour les rapports sur les produits Tivoli. Vous pouvez également utiliser des options de génération de rapports améliorés, notamment des fonctions de génération de rapports de produits croisés, de sécurité basée sur les rôles et de planification des rapports.

Pour connaître les versions prises en charge des produits, accédez à la section «Versions prises en charge», à la page 201.

Remarque : Si vous utilisez TADDM avec IBM Tivoli Change et Configuration Management Database (CCMDB) ou IBM SmartCloud Control Desk, consultez la documentation de CCMDB ou d'IBM SmartCloud Control Desk pour plus d'informations sur les versions de Tivoli Common Reporting qui sont prises en charge.

Pour plus d'informations sur Tivoli Common Reporting, accédez à https://www.ibm.com/developerworks/community/groups/service/html/communityview?communityUuid=9caf63c9-15a1-4a03-96b3-8fc700f3a364.

Installation de Tivoli Common Reporting et de IBM Cognos Framework Manager

Vous devez installer Tivoli Common Reporting et IBM Cognos Framework Manager.

Procédure

Pour installer Tivoli Common Reporting et IBM Cognos Framework Manager, procédez comme suit :

1. Installez Tivoli Common Reporting avec les options par défaut présentées. Si vous utilisez une base de données Oracle, vous devez utiliser Tivoli Common Reporting 2.1 ou 2.3.
2. Installez le package d'IBM Cognos Framework Manager disponible dans le dossier `CognosModeling`. Utilisez les options par défaut présentées.
3. S'il est disponible, installez également le correctif de sécurité qui se trouve dans le dossier `CognosModelingFix`. Utilisez les options par défaut qui vous sont présentées.

Installation et configuration du client de base de données

Si vous avez installé Tivoli Common Reporting sur un ordinateur autre que le serveur de base de données TADDM, vous devez installer un client de base de données pour la connexion à la base de données. Vous pouvez utiliser un client de base de données DB2 ou Oracle, selon le type de la base de données TADDM. Si vous avez installé Tivoli Common Reporting sur le même serveur que la base de données TADDM, il est inutile d'installer un client de base de données.

Procédure

Pour installer et configurer le client de base de données, procédez comme suit :

Exécutez l'une des tâches suivantes :

- Pour utiliser le client de base de données DB2, procédez comme suit :
  1. Installez le client DB2 sur la machine où se trouve TCR, avec les options par défaut présentées.
  2. Vérifiez que la base de données TADDM a été cataloguée. Cette étape est nécessaire pour que Tivoli Common Reporting se connecte au serveur DB2 à l'aide du client DB2.
- Si vous voulez utiliser le client de base de données Oracle, procédez comme suit afin de l'installer et de le configurer à l'aide de l'assistant Oracle Universal Installer et de l'assistant Oracle Net Configuration Assistant :
  1. Dans la page Select Installation Type de l'assistant Oracle Universal Installer, sélectionnez **Administrator** comme mode d'installation.
  2. Dans la page Specify Home Details, indiquez le nom de l'installation et le chemin d'accès à l'emplacement où vous voulez installer le produit.
  3. Dans la page Product-Specific Prerequisite Checks, vérifiez que toutes les exigences d'installation et de configuration sont respectées. Ne poursuivez pas l'installation tant que chaque vérification n'a pas un statut **Succeeded**.
  4. Dans la page Welcome de l'assistant Oracle Net Configuration Assistant, vérifiez que la case **Perform typical configuration** est décochée.

5. Dans la page Naming Methods Configuration, Select Naming Method, prenez **Local Naming** comme méthode de nommage.
6. Dans la page Net Service Name Configuration, Service Name, entrez le nom du service de votre serveur de base de données Oracle distant ; par exemple, `ORCL`.
7. Dans la page Net Service Name Configuration, Select Protocols, sélectionnez **TCP** comme protocole à utiliser pour la connexion à la base de données.
8. Dans la page Net Service Name Configuration, TCP/IP Protocol, entrez le nom d'hôte de l'ordinateur où s'exécute la base de données. Sélectionnez **Use the standard port number of 1521**.
9. Dans la page Net Service Name Configuration, Test, sélectionnez **Yes, perform a test**.

   Si votre nom d'utilisateur et votre mot de passe pour la base de données sont corrects, le texte suivant s'affiche :

   ```
   Connecting... Test successful.
   ```

   Si la connexion à la base de données échoue, vous devez éventuellement modifier vos données d'identification. Pour modifier les donnée d'identification, cliquez sur **Change Login** et entrez un nom d'utilisateur et un mot de passe valides.
10. Dans la page Net Service Name Configuration, Net Service Name, acceptez le nom de service par défaut, qui doit correspondre au nom de service indiqué plus tôt.
11. Créez une variable système Windows nommée `TNS_ADMIN` et définissez la valeur au chemin d'accès complet du dossier contenant le fichier `tnsnames.ora`. Lors de l'installation, le fichier `tnsnames.ora` est créé dans le dossier `%ORACLE_HOME%/client_1/NETWORK/ADMIN`, par exemple `C:/oracle/product/10.2.0/client_1/NETWORK/ADMIN`.
12. Définissez la variable `TNS_ADMIN` dans le script `startTCRserver.sh/bat` pour qu'elle pointe vers l'emplacement du fichier `tnsnames.ora`, par exemple `%ORACLE_HOME%/client_1/NETWORK/ADMIN`.
13. Réamorcez l'ordinateur pour vous assurer que la nouvelle variable système est disponible.

Configuration d'IBM Cognos Framework Manager

Vous devez mettre à jour les propriétés d'IBM Cognos 10 Framework Manager avec les valeurs appropriées.

Pourquoi et quand exécuter cette tâche

Remarque : La procédure suivante concerne la configuration d'IBM Cognos 10 Framework Manager pour Tivoli Common Reporting 3.1. Notez qu'elle est identique pour IBM Cognos 8 Framework Manager pour Tivoli Common Reporting 2.1.

Quand vous installez Tivoli Common Reporting, le programme IBM Cognos Configuration est installé et certaines propriétés sont mises à jour. Quand vous installez IBM Cognos 10 Framework Manager, une autre version du programme IBM Cognos Configuration est installée, mais toutes les propriétés ne sont pas mises à jour. Vous devez copier manuellement certaines valeurs de propriété de la version Tivoli Common Reporting d'IBM Cognos Configuration vers la version IBM Cognos 10 Framework Manager d'IBM Cognos Configuration.

Procédure

Pour configurer IBM Cognos 10 Framework Manager, procédez comme suit :

1. Ouvrez la version d'IBM Cognos Configuration installée par Tivoli Common Reporting. Pour ouvrir ce programme, cliquez sur **Démarrer** > **Programmes** > **Tivoli Common Reporting 3.1** > **IBM Cognos Configuration**.
2. Ouvrez la version d'IBM Cognos Configuration installée par IBM Cognos 10. Pour ouvrir ce programme, cliquez sur **Démarrer** > **Programmes** > **IBM Cognos 10** > **IBM Cognos Configuration**.
3. Pour chaque version d'IBM Cognos Configuration, cliquez sur **Configuration locale** > **Environnement**.
4. Copiez la valeur de la propriété **Gateway URI** de la version de Tivoli Common Reporting d'IBM Cognos Configuration dans la propriété **Gateway URI** de la version IBM Cognos 10 version d'IBM Cognos Configuration. La syntaxe URI est la suivante : `http://tcrhost:16310/tarf/servlet/dispatch`.
5. Copiez la valeur de la propriété **External dispatcher URI** de la version de Tivoli Common Reporting d'IBM Cognos Configuration dans la propriété **Dispatcher URI for external applications** de la version IBM Cognos 10 d'IBM Cognos Configuration. La syntaxe URI est la suivante : `http://tcrhost:16310/tarf/servlet/dispatch`.
6. Enregistrez les modifications dans la version IBM Cognos 10 d'IBM Cognos Configuration.

Génération du modèle TADDM

Fix Pack 1

Vous pouvez générer le modèle TADDM de manière à disposer de l'image instantanée à jour du contenu de la base de données TADDM, y compris les définitions de tous les attributs étendus. Si vous n'utilisez pas d'attributs étendus, vous pouvez ignorer cette procédure et utiliser le fichier de modèle TADDM Cognos préconfiguré, `$COLLATION_HOME/etc/reporting/tcr/model.xml`.

Avant de commencer

Le modèle TADDM généré inclut toutes les classes de modèle de données communes prises en charge par TADDM et les définitions d'attribut étendu stockées dans la base de données TADDM. Vous pouvez publier le modèle TADDM sur le serveur Tivoli Common Reporting et l'utiliser dans des rapports Cognos. Le modèle TADDM peut être généré plusieurs fois. Chaque fois qu'il est régénéré, il intègre le contenu de la base de données TADDM mis à jour.

Notes :

- Si des définitions d'attribut étendu sont supprimées de la base de données TADDM après publication du modèle TADDM sur le serveur Tivoli Common Reporting, les rapports Cognos qui utilisent ces définitions risquent de ne plus fonctionner.
- Sous Windows, modifiez l'extension des scripts utilisés dans la procédure suivante de `.sh` en `.bat`.

Procédure

1. Sur le serveur TADDM, ouvrez le répertoire `$COLLATION_HOME/bin`.
2. Actualisez les vues des attributs étendus en procédant comme suit :

a. Si vous avez créé des vues des attributs étendus, supprimez-les en exécutant la commande suivante :

   ```
   ./extattr_views.sh remove
   ```

b. Générez des scripts SQL avec des définitions de vue d'attribut étendu en exécutant la commande suivante :

   ```
   ./extattr_views.sh scripts
   ```

c. Créez les vues des attributs étendus avec les scripts SQL générés en exécutant la commande suivante :

   ```
   ./extattr_views.sh create
   ```

3. Pour générer le fichier de modèle Cognos, exécutez la commande suivante :

   ```
   ./genCognosModel.sh
   ```

   Le modèle TADDM généré est stocké dans le fichier `model.xml`, qui est placé dans le répertoire ⌂`$COLLATION_HOME/etc/reporting/tcr`. Les messages de journal de la commande se trouvent dans le fichier `$COLLATION_HOME/log/genCognosModel.log`.

Que faire ensuite

Vous pouvez publier le modèle TADDM généré sur le serveur Tivoli Common Reporting à l'aide d'IBM Cognos Framework Manager. Pour plus d'informations, voir «Publication du modèle à l'aide d'IBM Cognos Framework Manager», à la page 173.

Pour plus d'informations sur les vues des attributs étendus, voir la rubrique *Vues des attributs étendus* du *Guide du développeur SDK* de TADDM.

Importation du modèle et des exemples de rapports dans Tivoli Common Reporting

Vous pouvez importer des exemples de rapports TADDM dans Tivoli Common Reporting versions 2.1 et 3.1.

Pourquoi et quand exécuter cette tâche

Cette procédure s'applique à **Tivoli Common Reporting version 2.1**.

Procédure

Pour importer le modèle et les exemples de rapports dans Tivoli Common Reporting 2.1, procédez comme suit :

1. Copiez le module `$COLLATION_HOME/etc/reporting/TADDMPackage.zip` depuis le serveur TADDM vers le dossier `TCRComponent/cognos/deployment` du serveur Tivoli Common Reporting.
2. Ouvrez la page d'accueil de Tivoli Common Reporting.
3. Cliquez sur **Rapport** > **Common Reporting**.
4. Dans le menu **Lancer**, sélectionnez **Administration**. La sous-fenêtre Administration s'ouvre.
5. Cliquez sur l'onglet **Configuration**.
6. Cliquez sur l'icône **Nouvelle importation**. L'assistant Nouvelle importation s'ouvre.
7. Dans la liste de packages disponibles, sélectionnez **TADDMPackage**. Cliquez sur **Suivant**.

8. Facultatif : Dans la zone **Description**, entrez une description du package. Cliquez sur **Suivant**.
9. Cochez la case en regard du nom du package.
10. Dans la section **Options**, cliquez sur **Propriétaire de la source** et sur **Entrées nouvelles et existantes**. Dans le menu de **niveau d'enregistrement**, sélectionnez l'option **de base**. Cliquez sur **Suivant**.
11. Cliquez sur l'option de **sauvegarde et d'exécution unique**. Cliquez sur **Suivant**.

Pourquoi et quand exécuter cette tâche

Cette procédure s'applique à **Tivoli Common Reporting version 3.1**.

Procédure

Pour importer le modèle et les exemples de rapports dans Tivoli Common Reporting 3.1, procédez comme suit :

1. Copiez le module `$COLLATION_HOME/etc/reporting/TADDMPackage.zip` depuis le serveur TADDM vers le dossier `reporting/cognos/deployment` de l'installation de JazzSM.
2. Ouvrez la page d'accueil de Tivoli Common Reporting.
3. Cliquez sur **Rapport** > **Common Reporting**.
4. Dans le menu **Lancer**, sélectionnez **Administration IBM Cognos**. La sous-fenêtre Administration s'ouvre.
5. Cliquez sur l'onglet **Configuration**.
6. Sélectionnez Administration de contenu. Cliquez sur l'icône **Nouvelle importation**. L'assistant Nouvelle importation s'ouvre.
7. Dans la liste de packages disponibles, sélectionnez **TADDMPackage**. Cliquez sur **Suivant**.
8. Facultatif : Dans la zone **Description**, entrez une description du package. Cliquez sur **Suivant**.
9. Cochez la case en regard du nom du package. Cliquez sur **Suivant**.
10. Dans la section **Propriétaire de l'entrée**, cliquez sur **Propriétaire de la source** et sur **Entrées nouvelles et existantes**. Dans le menu de **niveau d'enregistrement**, sélectionnez l'option **de base**. Cliquez sur **Suivant**.
11. Vérifiez que les valeurs sont correctes. Cliquez sur **Suivant**.
12. Cliquez sur l'option de **sauvegarde et d'exécution unique**. Cliquez sur **Terminer**.
13. Cliquez sur **Exécuter**.

Vues de données dans le modèle TADDM

Vous pouvez générer des rapports à partie du fichier de modèle de données TADDM `model.xml`.

Le modèle de données est organisé en plusieurs espaces de nom. Un espace de nom est un conteneur logique dans lequel tous les noms sont uniques. Chaque espace de nom contient des sujets de requête, des éléments de requête et des objets. Les espaces de nom suivants sont présents après que vous ayez importé le fichier TADDM `model.xml` :

Fix Pack 1 **espaces de nom CDM**

Ces vues contiennent les sujets de requête de pratiquement toutes les

classes de modèle de données communes, y compris les classes de reconnaissance, divisés en plusieurs espaces de nom d'après leurs noms de package. Les noms de package sont triés par ordre alphabétique. Les classes de modèle simplifié se distinguent par le préfixe `simple` dans le nom de l'espace de nom. Ces données vous permettent de générer des rapports contenant différents types d'objets CDM.

Les sujets de requête des espaces de nom CDM contiennent des relations prédéfinies liées aux attributs `Parent`. Par exemple, la classe `app.j2ee.J2EEDomain` possède l'attribut `Servers` de type `app.j2ee.J2EEServer[]`. Et la classe `app.j2ee.J2EEServer`, l'attribut `Parent` de type `app.j2ee.J2EEDomain`. Par conséquent, il existe des relations prédéfinies entre toutes les paires de classes CDM compatibles, par exemple :

- `app.j2ee.J2EEDomain [0..1] - [0..n] app.j2ee.J2EEServer`
- `app.j2ee.J2EEDomain [0..1] - [0..n] app.j2ee.jboss.JBossServer`
- `app.j2ee.J2EEDomain [0..1] - [0..n] app.j2ee.weblogic.WebLogicServer`
- `app.j2ee.jboss.JBossDomain [0..1] - [0..n] app.j2ee.jboss.JBossServer`
- `app.j2ee.websphere.WebSphereCell [0..1] - [0..n] app.j2ee.websphere.WebSphereServer`

Dans TADDM 7.3.0.1, certains sujets de requête des espaces de nom CDM sont définis pour des attributs non permanents de type tableau. Dans TADDM 7.3.0.2, les sujets de requête sont définis pour tous les attributs de type tableau. Leurs noms sont au format suivant : "*[nom de la classe qui déclare l'attribut de tableau]-->[nom attribut de tableau]*". Par exemple, la classe `simple.SGroup` possède l'attribut `GroupMembers` du type `ModelObject[]`, de sorte que le sujet de requête est `"SGroup-->GroupMembers"`. Ces sujets de requête contiennent des relations prédéfinies entre les attributs de tableau décrits et toutes les classes CDM contenant ces attributs. Par exemple, pour l'attribut `GroupMembers` indiqué, les relations suivantes sont notamment définies :

- `simple.SGroup [1..1] - [0..n] simple."SGroup-->GroupMembers"`
- `simple.SBaseCollection [1..1] - [0..n] simple."SGroup-->GroupMembers"`
- `app.biztalk.BizTalkGroup [1..1] - [0..n] simple."SGroup-->GroupMembers"`
- `app.hacmp.HACMPResourceGroup [1..1] - [0..n] simple."SGroup-->GroupMembers"`

Pour utiliser des attributs de type tableau, vous devez définir une relation entre un attribut de type tableau et la classe CDM requise à l'aide de son attribut `PK_C` ou, dans le cas d'un attribut non permanent de type tableau (`ModelObject[]`), son attribut `Guid`. Par exemple :

- Fix Pack 2 Pour créer un rapport Cognos qui présente des objets `sys.zOS.ZReportFile` sous forme de `ZReportfiles` des objets `sys.ComputerSystem`, vous devez définir une jointure entre les colonnes suivantes d'IBM Cognos Report Studio :

  ```
  sys."ComputerSystem-->ZReportfiles".PK__ZReportfiles_C
   [0..n]-[0..1] sys.zOS.ZReportFile.PK_C
  ```

- Pour créer un rapport Cognos qui présente des objets app.AppServer sous forme de GroupMembers des objets simple.SBaseCollection, vous devez définir une jointure entre les colonnes suivantes d'IBM Cognos Report Studio :

```
simple."SGroup-->GroupMembers".GroupMembersGuids [0..n]-
[0..1] app.AppServer.Guid
```

Fix Pack 2 Dans bon nombre de cas, il n'est pas nécessaire de créer manuellement des jointures pour les attributs de type tableau car il existe des attributs Parent correspondants des objets dépendants. Le modèle Cognos contient des relations pour ces attributs. Par exemple, vous n'avez pas besoin de créer de jointures manuellement pour créer un rapport présentant des objets sys.FileSystem sous forme de FileSystems des objets sys.ComputerSystem, car les objets sys.FileSystem présentent un attribut Parent qui pointe vers les objets sys.ComputerSystem.

Fix Pack 3 Dans TADDM version 7.3.0.3 et ultérieures, le modèle Cognos contient des éléments de requête du type DataTime pour tous les attributs du type horodatage. Par exemple, le sujet de requête sys.aix.AixUnitaryComputerSystem contient les éléments de requête suivants :

- LastStoredTime du type Int64, qui pointe vers la colonne LASTSTOREDTIME_C dans la vue du bloc de construction. Exemple de valeur dans la colonne : 1445417251307.
- LastStoredTimeT du type Data, qui pointe vers la colonne LASTSTOREDTIME_T dans la vue du bloc de construction. Exemple de valeur dans la colonne : Oct 21, 2015 10:47:31 AM.

L'élément de requête LastStoredTimeT est l'équivalent de l'élément de requêteLastStoredTime seulement s'il est exprimé dans le format Temps Universel Coordonné (TUC) à la place de l'époque UNIX (entier long). Les éléments de requête contenant le suffixe T sont les équivalents d'horodatage de l'attribut d'entier long d'origine.

Espace de nom WebSphere

Remarque : Fix Pack 1 L'espace de nom WebSphere est obsolète dans TADDM versions 7.3.0.1 et ultérieures.
Cette vue contient les principaux sujets de requête relatifs à un environnement WebSphere. Ces données vous permettent de générer des rapports spécifiques de WebSphere, comme la liste de propriétés ou les paramètres de machines virtuelles Java des serveurs WebSphere. Ce sujet de requête Serveur WebSphere est lié au sujet de requête Serveur d'applications contenu dans l'espace de nom partagé. Les objets de requête Cluster WebSphere et Cellule WebSphere sont liés aux objets de requête Cluster de serveurs d'applications et Domaine J2EE contenus dans l'espace de nom partagé.

Espace de nom partagé

Remarque : Fix Pack 1 L'espace de nom partagé est obsolète dans TADDM versions 7.3.0.1 et ultérieures.
Cette vue contient des sujets de requête qui sont considérées comme des classes clé et qui peuvent être utilisés comme un pont joignant les données entre différents espaces de nom. L'espace de nom partagé contient des informations sur les systèmes informatiques et les classes de collection. Ces données vous permettent de créer des rapport d'inventaire.

Espace de nom d'applications métier

Remarque : Fix Pack 1 L'espace de nom d'applications métier est obsolète dans TADDM versions 7.3.0.1 et ultérieures.
Cette vue contient des sujets de requête pour une application métier, à savoir, des sujets de requête `Application` et `Groupe fonctionnel`. L'objet de requête Groupe fonctionnel est lié à l'espace de nom partagé par le biais de l'objet de requête `Collection`. Ces données vous permettent de créer des rapports montrant des applications métier ainsi que leurs membres.

Espace de nom base de données

Remarque : Fix Pack 1 L'espace de nom de base de données est obsolète dans TADDM versions 7.3.0.1 et ultérieures.
Cette vue contient des sujets de requête se rapportant à une base de données et à des serveurs de base de données. Le sujet de requête `Toutes les bases de données` vous permet de générer des rapports de base de données généraux plutôt que des rapports de base de données spécifiques du fournisseur. Le contenu de base de données est lié au nom d'espace partagé par le biais du sujet de requête `Serveurs d'applications`.

Espace de nom Dépendances et relations

Remarque : Fix Pack 1 L'espace de nom de dépendances et relations est obsolète dans TADDM versions 7.3.0.1 et ultérieures.
Cette vue contient des sujets de requête qui représentent des relations et dépendances générées, comme des dépendances IP ou une commutation en relations de périphériques. L'objet de requête à usage général `relationship(unlinked)` vous permet de créer des liens manuels lors de la création d'un rapport ou d'une requête. L'objet de requête `SwitchToDevice` joint des commutateurs à des objets de système informatique dans l'espace de nom partagé. Trois objets de requête sont apparentés à une affinité de serveurs. L'objet de requête `Serveur` montre l'union de tous les systèmes informatiques, des serveurs d'applications et des objets de service au sein de la base de données. L'objet de requête `Affinity (target-linked)` joint chaque relation d'affinité à sa cible dans l'objet de requête `Serveur`. L'objet de requête `Affinity (source-linked)` joint chaque relation d'affinité à sa source dans l'objet de requête `Serveur`. Le contenu du serveur est lié à l'espace de nom partagé par le biais du système informatique, du serveur d'applications et des objets de requête de service. Ces données vous permettent de générer un rapport général montrant les relations entre des éléments de configuration au sein du réseau.

Publication du modèle à l'aide d'IBM Cognos Framework Manager

Si vous voulez ajouter des objets au modèle de données TADDM (fichier `model.xml`), vous devez modifier le fichier, puis le réimporter à l'aide d'IBM Cognos 10 Framework Manager.

Pourquoi et quand exécuter cette tâche

La procédure suivante concerne IBM Cognos 10 Framework Manager. Notez qu'elle est identique pour IBM Cognos 8 Framework Manager.

Procédure

Pour importer le modèle de données à l'aide d'IBM Cognos 10 Framework Manager, procédez comme suit :

1. Démarrez IBM Cognos 10 Framework Manager.
2. Créez un projet.
3. Lorsque vous y êtes invité, entrez les données d'identification pour le serveur Tivoli Common Reporting. Un message peut vous demander d'entrer ces données plusieurs fois.
4. Fermez IBM Cognos 10 Framework Manager.
5. Copiez le fichier suivant du serveur TADDM dans le dossier du projet Cognos Framework :

   ```
   $COLLATION_HOME/etc/reporting/tcr/model.xml
   ```

   Remplacez le fichier `model.xml` existant dans le dossier du projet Cognos Framework.
6. Démarrez IBM Cognos 10 Framework Manager et ouvrez le projet créé plus tôt.
7. Dans la sous-fenêtre de l'afficheur de projet, cliquez sur **Sources de données** > ***nom_source_données_gestionnaire_contenu***.
8. Si vous utilisez une base de données DB2 différente de celle définie dans la source de base de données Cognos, remplacez le contenu du champ **Schéma** par le nom de l'instance DB2 utilisée pour la base de données TADDM.
9. Sauvegardez le projet.
10. Dans la sous-fenêtre d'afficheur de projet, cliquez sur **Packages**.
11. Cliquez avec le bouton droit sur le nom du package et sélectionnez l'option de **publication de packages**. La vérification et la publication du modèle Cognos TADDM peut prendre plusieurs minutes.

Configuration de la source de données dans Tivoli Common Reporting

Vous pouvez utiliser Tivoli Common Reporting pour configurer la source de données.

Avant de commencer

Vérifiez que l'une des situations suivantes se vérifie :

- La base de données TADDM est cataloguée localement.
- Tivoli Common Reporting s'exécute sur le serveur hébergeant la base de données TADDM.

Si vous utilisez une base de données DB2, vérifiez que le nom du schéma correspond au nom de l'instance DB2. Le nom de schéma indique le nom de la base de données DB2 utilisée pour autoriser l'accès à la base de données spécifiée. Vous avez indiqué le nom de l'instance DB2 à l'installation de TADDM. Le nom d'instance par défaut indiqué dans le fichier `model.xml` de TADDM est `DB2INST1`. Si nécessaire, changez le nom du schéma.

Si vous utilisez une base de données Oracle, vérifiez que le nom du schéma est blanc.

Procédure

Pour configurer la source de données à l'aide de Tivoli Common Reporting, procédez comme suit :

1. Ouvrez la page d'accueil de Tivoli Common Reporting.
2. Cliquez sur **Rapport** > **Common Reporting**.
3. Dans le menu **Lancer**, selon la version de Tivoli Common Reporting que vous utilisez, sélectionnez l'une des options suivantes du menu :
   - Version 2.1 - **Administration**.
   - Version 3.1 - **Administration IBM Cognos**.

   La sous-fenêtre Administration s'ouvre.
4. Cliquez sur l'onglet **Configuration**.
5. Cliquez sur l'icône **Nouvelle source de données**. L'assistant Nouvelle source de données s'affiche.
6. Dans la zone **Nom**, entrez `CMDBTCR`. Le nom `CMDBTCR` est référencé dans le modèle de données ; vous devez donc attribuer le même à la nouvelle source de données.
7. Dans le menu **Type**, sélectionnez le type de base de données utilisé.
8. Exécutez l'une des étapes suivantes :
   - Si votre type de base de données est DB2, dans la zone **Nom de la base de données DB2**, entrez le nom de la base de données TADDM ou l'alias de la base de données TADDM cataloguée.
   - Si votre type de base de données est Oracle, dans la zone de **chaîne de connexion SQL*Net**, entrez le nom du service de le base de données Oracle ; par exemple, `ORCL`. Vous avez indiquer le nom du service de la base de données Oracle lors de la configuration du client de la base de données Oracle. Vous pouvez vérifier le nom du service de la base de données Oracle dans le fichier `%TNS_ADMIN%/tnsnames.ora`. Recherchez la chaîne suivante :

     ```
     SERVICE_NAME =
     ```
9. Dans la section de **connexion**, entrez le nom et le mot de passe d'utilisateur de la base de données.
10. Pour tester la connexion à la base de données, cliquez sur **Tester**. Dans la page d'affichage des résultats de l'assistant Nouvelle source de données, le statut du test apparaît.

Importation du module de rapports TADDM dans Tivoli Common Reporting

Pour importer les rapports TADDM prédéfinis dans Tivoli Common Reporting, vous pouvez importer le module de rapports TADDM.

Avant de commencer

Vous devez commencer par installer la fonction Tivoli Common Reporting sur votre système. Tivoli Common Reporting est fourni avec certains produits Tivoli mais n'est pas inclus actuellement dans TADDM.

Pourquoi et quand exécuter cette tâche

Un *module de rapports* Tivoli Common Reporting est un fichier .zip contenant une ou plusieurs conceptions de rapports ainsi que leurs ressources nécessaires, dans

un format utilisable par Tivoli Common Reporting. Les rapports BIRT prédéfinis pour TADDM sont fournis sous forme de module de rapports que vous pouvez importer dans Tivoli Common Reporting.

Pour certains rapports BIRT, il existe différentes versions du même rapport disponibles selon le serveur sur lequel le rapport est exécuté, par exemple, le rapport TADDM_SNAPSHOT_CHANGE sur le serveur de domaine ou le serveur de stockage et le rapport TADDM_SNAPSHOT_SYNC_CHANGE sur le serveur de synchronisation. D'une manière générale, seule la version appropriée d'un rapport est accessible, lais après l'l'importation de rapports BIRT dans Tivoli Common Reporting, les deux versions d'un rapport pourraient être disponibles. Vérifiez que vous n'utilisez que la version du rapport qui convient au serveur sur lequel vous voulez exécuter le rapport.

Après l'importation de rapports BIRT dans Tivoli Common Reporting, certains rapports portant l'intitulé «Drill-through only» dans le nom du rapport pourraient être disponibles. Ces rapports sont destinés à être exécutés au moyen d'une exploration en aval via les données sélectionnées dans un autre rapport et vous ne devez pas les exécuter séparément.

Le rapport Affinité de serveur par portée ne peut pas être importé dans Tivoli Common Reporting.

Pour plus d'informations sur l'importation des modules de rapports, reportez-vous à la documentation de Tivoli Common Reporting.

Procédure

Pour importer les rapports TADDM, procédez comme suit :

1. Si vous utilisez Tivoli Common Reporting 1.3, procédez comme suit :
   a. Dans la fenêtre de navigation du rapport Tivoli Common Reporting, accédez à l'onglet **Navigation**.
   b. Cliquez avec le bouton droit de la souris sur le noeud racine de l'arborescence de navigation (Ensembles de rapports).
   c. Cliquez sur **Import Report Package** (Importer le package de rapports).
   d. Dans la fenêtre d'importation des packages de rapports, indiquez l'emplacement du fichier du package de rapports `TADDMReports.zip`. Ce fichier se trouve dans le répertoire `$COLLATION_HOME/etc/Reporting`.
   e. Développez **Advanced Options** (Options avancées), et procédez comme suit :
      1) Sélectionnez la case à cocher **Overwrite** (écraser). Cela garantit que toutes les copies de rapports précédemment installées sont écrasées.
      2) Dans la zone **Security Set**, entrez le nom de l'ensemble de sécurité dans lequel vous souhaitez importer le contenu du package de rapports.
   f. Cliquez sur **Importer**. Le package de rapports TADDM est importé dans le magasin de données Tivoli Common Reporting.
2. Si vous utilisez Tivoli Common Reporting 2.1, procédez comme suit :
   a. Ouvrez une ligne de commande et accédez au `TIP_install_dir/tipv2Components/TCRComponent/bin`.
   b. Exécutez la commande d'importation :

      ```
      trcmd -user ID_utilisateur -password mot_de_passe -import -bulk pkgFile
      ```

où *pkgFile* est le chemin d'accès au fichier package de rapports `taddmreports.zip` copié sur le serveur Tivoli Common Reporting à partir de `$COLLATION_HOME/etc/Reporting` sur le serveur TADDM.

c. Le package de rapports TADDM est importé dans le magasin de données Tivoli Common Reporting.

3. Si vous utilisez Tivoli Common Reporting 3.1, procédez comme suit :
   a. Ouvrez une invite de commande et accédez au fichier `rép_install_JazzSM/reporting/bin`.
   b. Exécutez la commande d'importation :

      ```
      trcmd -user ID_utilisateur -password mot_de_passe -import -bulk pkgFile
      ```

      où *pkgFile* est le chemin d'accès au fichier package de rapports `taddmreports.zip` copié sur le serveur Tivoli Common Reporting à partir de `$COLLATION_HOME/etc/Reporting` sur le serveur TADDM.
   c. Le package de rapports TADDM est importé dans le magasin de données Tivoli Common Reporting.

Que faire ensuite

Après avoir importé les rapports TADDM, vous devez reconfigurer la source de données JDBC pour chaque rapport.

Configuration de rapports TADDM BIRT dans Tivoli Common Reporting

Après avoir importé les rapports TADDM dans Tivoli Common Reporting, vous devez configurer les sources de données JDBC utilisées par chaque rapport.

Avant de commencer

Avant de configurer l'accès JDBC, vérifiez que les fichiers du pilote JDBC appropriés sont installés dans le répertoire des pilotes Tivoli Common Reporting. Pour Tivoli Common Reporting 1.3, ces fichiers résident dans le répertoire suivant :

```
rép_install_tcr/products/tcr/lib/birt-runtime-2_2_1/ReportEngine/plugins/
  org.eclipse.birt.report.data.oda.jdbc_2.2.1.r22x_v20070919/drivers
```

Pour Tivoli Common Reporting 2.1, ces fichiers résident dans le répertoire suivant :

```
rép_install_tip/tip21Components/TCRComponent/lib/birt-runtime-2_2_2/ReportEngine/plugins/
org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/drivers
```

Pour Tivoli Common Reporting 3.1, ces fichiers résident dans le répertoire suivant :

```
rép_install_JazzSM/reporting/lib/birt-runtime-2_2_2/ReportEngine/plugins/
org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/drivers
```

Si vous utilisez une base de données Oracle, vérifiez que le répertoire contient `ojdbc14.jar` ou `ojdbc5.jar`.

Pourquoi et quand exécuter cette tâche

Les rapports importés sont initialement configurés pour utiliser une source de données par défaut. Vous devez modifier les propriétés de source de données pour chaque rapport TADDM afin d'utiliser la base de données dans laquelle les données de reconnaissance sont stockées. Les rapports TADDM n'utilisent pas une source de données partagées. Par conséquent, vous devez effectuer les opérations suivantes pour configurer les propriétés de source de données de l'ensemble des rapports TADDM.

Procédure

Pour configurer des sources de données JDBC pour Tivoli Common Reporting, procédez comme suit :

1. Si vous utilisez Tivoli Common Reporting 1.3, procédez comme suit :
   a. Dans le tableau **Rapports** Tivoli Common Reporting, cliquez avec le bouton droit de la souris sur le rapport TADDM à configurer.
   b. Dans le menu en incrustation, cliquez sur **Sources de données**.
   c. Dans la fenêtre **Report Data Sources** (sources de données de rapport), entrez les informations de pilote JDBC, d'adresse URL, d'ID utilisateur et de mot de passe. Vous pouvez trouver les valeurs correctes de ces paramètres dans le fichier `collation.properties` du répertoire `$COLLATION_HOME/etc` .
   d. Répétez les étapes précédentes pour chacun des rapports TADDM à configurer.
2. Si vous utilisez Tivoli Common Reporting 2.1 ou 3.1, procédez comme suit :
   a. Ouvrez une invite de commande et accédez `rép_install_tip/tip21Components/TCRComponent/bin` pour Tivoli Common Reporting 2.1, ou `rép_install_JazzSM/reporting/bin` pour Tivoli Common Reporting 3.1.
   b. Pour configurer toutes les sources JDBC pour l'ensemble des rapports, exécutez la commande **`modify`** sur une ligne :

      Important : Les commandes suivantes incluent le nom du répertoire contenant les rapports BIRT, `'IBM Tivoli Products'`. Ce nom s'applique à TADDM version 7.3.0.1, ou ultérieure. Si vous utilisez TADDM 7.3.0, remplacez-le par `'Tivoli Products'`.

      ```
      trcmd -user userID -password password -modify
      -datasources -reports -reportname "/content/package[@name='IBM Tivoli
      Products']/folder[@name='TADDM Reports']//report" -setdatasource
      odaDriverClass=driverClass odaURL=jdbcUrl
      odaUser=dbUser odaPassword=dbPassword
      ```

      Par exemple, si vous utilisez une base de données DB2, entrez la commande suivante sur une ligne :

      ```
      trcmd -user tipadmin -password tipadmin -modify -datasources -reports
      -reportname "/content/package[@name='IBM Tivoli Products']/folder[@name=
      'TADDM Reports']//report" -setdatasource
      odaDriverClass=com.ibm.db2.jcc.DB2Driver
      odaURL=jdbc:db2://100.101.102.103:50000/SAMPLEDB
      odaUser=db2inst1 odaPassword=db2inst1
      ```

      Par exemple, si vous utilisez une base de données Oracle, entrez la commande suivante sur une ligne :

      ```
      trcmd -user tipadmin -password tipadmin -modify -datasources -reports
      -reportname "/content/package[@name='IBM Tivoli Products']/folder[@name=
      'TADDM Reports']//report" -setdatasource
      odaDriverClass=oracle.jdbc.driver.OracleDriver
      odaURL=jdbc:oracle:thin:@192.168.0.1:1521:orcl
      odaUser=taddm_dev odaPassword=taddm_dev
      ```

Vérification des rapports TADDM

Vous pouvez vérifier que les rapports TADDM s'affichent correctement dans Tivoli Common Reporting.

Procédure

Pour vérifier que les rapports TADDM s'affichent correctement dans Tivoli Common Reporting, procédez comme suit :

1. Ouvrez la page d'accueil de Tivoli Common Reporting.
2. Cliquez sur **Rapport** > **Common Reporting**.
3. Vérifiez que les dossiers **TADDM** et **Tivoli Products** sont visibles.
4. Cliquez sur **TADDM**.
5. Cliquez sur l'icône **Exécuter** pour exécuter l'un des rapports. Le rapport s'affiche.
6. Vérifiez que le rapport s'affiche correctement et en entier.
7. A l'aide du trajet de navigation, revenez à **Dossiers publics**.
8. Cliquez sur **Produits Tivoli** > **Rapports TADDM**. Cliquez sur l'icône **Exécuter** pour exécuter l'un des rapports. Le rapport s'affiche.
9. Vérifiez que le rapport s'affiche correctement et en entier.

Génération de rapports avec BIRT

Vous pouvez utiliser la fonction de génération de rapports BIRT (Business Intelligence and Reporting Tools) pour produire des rapports prédéfinis et personnalisés à partir des données de la base de données TADDM.

Présentation des rapports BIRT

Outre les rapports intégrés disponibles à partir du portail de gestion de données, vous pouvez également concevoir, développer et installer des rapports basés sur le système open source BIRT (Business Intelligence and Reporting Tools).

Important : La visualisation des rapports BIRT dans le visualiseur de rapports du portail de gestion de données (moteur d'exécution BIRT) étant peu sûre, cette fonctionnalité est désactivée. Il est préférable d'afficher les rapports BIRT avec Tivoli Common Reporting après y avoir importé les rapports de TADDM.

Si vous êtes avisé des risques, vous pouvez restaurer le visualiseur de rapports BIRT et l'utiliser comme indiqué dans les paragraphes suivants.

TADDM inclut le moteur d'exécution à source ouverte BIRT en tant que composant intégré. De plus, TADDM comprend également des centaines de vues de base de données et rapports prédéfinis. En plus des rapports prédéfinis, vous pouvez également utiliser le concepteur BIRT pour créer des rapports à utiliser avec le moteur d'exécution TADDM BIRT. Ces rapports peuvent utiliser des sources de données JDBC qui extraient les données à l'aide de vues de bases de données prédéfinies.

L'interface du portail de gestion de données fournit les moyens de gérer ces rapports BIRT. Vous pouvez ajouter de nouveaux rapports, télécharger des rapports sélectionnés, supprimer des rapports que vous avez téléchargés ou exécuter un rapport. Les rapports prédéfinis sont également mis en forme pour pouvoir être utilisés avec l'outil Tivoli Common Reporting.

Business Intelligence and Reporting Tools

Business Intelligence and Reporting Tools (BIRT) est un système à source ouverte basé sur Eclipse permettant de concevoir, développer et exécuter des rapports.

Vous pouvez développer des rapports BIRT pour TADDM, les concevoir pour utiliser des sources de données JDBC et des requêtes SQL de vues de base de données prédéfinis.

Important : Les rapports BIRT ne doivent pas utiliser les données provenant directement des tables de base de données TADDM. Pour cette raison, vous devez toujours concevoir vos rapports de manière à utiliser une source de données JDBC et les vues de la base de données TADDM qui sont décrites dans le *Guide du développeur SDK* de TADDM.

Le système BIRT inclut deux principaux composants :

- Le concepteur BIRT, un outil graphique permettant de concevoir et de développer de nouveaux rapports.
- Le moteur d'exécution BIRT, qui fournit le support pour l'exécution de rapports et du rendu des rapports publiés.

TADDM comprend le moteur d'exécution BIRT, que vous pouvez utiliser pour exécuter les rapports prédéfinis. Pour créer vos propres rapports BIRT, vous devez télécharger le concepteur BIRT qui correspond à la version du moteur d'exécution BIRT inclut dans TADDM (actuellement la version 2.2.1).

Pour plus d'informations sur le projet BIRT, notamment comment télécharger le concepteur BIRT, voir http://www.eclipse.org/birt.

Tâches associées:

«Restauration du visualiseur de rapports BIRT», à la page 196
Si vous êtes avisé des risques liés à la sécurité mais que vous souhaitez néanmoins utiliser le visualiseur de rapports BIRT, vous pouvez le restaurer.

Rapports BIRT prédéfinis

Les rapports BIRT prédéfinis inclus dans TADDM fournissent des informations sur les systèmes reconnus, les systèmes d'exploitation et les processus serveur.

Rapport d'inventaire AppServer :

Le rapport d'inventaire AppServer inclut tous les serveurs d'applications reconnus par TADDM. Lorsque vous exécutez le rapport, vous pouvez indiquer une valeur de paramètre limitant le rapport aux serveurs d'applications d'un type spécifique. Le rapport regroupe les serveurs d'applications reconnus selon le système, et les répertorie en fonction du nom de système hôte qualifié complet.

Les données de ce rapport proviennent de la vue de base de données CM_APP_SERVERS_PER_HOST_V.

Rapport d'inventaire de système informatique :

Le rapport d'inventaire du système informatique inclut tous les systèmes informatiques de la base de données TADDM auxquels ont été affectés des adresses IP, et les répertorie en fonction du nom de système hôte qualifié complet. Ce rapport ne contient pas de paramètres.

Ce rapport est conçu pour être exporté dans un fichier séparé par des virgules qui peut être importé dans une application de tableur. Si un système ne possède pas d'adresse IP, il n'est pas inclus dans le rapport. Le même nom de système informatique peut être répertorié plusieurs fois dans le rapport, une fois pour chaque adresse IP unique (y compris l'adresse de bouclage 127.0.0.1).

Les données de ce rapport proviennent de la vue de base de données CM_COMPUTER_SYSTEMS_V.

Rapport d'inventaire de système informatique par type de système d'exploitation :

Le rapport d'inventaire du système informatique par type de système d'exploitation inclut tous les systèmes informatiques reconnus dont les systèmes d'exploitation ont également été reconnus. Ce rapport ne contient pas de paramètres.

Ce rapport est conçu pour être exporté dans un fichier séparé par des virgules qui peut être importé dans une application de tableur. Le même nom de système informatique peut être répertorié plusieurs fois dans le rapport, une fois pour chaque adresse IP unique (y compris l'adresse de bouclage 127.0.0.1). Pour être inclus dans ce rapport, un système d'exploitation doit être associé à un système dans la base de données TADDM. De même, tout système pour lequel un système d'exploitation n'est pas défini dans la base de données TADDM n'est pas inclus.

Cliquez sur le nom d'un système dans le rapport pour ouvrir un rapport d'informations d'inventaire détaillées pou ce système.

Les données de ce rapport proviennent des vues de base de données suivantes :
- DP_UNITARY_COMP_GENERAL_V
- DP_UNITARY_COMP_OS_V
- DP_UNITARY_COMP_IP_INTERFACE_V
- BB_OPERATINGSYSTEM62_V

Rapport ITNM IP :

Fournit des informations sur les instances installées du produit Network Manager et répertorie toutes les ressources Network Manager ayant une relation au système informatique.

Le rapport Network Manager Inventory est disponible dans la console du gestionnaire de domaine TADDM. Il comporte les sections suivantes :

Récapitulatif des serveurs
Fournit des informations sur les instances installées du produit Network Manager, dont les versions installées de Network Manager, les adresses hôte des serveurs où Network Manager est installé et les URL pour accéder à l'interface graphique de Network Manager.

Récapitulatif des ressources
Répertorie toutes les ressources Network Manager ayant une relation avec un système informatique, dont l'adresse IP, le fabricant, le type de ressource (par exemple, un routeur) et l'identificateur unique dans la base de données Network Manager.

Rapport concis d'inventaire du système informatique :

Ce rapport permet d'afficher les adresses IP reconnues à l'aide d'un profil de reconnaissance de niveau 1. Pour chaque adresse IP, le rapport indique le nom du système informatique associé, ainsi que le nom du système d'exploitation ou du logiciel de contrôle (si cette information a été reconnue).

Bien que le rapport concis d'inventaire du système informatique soit destiné à être utilisé après une reconnaissance de niveau 1, vous pouvez également l'utiliser après une reconnaissance de niveau 3. Cependant, d'autres rapports tels que le rapport d'inventaire du système informatique fournissent des informations plus détaillées après une reconnaissance avec autorisations d'accès.

Rapport de réseau canal optique :

Le rapport de réseau canal optique affiche des connexions canal optique entre un commutateur canal optique et d'autres systèmes informatiques.

Pour exécuter le rapport, indiquez le nom WWN du commutateur canal optique pour afficher les connexions canal optique entre ce commutateur et d'autres systèmes informatiques. Dans la fenêtre Paramètre, entrez le nom WWN ou sélectionnez-le dans la liste déroulante des commutateur fibre optique reconnus.

Les informations suivantes sont affichées dans le rapport pour chaque système informatique connecté :

- Système informatique (nom affiché ; WWN dans le cas de commutateur canal optique)
- Fabricant
- Modèle
- Numéro de série

Vous pouvez cliquer sur un nom affiché de système informatique due rapport pour ouvrir un autre rapport réseau canal optique. Ce rapport affiche les connexions canal optique entre le système informatique sélectionné et d'autres systèmes informatiques.

Rapport d'inventaire d'adaptateur de bus hôte :

Le rapport d'inventaire d'adaptateur de bus hôte affiche la liste de tous les adaptateurs de bus hôte ainsi que des systèmes informatiques sur lesquels ils sont installés.

Pour chaque adaptateur de bus hôte reconnu, les informations suivantes sont affichées dans le rapport :

Nom de l'adaptateur de bus hôte
Le nom de l'adaptateur de bus hôte.

Nom de domaine complet
Le nom de domaine complet du système informatique sur lequel l'adaptateur de bus hôte est installé.

Hôte utilisant des modules de stockage
Une valeur booléenne indiquant si le système informatique qui héberge utilise des volumes de stockage situés dans un système de stockage.

Récapitulatif de l'inventaire :

Le récapitulatif d'inventaire comprend un graphique circulaire des systèmes d'exploitation installés sur les systèmes informatiques reconnus, en fonction des portées reconnues par TADDM. Chaque segment du graphique représente un type de système d'exploitation et indique le nombre total de serveurs reconnus exécutant ce système d'exploitation. Ce rapport ne contient pas de paramètres.

Cliquez sur un segment du diagramme pour ouvrir un rapport d'inventaire de système informatique pour le type de système d'exploitation sélectionné.

Les données de ce rapport proviennent de la vue de base de données BB_OPERATINGSYSTEM62_V.

Rapports sur la portée de la surveillance :

Les rapports sur la portée de la surveillance présentent en détail les différents composants de votre environnement. Vous pouvez générer un rapport pour des systèmes d'exploitation, des bases de données, des applications Microsoft, des serveurs VMware et des composants System p dans votre environnement. Ces composants sont surveillés par des agents IBM Tivoli Monitoring 6.1 ou ultérieurs. Vous pouvez exécuter ce rapport à partir du panneau Rapports BIRT du portail de gestion de données.

Le tableau 37, à la page 184 répertorie les rapports de portée disponibles. Le rapport sur la portée de la surveillance pour les systèmes d'exploitation peut être alimenté par le détecteur IBM Tivoli Monitoring Scope. Les autres rapports ont en revanche besoin de l'adaptateur de bibliothèque de reconnaissance (DLA) IBM Tivoli Monitoring pour renseigner les rapports.

Les rapports comptent trois sections :

Portée par type

Cette section montre le nombre d'instances surveillées, non surveillées et totales regroupées par type de rapport. La fenêtre Détails de la couverture offre une représentation graphique des statistiques suivantes :

- Portée globale
- Portée par plateforme

Détails de la couverture

Cette section montre le nom de domaine complet, le nom de système géré et l'état de surveillance, regroupés par type de rapport. L'état de surveillance est répertorié, ainsi que les informations relatives à la version de l'agent, si surveillé. Cliquez sur le nom du système surveillé (MSN) d'un système surveillé pour ouvrir la fenêtre Détails de l'agent.

Détails de l'agent

Cette section affiche des informations détaillées sur l'agent et le système d'exploitation sur lequel il est exécuté. Les informations affichées dépendent si l'agent est surveillé ou non. Les informations d'affinité et de jeton source sont incluses avec un lien de lancement en contexte de la vue Tivoli Enterprise Portal d'IBM Tivoli Monitoring.

La section Système logiciel de gestion fournit l'inventaire des agents IBM Tivoli Monitoring installés et un lien de lancement en contexte vers les espaces de travail d'IBM Tivoli Monitoring. Le récapitulatif de la portée de la surveillance fournit la liste des systèmes surveillés et non surveillés, que vous pouvez utiliser pour surveiller et gérer les agents de surveillance.

Une reconnaissance de niveau 1 peut utiliser le détecteur IBM Tivoli Monitoring Scope pour renseigner le rapport sur la portée de la surveillance pour les systèmes d'exploitation. Les autres rapports doivent être renseignés par l'adaptateur de

bibliothèque de reconnaissance (DLA) IBM Tivoli Monitoring. Voir le *Guide d'administration* de TADDM pour plus d'informations sur le DLA IBM Tivoli Monitoring.

Le tableau 37 répertorie les rapports de portée disponibles.

Tableau 37. Rapports sur la portée de la surveillance

Nom du rapport	Description
Portée de la surveillance pour les systèmes d'exploitation	Ce rapport fournit des détails pour le système d'exploitation dans votre environnement.
Portée de la surveillance pour les bases de données	Ce rapport fournit des détails sur l'instance DB2 et le serveur SQL dans votre environnement.
Portée de la surveillance pour les applications Microsoft	Ce rapport fournit des détails sur le rôle activé Active Directory, Cluster Server, Exchange Server, Host Integration Server et Hyper-V Server, ainsi que sur le serveur Internet Information Services.
Portée de la surveillance pour VMware	Ce rapport fournit des détails sur les serveurs VMware ESX et les serveurs VMware Virtual Center.
Portée de la surveillance pour System p	Ce rapport fournit des détails sur les partitions logiques de System p, de la console de gestion du matériel, de Virtual I/O Server et d'AIX.

Rapports de détecteurs :

Les rapports de détecteur réunissent les informations collectées sur des unités de mesure des détecteurs.

Le tableau 38 répertorie les rapports disponibles des détecteurs prédéfinis.

Tableau 38. Rapports de détecteurs prédéfinis

Nom du rapport	Description
TADDM_SENSORS_WEEKLY_METRICS_ALL TADDM_SENSORS_WEEKLY_METRICS	Ce rapport indique le taux de pourcentage réussite hebdomadaire pour des détecteurs activés dans un profil de reconnaissance de niveau 1, un profil de reconnaissance de niveau 2 ou un profil de reconnaissance de niveau 3. Les informations suivantes sont affichées : • Date • % de réussite au niveau 1 (N1) • % de réussite au niveau 2 (N2) • % de réussite au niveau 3 (N3) • % de réussite aux N1 et N2 • Tous les % de réussite Le deuxième rapport «TADDM_SENSORS_WEEKLY_METRICS» contient les mêmes informations, mais présente les informations sous la forme d'un diagramme à barres.

Tableau 38. Rapports de détecteurs prédéfinis (suite)

Nom du rapport	Description
TADDM_SENSORS_SUMMARY_TOTAL TADDM_SENSORS_SUMMARY	Ce rapport affiche le nombre total de détecteurs qui se sont correctement exécutés et bien terminés. Les informations suivantes sont affichées : • Niveau • Exécutions avec EC stockés • Réussites • Echecs En outre, l'affichage présente un récapitulatif présentant les niveaux de profil de reconnaissance et les taux globaux de pourcentage de réussite et d'échec pour chaque niveau. Le rapport «TADDM_SENSORS_SUMMARY» présente le pourcentage du taux de réussite ou d'échec pour chacun des détecteurs lors d'une reconnaissance. Les informations suivantes sont affichées : • Niveau • Détecteur • Exécutions • Réussites • Echecs • % de réussite • % d'échec
TADDM_SENSORS_SERVER_SCANS_IP	Ce rapport indique le statut après l'analyse d'un serveur en spécifiant l'adresse IP. Les informations suivantes sont affichées : • Semaine • Statut Le début du rapport affiche des informations récapitulatives sur l'adresse IP, le nom d'hôte, le nom de domaine complet, la date et le statut de la première analyse, la date et le statut de la dernière analyse.
TADDM_SENSORS_SERVER_SCANS_ HOSTNAME	Ce rapport indique le statut après l'analyse d'un serveur en spécifiant le nom d'hôte. Les informations suivantes sont affichées : • Semaine • Statut Le début du rapport affiche des informations récapitulatives sur le nom d'hôte, l'adresse IP, le nom de domaine complet, la date et le statut de la première analyse, la date et le statut de la dernière analyse.
TADDM_SENSORS_MONTHLY_COVERAGE	Ce rapport affiche un diagramme à barres montrant la portée mensuelle du détecteur de session. Il inclut des informations sur le nombre d'analyses exécutées ainsi que sur le nombre d'analyses ayant ou non réussi. Le détecteur de session crée une session entre le serveur TADDM et le système informatique cible.

Tableau 38. Rapports de détecteurs prédéfinis (suite)

Nom du rapport	Description
TADDM_SENSORS_METRICS_LEVEL_1_ AND_2 TADDM_SENSORS METRICS_LEVEL3	Ce rapport affiche un diagramme à barres présentant pour une semaine donnée, le pourcentage du taux de réussite de chacun des détecteurs lors de l'exécution d'une reconnaissance de niveau 1 et de niveau 2. Le diagramme à barres associé au rapport «TADDM_SENSORS_METRICS_LEVEL3» affiche les unités de mesure pour chacun des détecteurs lors de l'exécution d'une reconnaissance de niveau 3.
TADDM_SENSORS_FAILED_LEVELS_1_2_3 TADDM_SENSORS_FAILED_LEVEL	Ce rapport affiche un diagramme circulaire pour une semaine donnée, basé sur les échecs lors de l'exécution d'une reconnaissance de niveau 1, niveau 2 ou de niveau 3. Chaque segment du graphique représente des problèmes de sessions, des problèmes avec des détecteurs, des problèmes de connexion et d'autres problèmes. Le diagramme circulaire du rapport «TADDM_SENSORS_FAILED_LEVEL» présente les unités de mesure pour un niveau de reconnaissance donné.
TADDM_SENSORS_EVENTS_SENSOR_IP TADDM_SENSORS_EVENTS_SENSOR TADDM_SENSORS_EVENTS_IP TADDM_SENSORS_DONE_EVENTS_RUN	Ce rapport affiche les données des événements pour un détecteur et une adresse IP donnés. Les informations suivantes sont affichées : • Date • Détails du détecteur • Gravité • Description Le rapport «TADDM_SENSORS_EVENTS_SENSOR» contient les mêmes informations, mais affiche les données d'événements d'un détecteur donné. Le rapport «TADDM_SENSORS_EVENTS_IP» contient les mêmes informations, mais affiche les données d'événements pour une adresse IP donnée. Le rapport «TADDM_SENSORS_DONE_EVENTS_RUN» contient les mêmes informations, mais affiche les données d'événements pour une exécution de reconnaissance spécifiée.

Affinité de serveur par portée :

Le rapport Affinité de serveur par portée indique les relations entre serveurs, classées selon la source et la cible de chaque relation. Le premier tableau affiche tous les serveurs compris dans la portée spécifiée qui sont des sources de relation. Il affiche également les connexions partant de ces serveurs vers d'autres serveurs. Le deuxième tableau affiche tous les serveurs compris dans la page spécifiée qui sont des cibles de relations, et les connexions à ces serveurs depuis d'autres serveurs.

Le rapport Affinité de serveur par portée n'est accessible que dans des déploiements de serveurs de domaine.

Pour afficher un graphique montrant les communications serveur-à-serveur, cliquez sur **Lancer le graphique d'affinité**. Le graphique montre des dépendances transactionnelles et de service entre les systèmes informatiques, avec des

dépendances indiquées par des liens tirés entre les systèmes. Le graphique inclut tous les liens de dépendance qui comportent au moins un système à l'intérieur de la portée de la reconnaissance, avec des systèmes qui sont des membres de la portée mise en évidence en jaune.

Les liens qui apparaissent dans le graphique d'affinité peuvent représenter des relations transactionnelles ou de service. Le sens d'un lien indique quel système est la source et lequel est la cible de la relation de dépendance. Les objets source et cible peuvent être de plusieurs types, selon la relation :

- Système informatique
- Serveur d'applications
- Service

Les liens sur le graphique sont toujours dessinés entre des systèmes informatiques. Pour une relation impliquant un serveur d'applications ou un service, le lien se connecte au système de l'ordinateur hôte. Pour plus d'informations sur une relation de dépendance (y compris la source, la cible, le nom de la commande et le numéro de port impliqué), déplacez le pointeur de la souris sur le lien dans le diagramme.

Le rapport Affinité de serveur par portée ne peut pas être importé dans Tivoli Common Reporting.

Rapports instantanés :

Les rapports instantanés prédéfinis assemblent les informations capturées par un ou plusieurs instantanés.

Un instantané est une copie des informations sur l'ordinateur reconnu prises à instant spécifique. Pour plus d'informations sur la création d'instantanés, voir «Utilisation de l'outil d'image instantanée», à la page 196.

Le nom du rapport spécifique dépend le serveur sur lequel vous exécutez et visualisez des rapports BIRT. Si vous utilisez le portail de gestion de données sur le serveur de domaine ou le serveur de stockage, exécutez le rapport standard, par exemple, TADDM_SNAPSHOT_CHANGE. Si vous utilisez le portail de gestion de données sur le serveur de synchronisation, exécutez le rapport avec "SYNC" dans le nom, par exemple, TADDM_SNAPSHOT_SYNC_CHANGE. Les rapports suivants sont des exceptions et ont le même nom pour tous les serveurs:

- TADDM_SNAPSHOT_FRAME
- TADDM_SNAPSHOT_HOST

Lorsque vous importez un rapport BIRT dans Tivoli Common Reporting, un nom de rapport modifiée s'affiche, par exemple, le rapport TADDM_SNAPSHOT_SYNC_SESSION_FAILED s'affiche en tant que «TADDM : Détails sur les sessions ayant échoué (Entreprise)».

Le tableau 39, à la page 188 énumère les rapports instantanés prédéfinis disponibles.

Tableau 39. Rapports instantanés prédéfinis

Nom du rapport	Description
TADDM_SNAPSHOT_FRAME	Affiche les informations détaillées suivantes sur les serveurs reconnus : • nom de trame • numéro de série • fabricant • modèle • type d'UC • Vitesse de l'UC • nombre d'UC • mémoire • emplacement • zone de prise en charge • date de la dernière reconnaissance
TADDM_SNAPSHOT_HOST	Affiche les informations détaillées suivantes sur les serveurs physiques et virtuels : • nom de trame • nom du système • adresse IP • type de système d'exploitation • type d'hôte • nom du système géré • date de la dernière reconnaissance
TADDM_SNAPSHOT_SESSION_FAILED TADDM_SNAPSHOT_SYNC_SESSION _FAILED	Affiche les informations relatives au nom et à l'adresse IP des serveurs reconnus pour lesquels TADDM n'est pas parvenu à obtenir des informations de niveau 2 à cause de sessions échouées.
TADDM_SNAPSHOT_CHANGE TADDM_SNAPSHOT_SYNC_CHANGE	Compare deux instantanée pris à différents moments. Pour chaque serveur ajouté ou supprimé dans l'intervalle de temps entre la prise des deux instantanés, les informations suivantes sont affichées : • nom • adresse IP • virtual Des informations s'affichent également sur la modification du rapport serveurs physiques/serveurs virtuels pendant la durée comprise les deux instantanés.
TADDM_SNAPSHOT_DISCOVERY_ERROR TADDM_SNAPSHOT_SYNC _DISCOVERY_ERROR	Affiche des informations sur les erreurs générées pendant des reconnaissances.
TADDM_SNAPSHOT_FQDN_OS _CHANGES TADDM_SNAPSHOT_SYNC_FQDN _OS_CHANGES	Affiche des informations sur des serveurs avec un nom de domaine complet modifié ou des informations sur le système d'exploitation pendant la durée comprise entre les deux instantanés.

Tableau 39. Rapports instantanés prédéfinis (suite)

Nom du rapport	Description
TADDM_SNAPSHOT_REFERENCE TADDM_SNAPSHOT_SYNC_REFERENCE	Compare un instantané à une liste de référence. Affiche des informations sur les serveurs dans la liste de référence, mais pas dans l'instantané, et les serveurs dans l'instantané, mais pas dans la liste de référence.
TADDM_SNAPSHOT_RECONCILIATION_SUMMARY TADDM_SNAPSHOT_SYNC_RECONCILIATION_SUMMARY	Vous demande un instantané et affiche les informations récapitulatives suivantes sur les serveurs reconnus : • nom d'hôte de référence • adresse IP de référence • nom d'hôte TADDM • adresse IP TADDM • statut • cause d'erreur
TADDM_SNAPSHOT_RECONCILIATION_DETAIL TADDM_SNAPSHOT_SYNC_RECONCILIATION_DETAIL	Vous demande un instantané et affiche les informations suivantes sur les serveurs reconnus : • nom d'hôte de référence • adresse IP de référence • nom d'hôte TADDM • adresse IP TADDM • statut • cause d'erreur • description de l'erreur • nom de portée • exclusion filtrée • cadre TADDM • nom d'hôte TADDM • nom de domaine complet TADDM • nom TADDM • nom d'affichage TADDM • JdoClass TADDM • TADDM dérivé OS • TADDM nom OS • adresse IP TADDM • numéro de série TADDM • fabricant TADDM • modèle TADDM • type d'hôte TADDM • TADDM virtuel • type TADDM • date de reconnaissance TADDM

Rapport Modules de stockage par hôte :

Le rapport Module de stockage par hôte dresse la liste des volumes de stockage et des modules de stockage utilisés par un système informatique spécifique.

Lors de l'exécution du rapport, vous êtes invité à entrer le nom d'hôte du système informatique pour lequel vous souhaitez afficher les informations de stockage. Dans la fenêtre Paramètre, entrez le nom d'hôte ou sélectionnez-le dans la liste déroulante.

Les informations suivantes sont affichées dans le rapport :

- Volume de stockage
- Module de stockage
- Fabricant
- Modèle
- Numéro de série
- Capacité disponible
- Capacité allouée

Rapport de consommateurs de modules de stockage :

Le rapport de consommateurs de modules de stockage dresse la liste des systèmes informatiques et des serveurs d'applications qui utilisent un module de stockage spécifique.

Lors de l'exécution du rapport, vous êtes invité à entrer le nom du module de stockage. Dans la fenêtre Paramètre, entrez le nom du module de stockage ou sélectionnez-le dans la liste déroulante.

Le rapport se présente sous la forme de trois tableaux :

Systèmes informatiques utilisant le module de stockage ***nom_module_stockage***
Ce tableau répertorie tous les systèmes informatiques reconnus qui utilisent le système de stockage spécifié.

Serveur d'applications utilisant le module de stockage ***nom_module_stockage***
Ce tableau répertorie tous les serveurs d'applications reconnus qui utilisent le système de stockage spécifié.

Applications métier utilisant le module de stockage ***nom_module_stockage***
Ce tableau répertorie toutes les applications métier reconnues qui utilisent le système de stockage spécifié.

Rapport de topologie de connexion système :

Ce rapport affiche un rapport textuel des systèmes informatiques avec les connexions réseau vers ou émanant d'autres systèmes informatiques. Lorsque vous lancez le rapport, vous devez entrer l'élément de configuration pour lequel vous voulez exécuter le rapport et vous devez indiquer s'il s'agit d'un système informatique ou d'une application métier.

Si le rapport est exécuté pour un système informatique, tous les systèmes informatiques avec des connexions réseau vers ou émanant du système informatique sélectionné s'affichent dans un tableau, avec les mesures correspondant à chaque connexion réseau. Si le rapport est exécuté pour une

application métier, tous les systèmes informatiques avec des connexions réseau vers ou émanant de l'application métier sélectionnée s'affichent dans un tableau.

Vous pouvez afficher la topologie de connexion système pour chaque système informatique en cliquant sur le nom du système dans le rapport.

Rapport d'utilisation système pendant les heures pleines :

Ce rapport affiche les valeurs d'utilisation du système aux heures les plus fortes pour les systèmes de la portée indiquée à la date spécifiée.

Les mesures d'utilisation incluent les informations suivantes :

- utilisation horaire de l'UC à 95%
- utilisation horaire de la mémoire au pourcentage le plus élevé
- utilisation horaire la plus forte de la bande passante réseau
- utilisation horaire la plus forte des E-S du disque

Rapport d'utilisation système :

Ce rapport affiche la configuration du système d'exploitation du serveur générique et les informations d'utilisation connexes.

Les données de configuration du système d'exploitation incluent les informations suivantes :

- UC
- mémoire
- système de fichiers

Il s'agit des informations les plus récentes sur la configuration du serveur, disponibles pour TADDM. Ces données incluent les éléments suivants :

- UC
- mémoire
- réseau
- disque

Rapports de serveurs inconnus :

Les rapports de serveurs inconnus comportent tous les processus de serveurs détectés non reconnus par TADDM. Le rapport regroupe les processus de serveur reconnus selon le système, et les répertorie en fonction du nom de système hôte qualifié complet. Ce rapport ne contient pas de paramètres.

Les serveurs inconnus sont identifiés après une reconnaissance par un agent de génération de la topologie. L'agent de génération de la topologie s'exécute en arrière-plan sur une base périodique en fonction de la valeur de la fréquence configurée, en conséquence il est possible que des serveurs inconnus ne soient pas reconnus immédiatement à l'issue de la reconnaissance. La fréquence par défaut d'exécution de l'agent de génération de la topologie est toutes les quatre heures.

Pour cette raison, si vous exécutez le rapport de serveurs inconnus avant que l'agent de génération de la topologie ait terminé, le rapport risque de ne pas répertorier tous les serveurs inconnus.

Les informations suivantes sont affichées dans le rapport :

Nom Le nom de l'ordinateur sur lequel le processus de serveur inconnu est exécuté.

Protocole IP du contexte
L'adresse IP de l'ordinateur sur lequel le processus de serveur inconnu est exécuté.

ID processus
L'ID processus du processus de serveur inconnu.

ID de processus parent
L'ID processus du processus parent du processus de serveur inconnu.

Ligne de commande
La commande étant utilisée pour exécuter le processus de serveur inconnu.

Les données de ce rapport proviennent de la base de données BB_RUNTIMEPROCESS15_V.

Exécution d'un rapport BIRT

Vous pouvez utiliser la section Analyse du portail de gestion de données pour exécuter un rapport BIRT.

Pourquoi et quand exécuter cette tâche

Important : L'exécution d'un rapport BIRT dans le portail de gestion de données est possible uniquement si le visualiseur de rapports BIRT est activé. Le visualiseur de rapports est désactivé pour des raisons de sécurité. L'autre moyen d'afficher les rapports BIRT consiste à utiliser Tivoli Common Reporting après y avoir importé des rapports de TADDM. Si vous êtes conscient des risques, vous pouvez toujours restaurer le visualiseur de rapports BIRT.

Procédure

Pour produire un rapport BIRT, procédez comme suit :

1. Dans le panneau Fonctions, cliquez sur **Analyse**.
2. Dans la section Analyse, cliquez sur **Rapports BIRT**. La liste **Rapports TADDM BIRT** s'ouvre, affichant tous les rapports BIRT disponibles.
3. Dans la liste **Rapports TADDM BIRT**, cliquez sur le rapport à exécuter pour le mettre en évidence.
4. Facultatif : Spécifiez la valeur de la balise d'emplacement. La propriété `com.ibm.cdb.locationTaggingEnabled` du fichier `COLLATION_HOME/etc/collation.propertes` doit être définie sur `true`. Seules les données de rapport de cette balise d'emplacement spécifique sont affichées.

   Remarque : Les rapports BIRT inclus avec TADDM ne prennent pas en charge le filtrage d'emplacement sans personnalisation supplémentaire.
5. Cliquez sur **Produire le rapport**. Si le rapport possède des paramètres, vous êtes invité à en indiquer les valeurs. Lorsque vous avez fini d'indiquer les valeurs de paramètres, cliquez sur **OK**.

Résultats

Le rapport formaté apparaît dans la fenêtre de l'afficheur de rapport BIRT. Cliquez sur les icônes en haut du rapport pour avancer ou revenir en arrière dans le rapport, imprimer le rapport ou l'exporter dans un fichier. Pour ouvrir un rapport

approfondi présentant des informations supplémentaires sur un sous-ensemble des données de rapport, cliquez sur un lien dans le rapport.

Remarque : Les rapports exportés au format .doc sont compatibles avec Microsoft Word 2003 ou version ultérieure.

Exécution d'un rapport BIRT à partir de l'interface de ligne de commande

Vous pouvez exécuter un rapport BIRT à partir de l'interface de ligne de commande du serveur TADDM.

Procédure

Pour exécuter un rapport BIRT à partir de l'interface de ligne de commande, procédez comme suit :

1. Ouvrez une invite de commande et, selon la version de TADDM que vous utilisez, accédez à l'un des répertoires suivants :
   - 7.3.0 : `$COLLATION_HOME/deploy-tomcat/birt-viewer/WEB-INF/resources`
   - 7.3.0.1 et ultérieures : `$COLLATION_HOME/apps/birt-viewer/WEB-INF/resources`
2. Définissez la variable `BIRT_HOME`. Procédez de l'une des façons suivantes :
   - Sous Linux, selon la version de TADDM que vous utilisez, exécutez l'une des commandes suivantes :
     - 7.3.0 :
       ```
       export BIRT_HOME=$COLLATION_HOME/deploy-tomcat/birt-viewer
       ```
     - 7.3.0.1 et ultérieures :
       ```
       export BIRT_HOME=$COLLATION_HOME/apps/birt-viewer
       ```
   - Sous Windows, selon la version de TADDM que vous utilisez, exécutez l'une des commandes suivantes :
     - 7.3.0 :
       ```
       set BIRT_HOME=%COLLATION_HOME%/deploy-tomcat/birt-viewer
       ```
     - 7.3.0.1 et ultérieures :
       ```
       set BIRT_HOME=%COLLATION_HOME%/apps/birt-viewer
       ```
3. Exécuter le rapport BIRT. Procédez de l'une des façons suivantes :
   - Sous Linux, exécutez la commande suivante :
     ```
     ./genReport.sh -f format -o sortie -F paramètres rapport
     ```
   - Sous Windows, exécutez la commande suivante :
     ```
     genReport.bat -f format -o sortie -F paramètres rapport
     ```

   Les options de ligne de commande sont utilisés avec le programme **genReport** :

   format
   Le format de sortie du fichier de rapport. Les valeurs valides sont PDF et HTML.

   sortie Le chemin d'accès au fichier de rapport que vous souhaitez produire. Par exemple, `/home/cognos/utilization.pdf` sous Linux ou `C:\data\utilization.pdf` sous Windows.

   paramètres
   (Facultatif) Le chemin d'accès à un fichier de propriétés, où chaque propriété représente un paramètre requis par le rapport. Par exemple, `/home/cognos/utilization.properties` sous Linux ou `C:\data\utilization.properties` sous Windows.

Le texte suivant est un exemple de contenu d'un fichier de propriétés :

```
scope=All Windows Machines
metric=ALL
operator=N/A
value1=N/A
value2=N/A
appdeps=N/A
```

Vous devez vous assurer que les espaces figurant dans un nom de paramètre sont protégés par une barre oblique inversée. Par exemple, si le nom de paramètre est `Snapshot ID Parameter`, l'entrée figurant dans le fichier de propriétés doit être

```
Snapshot\ ID\ Parameter=my_id
```

rapport

Le chemin d'accès au rapport que vous souhaitez exécuter, avec l'intitulé "compiled" ajouté au nom. Par exemple :

- Sous Linux et TADDM 7.3.0 : `$COLLATION_HOME/deploy-tomcat/birt-viewer/WEB-INF/report/taddm_server_utilization.rptdesigncompiled`.
- Sous Linux et TADDM versions 7.3.0.1 et ultérieures : `$COLLATION_HOME/apps/birt-viewer/WEB-INF/report/taddm_server_utilization.rptdesigncompiled`.
- Sous Windows et TADDM 7.3.0 : `%COLLATION_HOME%\deploy-tomcat\birt-viewer\WEB-INF\report\taddm_server_utilization.rptdesigncompiled`.
- Sous Windows et TADDM versions 7.3.0.1 et ultérieures : `%COLLATION_HOME%\apps\birt-viewer\WEB-INF\report\taddm_server_utilization.rptdesigncompiled`

Résultats

Remarque : La commande **`genReport`** ne génère pas de rapport approfondi. En conséquence, les liens figurant dans le rapport généré ne fonctionnent pas.

Importation d'un rapport BIRT

Le portail de gestion de données permet d'ajouter des rapports personnalisés en important des conceptions de rapport BIRT.

Avant de commencer

Pour ajouter un rapport personnalisé, vous devez d'abord concevoir et développer le rapport à l'aide du concepteur BIRT. La conception de rapport doit être sauvegardé dans un fichier `.rptdesign` auquel vous pouvez accéder à partir du système client.

Remarque : Fix Pack 3 Dans TADDM version 7.3.0.3 et ultérieures, les colonnes dans les vues de base de données d'attributs ont des types de données spécifiques, par exemple, VARCHAR. Dans les éditions de TADDM précédentes, les colonnes n'avaient que le type CLOB. Par conséquent, après la mise à niveau vers le groupe de correctifs 3, il est possible que les rapports BIRT utilisant des attributs étendus ne fonctionnent plus. Par exemple, si les colonnes d'attributs étendus ne sont pas distribuées dans un type de données spécifique, tel que VARCHAR, des erreurs risquent d'être générées.

Procédure

Pour importer un rapport BIRT, procédez comme suit :

1. Dans la sous-fenêtre Fonctions du portail de gestion de données, cliquez sur **Analyse**.
2. Dans la section Analyse, cliquez sur **Rapports BIRT**. La liste **Rapports TADDM BIRT** s'ouvre, affichant tous les rapports BIRT disponibles.
3. Cliquez sur **Nouveau**.
4. A l'invite du système, indiquez les caractéristiques du nouveau rapport, en incluant le nom, la description et l'emplacement du fichier de conception de rapport. Les nom et description permettent d'identifier le rapport dans la liste **Rapports TADDM BIR** .
5. Cliquez sur **OK**.

Résultats

La conception de rapport est chargée dans le serveur, et le nouveau rapport devient disponible à partir du portail de gestion de données.

Remarque : Si le rapport existe déjà sur le serveur, l'importation échoue. Ceci peut se produire même si le rapport existant n'est pas visible dans le portail de gestion de données. (Par exemple, le rapport Affinité de serveur n'est pas pris en charge sur le serveur de synchronisation, et n'est donc pas affichée dans le portail de gestion de données, même s'il existe sur le serveur.)

Suppression d'un rapport BIRT

Le portail de gestion de données vous permet de supprimer des rapports BIRT à partir du serveur.

Avant de commencer

La suppression d'un rapport à partir du serveur supprime le fichier `.rptdesign` du fichier utilisé par le rapport, du répertoire de rapports sur le serveur. Si vous souhaitez conserver le modèle de rapport pour le réutiliser ultérieurement, vérifiez que vous possédez une copie de sauvegarde du fichier `.rptdesign` avant de supprimer le rapport.

Procédure

Pour supprimer un rapport BIRT, procédez comme suit :

1. Dans le panneau Fonctions, cliquez sur **Analyse**.
2. Dans la section Analyse, cliquez sur **Rapports BIRT**. La liste **Rapports TADDM BIRT** s'ouvre, affichant tous les rapports BIRT disponibles.
3. Sélectionnez le rapport à supprimer.
4. Cliquez sur **Supprimer**.
5. Pour régénérer la liste **Rapports TADDM BIRT**, cliquez sur **Régénérer**.

Résultats

Le rapport sélectionné est supprimé du serveur et n'apparaît plus dans la liste **Rapports TADDM BIRT** du portail de gestion de données. En outre, le fichier `.rptdesign` associé au rapport est supprimé du répertoire de rapports du serveur TADDM.

Exportation d'une conception de rapport BIRT

Le portail de gestion de données permet d'exporter une conception de rapport BIRT depuis le serveur.

Pourquoi et quand exécuter cette tâche

Vous voudrez peut-être exporter une conception de rapport pour utiliser un rapport existant en tant que base pour un nouveau rapport personnalisé ou si vous souhaitez importer la conception de rapport dans un autre serveur.

Procédure

Pour exporter une conception de rapport BIRT, procédez comme suit :

1. Dans le panneau Fonctions, cliquez sur **Analyse**.
2. Dans la section Analyse, cliquez sur **Rapports BIRT**. La liste **Rapports TADDM BIRT** s'ouvre, affichant tous les rapports BIRT disponibles.
3. Sélectionnez le rapport à exporter.
4. Cliquez sur **Télécharger**.
5. Lorsque le navigateur vous le demande, indiquez que vous souhaitez enregistrer le fichier et indiquer un emplacement.

Résultats

La conception utilisée par le rapport sélectionné est sauvegardé à l'emplacement que vous avez indiqué en tant que fichier .rptdesign. Vous pouvez ouvrir et modifier ce fichier à l'aide de l'outil de concepteur BIRT.

Restauration du visualiseur de rapports BIRT

Si vous êtes avisé des risques liés à la sécurité mais que vous souhaitez néanmoins utiliser le visualiseur de rapports BIRT, vous pouvez le restaurer.

Procédure

1. Dans le fichier `collation.properties`, définissez la propriété `com.ibm.taddm.birtviewer.enabled` sur `true`:

   ```
   com.ibm.taddm.birtviewer.enabled=true
   ```

2. Redémarrez le serveur TADDM.

   Remarque : Dans le cas d'une mise à niveau du serveur TADDM, par défaut, cet indicateur est défini à `false`.

Utilisation de l'outil d'image instantanée

Vous pouvez utiliser l'outil d'image instantanée pour faire une copie des informations du système informatique, des événements de reconnaissance et des applications serveurs en cours d'exécution au moment de la prise de l'image.

Vous pouvez également utiliser l'outil d'image instantanée pour charger des informations utilisées dans le processus de synchronisation, par exemple :

- charger une liste de serveurs attendus, également connus comme liste de référence
- charger une liste de serveurs exclus

Vous pouvez utiliser des rapports pour demander les informations capturées par l'outil d'image instantanée, par exemple :

- quels serveurs ont été ajoutés ou supprimés
- le rapport entre les serveurs physiques et les serveurs virtuels
- quels serveurs n'ont pas pu être totalement reconnus du fait qu'une session SSH n'a pas pu être établie avec succès
- le delta entre la liste des serveurs reconnus et la liste des serveurs attendus

Restriction : Effectuez des instantanés une fois l'exécution des agents de topologie et de reconnaissance terminée. Si vous effectuez un instantané avant que les agents de topologie ne terminent le traitement des informations détectées, certains rapports d'instantanés, tels le rapport d'échec de session d'instantané, peuvent être incomplets.

Syntaxe de la commande snapshot.sh :

La commande `snapshot.sh` permet de prendre une image instantanée du système et des événements et serveurs associés. La commande `snapshot.sh` se trouve dans le répertoire `$COLLATION_HOME/bin`.

Vous pouvez exécuter la commande `snapshot.sh` sur le serveur TADDM. Dans un déploiement de serveur de diffusion en continu, vous devez exécuter la commande `snapshot.sh` sur le serveur de stockage principal.

Syntaxe de la commande

snapshot.sh *action* [*paramètres_action*]

Paramètres

addexclude *nomfichier* [*liste_exclusion*]
Ajoute la liste d'exclusion au fichier, ou en remplace une instance existante dans le fichier.

addref *nomfichier* [*liste_référence*]
Ajoute la liste de référence au fichier, ou en remplace une instance existante dans le fichier.

clear
Efface toutes les données d'image instantanée et supprime les tables.

compare [*image_instantanée_A image_instantanée_B*]
Affiche le delta entre les deux dernières images instantanées ou une image_instantanée_A et une image_instantanée_B, en fonction du nom d'hôte.

compareref [*image_instantanée_A liste_référence*]
Affiche le delta entre l'image instantanée et la liste de référence.

comparesig [*snapshot_A snapshot_B*]
Affiche le delta entre les deux dernières images instantanées ou une image_instantanée_A et une image_instantanée_B, en fonction de la signature pour les modifications du nom d'hôte ou du système d'exploitation.

compsys
Affiche les systèmes informatiques.

detail [*image_instantanée_A*]
Affiche tous les détails des systèmes informatiques dans la dernière image instantanée ou l'image_instantanée_A.

detailos [*image_instantanée_A*]
Affiche les informations sur le système d'exploitation des systèmes informatiques dans la dernière image instantanée ou l'image_instantanée_A.

help
Affiche l'aide détaillée sur l'utilisation de la commande **snapshot.api**.

list [*image_instantanée_A*]
Affiche la toute dernière image instantanée ou l'image_instantanée_A.

listall [*par défaut*]
Affiche toutes les images instantanées.

listexclude [*liste_exclusion*]
Affiche la liste d'exclusion la plus récente ou celle spécifiée par le nom.

listref [*liste_référence*]
Affiche la liste de référence la plus récente ou celle spécifiée par le nom.

listallexclude
Affiche toutes les listes d'exclusion.

listallref
Affiche toutes les listes de référence.

nosession [*image_instantanée_A*]
Affiche les systèmes informatiques qui ne sont pas parvenus à héberger une session dans la toute dernière image instantanée ou l'image_instantanée_A.

remove *image_instantanée_A* [*type*]
Supprime l'image instantanée A ou toutes les images instantanées du type spécifié.

removeexclude *liste_exclusion*
Supprime la liste d'exclusion spécifiée par le nom.

removeref *liste_référence*
Supprime la liste de référence spécifiée par le nom.

session [*image_instantanée_A*]
Affiche les systèmes informatiques qui ont hébergé une session dans la toute dernière image instantanée ou l'image_instantanée_A.

sensorerror [*image_instantanée_A*]
Affiche toutes les erreurs de détecteur de la toute dernière image instantanée ou de l'image_instantanée_A.

take [*type*] [*description*]
Prend une image instantanée, en incluant le cas échéant, des informations sur le type et la description.

Utilisation de l'outil d'image instantanée pour réduire le nombre de serveurs physiques :

Vous pouvez utiliser l'outil d'image instantanée lors du remplacement d'un grand nombre de serveurs physiques par moins de serveurs physiques, exécutant des serveurs virtuels.

Procédure

Pour obtenir des informations utiles lors d'une tentative de réduction du nombre de serveurs physiques utilisés, procédez comme suit :

1. Effectuez une reconnaissance de tous les systèmes connus.

2. A l'aide de l'outil d'image instantanée, prenez une image instantanée :
   `snapshot.sh take`

   Vous pouvez éventuellement ajouter des informations (type et description) à l'image instantanée :
   `snapshot.sh take type description`
3. Dans le portail de gestion de données, exécutez le rapport TADDM_SNAPSHOT_SESSION_FAILED. Le rapport renvoie des informations sur les systèmes non reconnus car aucune session SSH n'a pu être établie.
4. Assurez-vous que des sessions SSH peuvent être établies avec tous les systèmes. Il peut être nécessaire de mettre à jour les détails d'authentification dans TADDM.
5. Effectuez une reconnaissance uniquement des systèmes qui n'ont pas pu être accédés au cours de la première reconnaissance pour vous assurer que tous les problèmes de connexion ont été résolus.
6. Au bout du délai approprié, un mois par exemple, effectuez une reconnaissance de tous les systèmes connus.
7. Dans le portail de gestion de données, exécutez le rapport TADDM_SNAPSHOT_CHANGE. Le rapport renvoie des informations sur les nouveaux systèmes visibles depuis la prise de l'image instantanée, les systèmes qui ont disparu et le rapport serveurs physiques/serveur virtuels sous forme de pourcentages.

Utilisation de l'outil d'image instantanée pour rapprocher les listes de systèmes attendus et réels :

Vous pouvez utiliser l'outil d'image instantanée et les rapports prédéfinis pour vérifier que la liste de serveurs disponibles sur le réseau correspond à la liste de serveurs attendus.

Procédure

Pour rapprocher les systèmes attendus et réels, procédez comme suit :

1. Préparez une liste de référence contenant la liste des serveurs attendus. La liste de référence est un fichier texte au format CSV (valeur séparées par des virgules) comportant les zones suivantes :
   - nom d'hôte
   - Adresse IP
   - cadre
   - système d'exploitation
   - type d'hôte
   - commentaires
   - zone de prise en charge
   - emplacement

   Pour plus d'informations sur la syntaxe du fichier de référence, exécutez la commande **snapshot.sh** avec le paramètre help :
   `snapshot.sh help`
2. Si besoin est, préparez une liste d'exclusion contenant la liste de serveurs à ignorer lors du rapprochement. La liste d'exclusion est un fichier texte au format CSV comportant les zones suivantes :
   - nom d'hôte

- type à exclure

Pour plus d'informations sur la syntaxe du fichier d'exclusion, exécutez la commande **snapshot.sh** avec le paramètre help :

```
snapshot.sh help
```

3. A l'aide de l'outil d'image instantanée, prenez une image instantanée :

```
snapshot.sh take
```

Vous pouvez éventuellement ajouter des informations (type et description) à l'image instantanée :

```
snapshot take type description
```

4. Dans le portail de gestion de données, exécutez l'un des rapports BIRT suivants :
   - TADDM_SNAPSHOT_RECONCILIATION_SUMMARY
   - TADDM_SNAPSHOT_RECONCILIATION_DETAIL

Utilisation de rapports instantanés dans un déploiement de serveur de synchronisation :

Vous pouvez collecter des informations dans un déploiement de serveur de synchronisation en exécutant la version d'entreprise des rapports instantanés prédéfinis.

Procédure

Pour exécuter des rapports instantanés prédéfinis dans un déploiement de serveur de synchronisation, procédez comme suit :

1. Si elle n'a pas déjà été créée, configurez la table d'instantanés. Pour ce faire, procédez comme suit :
   a. Sur chaque serveur TADDM, exécutez la commande snapshot.sh sans paramètres.
   b. Redémarrez TADDM sur chaque domaine et serveur de synchronisation.

   Cette procédure crée les tables d'instantanés si elles n'existent pas déjà. Les tables d'instantanés ne doivent être configurées qu'une seule fois par environnement TADDM.
2. Exécutez une reconnaissance sur chaque domaine TADDM, en prenant un instantané sur chaque domaine, si nécessaire.
3. Effectuez une synchronisation sur le serveur de synchronisation. Veillez à inclure tous les domaines.
4. Créez une image instantanée de l'entreprise. Sur le serveur de synchronisation, exécutez la commande suivante :

```
snapshot.sh take
```

5. Lancez les rapports sur chaque domaine. Utilisez la version standard de chaque rapport instantané, par exemple TADDM_SNAPSHOT_CHANGE.
6. Exécutez les rapports sur le serveur de synchronisation. Utilisez la version d'entreprise de chaque rapport instantané, par exemple TADDM_SNAPSHOT_SYNC_CHANGE.

Intégration de TADDM à d'autres produits Tivoli

Pour des fonctionnalités étendues dans la gestion de votre environnement informatique, vous pouvez intégrer IBM Tivoli Application Dependency Discovery Manager (TADDM) à d'autres produits Tivoli, notamment IBM Tivoli Business Service Manager, IBM Tivoli Monitoring et des systèmes de gestion des événements comme IBM Tivoli Netcool/OMNIbus.

Versions prises en charge

Vous pouvez vous reporter au tableau suivant pour connaître les versions prises en charge des produits auxquels TADDM peut être intégré.

Le tableau suivant montre les versions prises en charge des produits auxquels TADDM peut être intégré.

Tableau 40. Versions prises en charge des produits

Nom du produit	Version prise en charge
CMS/DIS (Context Menu Service et Data Integration Service)	
IBM Control Desk (ICD)	• 7.6
IBM SmartCloud Control Desk (SCCD)	• 7.5.1 - utilisez le niveau de groupe de correctifs le plus récent disponible
IBM Tivoli Business Service Manager (TBSM)	• 4.2.1 - utilisez le niveau de groupe de correctifs le plus récent disponible • 6.1.0 - utilisez le niveau de groupe de correctifs le plus récent disponible • 6.1.1 - utilisez le niveau de groupe de correctifs le plus récent disponible
IBM Tivoli Change And Configuration Management Database (CCMDB)	• 7.2.1
IBM Tivoli Integration Composer (ITIC)	• 7.5.1 - utilisez le niveau de groupe de correctifs le plus récent disponible
IBM Tivoli Monitoring (ITM)	• 6.2.1 • 6.2.2 - FP3 • 6.2.3 • 6.3
IBM Tivoli Netcool/OMNIbus	• 7.3 • 7.4 • Fix Pack 1 8.*x* - pris en charge par TADDM version 7.3.0.1 et ultérieure
IBM Tivoli Network Manager IP (ITNMIP)	• 3.9 • 4.1
Jazz for Service Management (JazzSM)	• 1.1
Tivoli Common Reporting (TCR)	• 1.3 • 2.1.1 • 3.1

Tableau 40. Versions prises en charge des produits (suite)

Nom du produit	Version prise en charge
Tivoli Directory Integrator (TDI)	• 7.0 • 7.1 • 7.1.1
Tivoli Netcool/IMPACT	• 7.1
Tivoli Workload Scheduler (TWS)	• 8.5.1 • 8.6

Pour plus d'informations sur les produits que vous intégrez à TADDM, consultez leur documentation respective :

- Pour plus d'informations sur Context Menu Service et Data Integration Service (CMS/DIS), voir la rubrique *Configuration de CMS (Context Menu Service) et DIS (Data Integration Service)* dans le *Guide d'installation* de TADDM
- IBM Control Desk (ICD)
- IBM SmartCloud Control Desk (SCCD)
- IBM Tivoli Business Service Manager (TBSM)
- IBM Tivoli Change and Configuration Management Database (CCMDB)
- IBM Tivoli Integration Composer (ITIC)
- IBM Tivoli Monitoring (ITM)
- IBM Tivoli Netcool/OMNIbus
- IBM Tivoli Network Manager IP (ITNMIP)
- Jazz for Service Management (JazzSM)
- Tivoli Common Reporting (TCR)
- Tivoli Directory Integrator (TDI)
- Tivoli Netcool/Impact
- Tivoli Workload Scheduler (TWS)

Intégration de TADDM à IBM Tivoli Monitoring via une automatisation OSLC

TADDM peut être intégré à IBM Tivoli Monitoring via une automatisation OSLC. Pour intégrer TADDM à IBM Tivoli Monitoring 6.3, nous recommandons d'utiliser une automatisation OSLC. L'ancienne méthode d'intégration à l'aide d'un détecteur IBM Tivoli Monitoring Scope est obsolète et sera retirée des prochaines éditions.

TADDM utilise l'infrastructure d'IBM Tivoli Monitoring des deux façons suivantes :

- TADDM obtient la liste des noeuds finaux d'IBM Tivoli Monitoring depuis Tivoli Enterprise Portal Server via une session d'automatisation OSLC.
- TADDM exécute des commandes de l'interface CLI sur les systèmes cible pour les détecteurs dans une reconnaissance de niveau 2 et de niveau 3 et capture la sortie de ces commandes.

En cas de problèmes, voir la rubrique *Problèmes avec le fournisseur de services d'automatisation d'exécution OSLC sous ITM* du *Guide de résolution de problèmes* de TADDM.

Fix Pack 5

Prérequis :

Si vous utilisez Windows 7 et ultérieur, vous aurez besoin de :

1. PowerShell version 2+
2. URL de protocole SOAP TEMS
3. Vérifiez que vous pouvez vous connecter à la fois à TEMS et TEPS

Le tableau suivant indique les étapes à exécuter pour activer l'intégration de TADDM à IBM Tivoli Monitoring via une automatisation OSLC.

Tableau 41. Intégration de TADDM à IBM Tivoli Monitoring via une automatisation OSLC

Etape	Détails
Configurez les hôtes ITM Tivoli Enterprise Monitoring Server (TEMS) et ITM TEPS	«Configuration des hôtes ITM Tivoli Enterprise Monitoring Server (TEMS) et ITM TEPS», à la page 207
Installez le fournisseur de services d'automatisation d'exécution OSLC sous IBM Tivoli Monitoring **Remarque :** Assurez-vous que vous toutes les exigences indiquées dans «Prérequis à l'installation du fournisseur de services d'automatisation d'exécution OSLC sous IBM Tivoli Monitoring», à la page 207 sont satisfaites.	«Installation du fournisseur de services d'automatisation d'exécution OSLC sous IBM Tivoli Monitoring», à la page 211
Configurez TADDM pour utiliser un fournisseur de services d'automatisation d'exécution OSCL	«Configuration de TADDM pour utiliser un fournisseur de services d'automatisation d'exécution OSLC», à la page 215
Configurez TADDM pour la reconnaissance : • Configurez les propriétés d'automatisation dans le fichier `collation.properties`. • Créez une nouvelle entrée de liste d'accès du type `<"Integration">"OSLC Automation"` dans la liste d'accès.	«Configuration pour reconnaissance sur une session d'automatisation OSLC», à la page 117

Une fois ces étapes effectuées, vous pouvez lancer une reconnaissance à l'aide du fournisseur de services d'automatisation d'exécution OSLC sous ITM.

Concepts associés:

«Intégration de TADDM à d'autres produits via une automatisation OSLC», à la page 214
TADDM peut être intégré à d'autres produits via une automatisation OSCL (Open Services for Lifecycle Collaboration). TADDM se connecte à un fournisseur de services d'automatisation d'exécution OSLC qui fournit des données sur d'autres infrastructures de produits qui peuvent être reconnues par TADDM à l'aide de session d'automatisation OSLC.

Fournisseur de services d'automatisation d'exécution OSLC sous ITM

Le fournisseur de services d'automatisation d'exécution OSLC sous ITM est utilisé pour importer des données concernant les adresses IP des noeuds finaux gérés par IBM Tivoli Monitoring pour TADDM et pour reconnaître des noeuds finaux IBM Tivoli Monitoring via une session d'automatisation OSLC.

La Figure 1. illustre un TADDM connecté à un fournisseur de services d'automatisation d'exécution OSLC sous ITM qui collecte des données sur une infrastructure gérée par ITM à l'aide de commandes KT1.

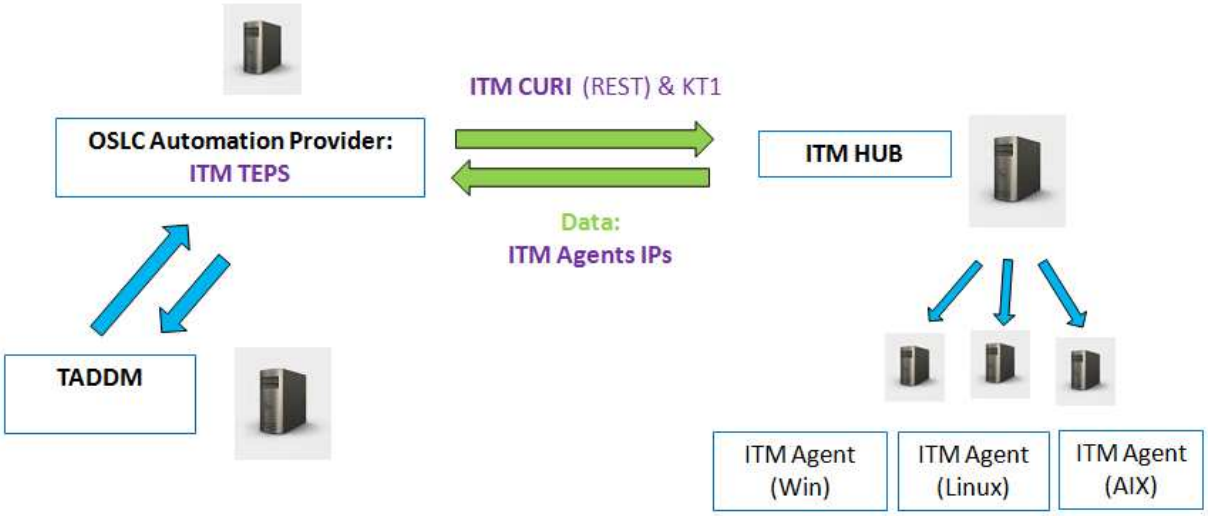

Figure 4. TADDM connecté à un fournisseur de services d'automatisation d'exécution OSLC sous ITM qui collecte des données sur une infrastructure gérée par ITM à l'aide de commandes KT1.

TADDM récupère la destination du fournisseur de services d'automatisation d'exécution OSLC à partir des services de registre dans Jazz SM ou à partir du fichier `collation.properties`. La Figure 2. illustre un TADDM utilisant des services de registre dans Jazz SM pour récupérer l'adresse du fournisseur de services d'automatisation d'exécution OSLC.

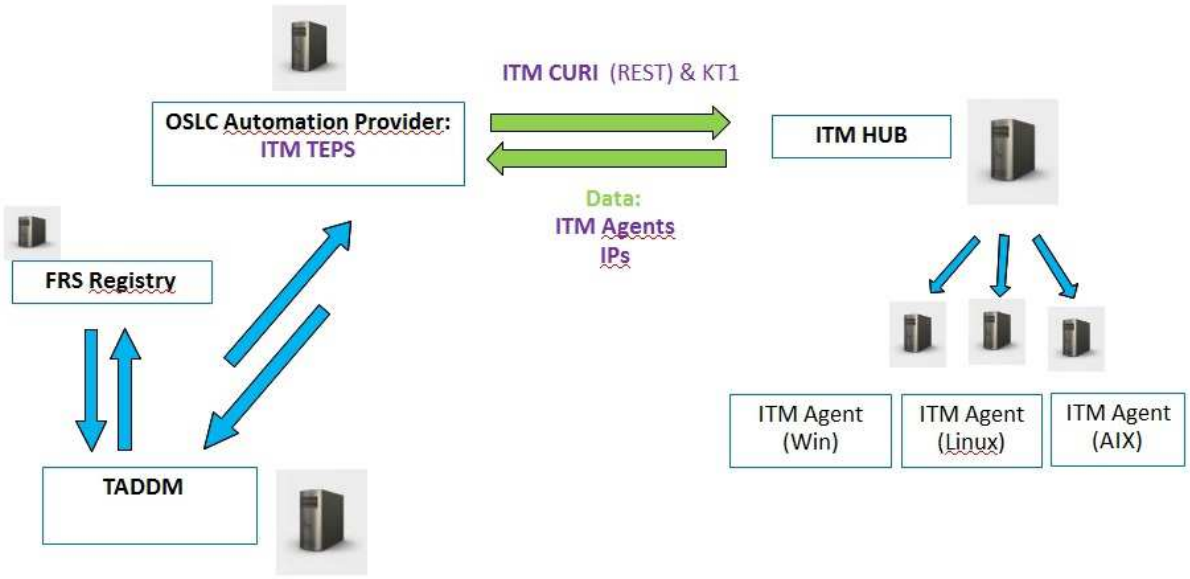

Figure 5. TADDM utilisant des services de registre dans Jazz SM pour récupérer l'adresse du fournisseur de services d'automatisation d'exécution OSLC.

TADDM peut être connecté directement à plusieurs fournisseurs de services d'automatisation d'exécution OSLC et à une instance unique des services de registre dans Jazz SM, là où plusieurs fournisseurs peuvent être enregistrés. La Figure 3. illustre des adresses de téléchargement TADDM des fournisseurs de services d'automatisation d'exécution OSLC déployés sur plusieurs ITM TEPS (serveur de portail) à partir des services de registre de Jazz SM.

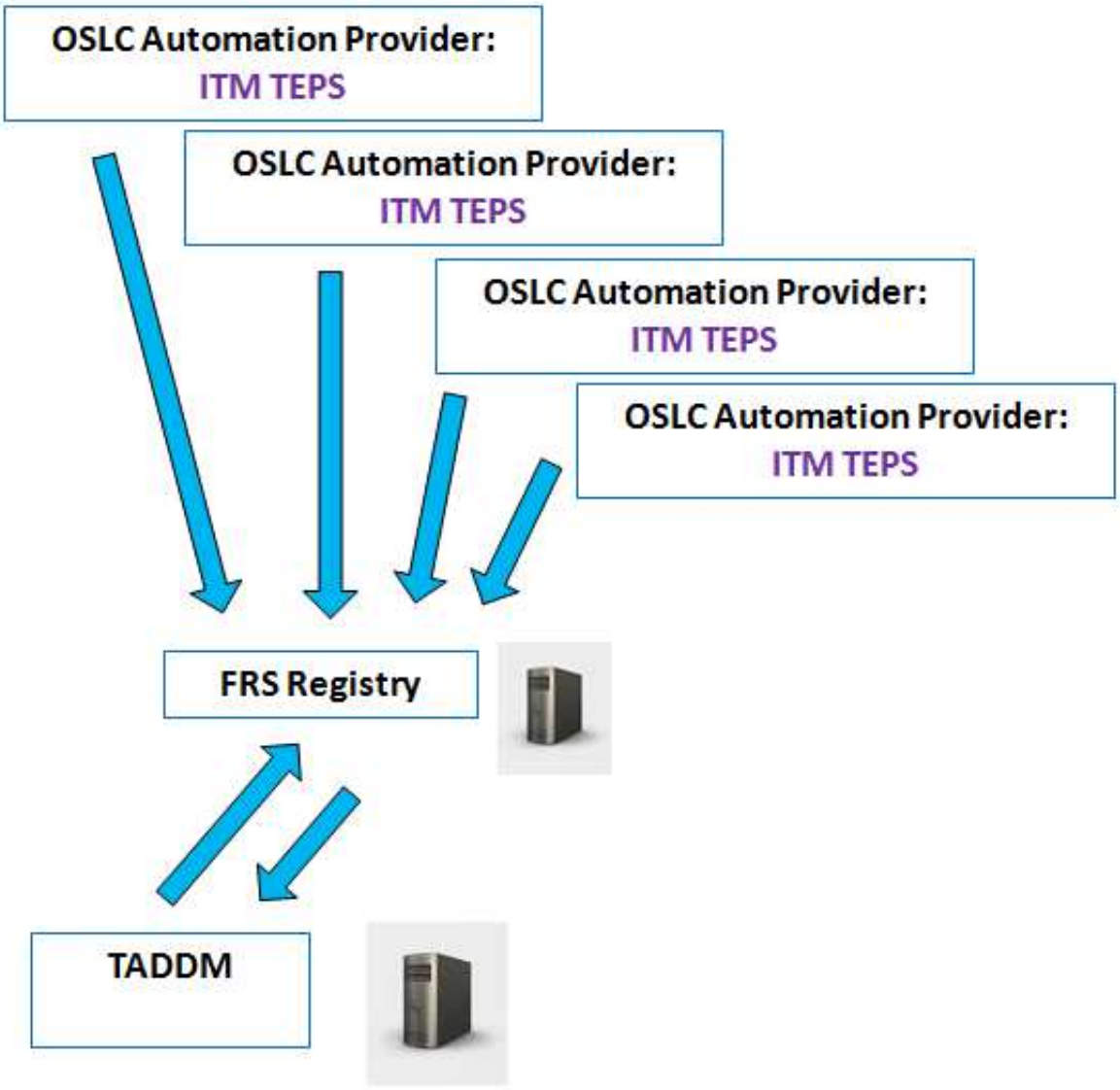

Figure 6. Adresses de téléchargement TADDM des fournisseurs de services d'automatisation d'exécution OSLC déployés sur plusieurs ITM TEPS (serveur de portail) à partir des services de registre dans Jazz SM.

Concepts associés:

«Fournisseur de services d'automatisation d'exécution OSLC», à la page 214
Le fournisseur de services d'automatisation d'exécution OSLC permet de renseigner des données concernant les adresses IP des noeuds finaux gérés par d'autres produits pour TADDM. Les données permettent de reconnaître des noeuds finaux via une session d'automatisation OSLC.

Installation du fournisseur de services d'automatisation d'exécution OSLC sous ITM

Pour importer des données concernant les adresses IP des noeuds finaux gérés par IBM Tivoli Monitoring (ITM) pour TADDM ou pour exécuter une reconnaissance, vous devez installer le fournisseur de services d'automatisation d'exécution OSLC sur IBM Tivoli Monitoring.

En cas de problèmes, voir la rubrique *Problèmes avec le fournisseur de services d'automatisation d'exécution OSLC sous ITM* du *Guide de résolution de problèmes* de TADDM.

Prérequis à l'installation du fournisseur de services d'automatisation d'exécution OSLC sous IBM Tivoli Monitoring :

Avant d'installer le fournisseur de services d'automatisation d'exécution OSLC sous IBM Tivoli Monitoring (ITM), vous devez configurer votre environnement afin de satisfaire à tous les prérequis.

Le fournisseur de services d'automatisation d'exécution OSLC sous ITM doit être installé sur un hôte ITM Tivoli Enterprise Portal Server (TEPS) host. La version prise en charge d'IBM Tivoli Monitoring est IBM Tivoli Monitoring 6.3.

Configuration des hôtes ITM Tivoli Enterprise Monitoring Server (TEMS) et ITM TEPS

Fix Pack 5 **Etape 1 - Reconfiguration de TEMS et TEPS**

La meilleure façon de configurer TEMS et TEPS est d'utiliser l'interface graphique MTEMS (Manage Tivoli Enterprise Monitoring Services).

Pour le système d'exploitation Windows, démarrez le processus **kinconfig.exe** ITM pour faire apparaître l'interface graphique de MTEMS (Manage Tivoli Enterprise Monitoring Services).

Pour Unix/Linux, vous pouvez démarrer l'interface graphique MTEMS à l'aide de la commande CLI "**./itmcmd manage**".

Pour chacun des deux composants ITM (TEMS et TEPS) :

- Mettez en évidence le composant sur l'interface utilisateur MTEMS
- Cliquez avec le bouton droit de la souris et sélectionnez Reconfigurer

Cela vous amènera dans la fenêtre de configuration de TEMS ou TEPS.

Fournissez tous les paramètres TEMS correctement (Type TEMS, Nom et protocole TEMS dans les paramètres de configuration principale et Nom d'hôte/adresse IP et Port dans les paramètres avancés) et sélectionnez "**OK**".

Sélectionnez "**Activer le fournisseur de données du tableau de bord**" dans la fenêtre de configuration de TEPS.

Fix Pack 5 **Etape 2 - Exécution des scripts TADDM et configuration**

Cette étape comprend l'exécution de deux scripts TADDM principaux pour faciliter l'intégration de TADDM à ITM.

1. Configurez le fichier provider.properties

Hôte ITM TEMS

Activez des commandes KT1 (**tacmd get/put/execute**) en exécutant un des scripts suivants sur l'hôte ITM TEMS :

- Pour le système d'exploitation Linux :

```
TADDM_CD_ISO/itm-discovery-support/configure_tems.sh <-i <ITM_HOME>>
 [-t <TEMP-DIR>
```

- Pour le système d'exploitation Windows :

```
TADDM_CD_ISO/itm-discovery-support/configure_tems.ps1 <-i <ITM_HOME>>
 [-t <TEMP-DIR>
```

où <*ITM_HOME*> est le répertoire d'installation d'ITM TEPS, par exemple `/opt/IBM/ITM` et <*TEMP-DIR*> le répertoire de destination des fichiers temporaires. La valeur par défaut du paramètre <*TEMP-DIR*> est `/var/log/automation_provider`.

Fix Pack 5 Une fois terminé, vous devriez voir les lignes suivantes à la fin de l'exécution du script.

```
INFO: Stopping ITM TEPS...
INFO: ITM TEPS has stopped.
INFO: Starting ITM TEPS...
INFO: ITM TEPS has started.
INFO: Checking if TEPS is running...
INFO: Checking if OSLC Automation Provider is installed...
INFO: Installation of OSLC Automation Provider successfully finished.
```

Remarque : Pour effectuer une validation d'ID utilisateur initiale (**tacmd get/put/execute**), utilisez **http:1920** ou **https:3661**, puis **ip.pipe:1920** ou **ip.spipe:3660** pour que KT1 puisse fonctionner depuis un fournisseur de services d'automatisation vers la cible reconnue. Ces protocoles seront activés dans ITM pour terminer la reconnaissance.

Hôte ITM TEPS

Vérifiez que le fournisseur de données du tableau de bord ITM est installé ou activé. Si ce n'est pas le cas, vous pouvez éventuellement l'installer ou l'activer. Voir la rubrique Vérification de l'activation du fournisseur de données du tableau de bord dans la documentation IBM Tivoli Monitoring.

Important : Si vous utilisez le système d'exploitation Windows 64 bits, assurez-vous que votre chemin de système (ou entrée de chemin dans le fichier `kfwenv`) pointe sur le répertoire TMAITM6 64 bits. Si tel n'est pas le cas, entrez-le manuellement. Par exemple, si vous avez installé ITM dans le répertoire `C:\IBM\ITM\`, `C:\IBM\ITM\TMAITM6_x64` doit être spécifié dans la variable d'environnement de chemin de système ou la directive PATH du fichier `C:\IBM\ITM\CNPS\kfwenv`.

Fix Pack 5

2. Exécutez le script `automation_provider` à partir de l'hôte d'ITM TEPS

Exécutez le script **`automation_provider`** sur votre serveur :

- Pour le système d'exploitation Linux :

  ```
  automation_provider.sh install  -t /tmp/log  -i /opt/IBM/ITM -c
  /tmp/provider.properties
  ```

- Pour le système d'exploitation Windows :

  ```
  automation_provider.ps1 install  -t /tmp/log  -i /opt/IBM/ITM -c
  /tmp/provider.properties
  ```

Un point important à noter ici est que même si un fichier provider.properties est créé avant d'exécuter le script automation_provider, il est ignoré et un fichier provider.properties 'par défaut' est créé dans le chemin de configuration ITM TEPS ($ITM_HOME/iw/profiles/ITMProfile/installedApps/ITMCell/itmautomationprovider.ear/itmautomationprovider.war/WEB-INF/provider.properties)

Vous devrez localiser ce fichier, apporter manuellement les modifications aux paramètres, puis redémarrer TEPS pour que les modifications du fichier prennent effet.

Fichiers requis

Les fichiers présents doivent être présents dans le répertoire, à partir duquel vous exécutez le script d'installation :

- Script d'installation :
  - Pour les systèmes d'exploitation Linux et AIX : `TADDM_CD_ISO/itm-discovery-support/automation_provider.sh`, et ses sous-modules situés dans `TADDM_CD_ISO/itm-discovery-support/mod/sh/`.
  - Pour le système d'exploitation Windows : `TADDM_CD_ISO/itm-discovery-support/automation_provider.ps1`, et ses sous-modules situés dans `TADDM_CD_ISO/itm-discovery-support/mod/ps/`.
- `itmautomationprovider.ear` - package fourni avec le fournisseur de services d'automatisation d'exécution OSLC sous ITM. L'emplacement exact du fichier est `TADDM_CD_ISO/itm-discovery-support/ear/itmautomationprovider.ear`.
- `provider.properties` - exemple de fichier de configuration pour le fournisseur de services d'automatisation d'exécution OSLC sous ITM. Vous pouvez configurer manuellement le fichier ou le transférer pour installer un script en tant que paramètre. S'il n'est pas transféré, vous devez fournir les paramètres requis au cours de l'installation. L'emplacement exacte du fichier est `TADDM_CD_ISO/itm-discovery-support/template_provider.properties`.
- KT1 prend en charge des bibliothèques pour le système d'exploitation approprié et son architecture, 32 ou 64 bits.
  - Pour le système d'exploitation Linux :

    ```
    TADDM_CD_ISO/itm-discovery-support/linux32
    TADDM_CD_ISO/itm-discovery-support/linux64
    ```

  - Pour le système d'exploitation AIX :

    ```
    TADDM_CD_ISO/itm-discovery-support/aix32
    TADDM_CD_ISO/itm-discovery-support/aix64
    ```

  - Pour le système d'exploitation Linux sur IBM System Z (zLinux) :

    ```
    TADDM_CD_ISO/itm-discovery-support/linuxz32
    TADDM_CD_ISO/itm-discovery-support/linuxz64
    ```

  - Pour le système d'exploitation Windows :

    ```
    TADDM_CD_ISO/itm-discovery-support/win32
    TADDM_CD_ISO/itm-discovery-support/win64
    ```

Configuration du fichier `provider.properties`

Vous pouvez éventuellement configurer le fichier `provider.properties` en réglant les paramètres suivants :

- `com.ibm.automationprovider.registration.host=`*`http://localhost:15210`* - enables connection to ITM. Le valeur spécifie une adresse URL publique pour TEPS. La valeur par défaut de ce paramètre est `http://localhost:15210`.

  Remarque : Modifiez le paramètre localhost pour représenter le nom d'hôte ou l'adresse IP du serveur TEPS.
- `com.ibm.automationprovider.itm.curi.url=`*`http://localhost:15210`* - spécifie l'adresse URL du fournisseur ITM CURI (REST). La valeur par défaut est `http://localhost:15210`.

  Remarque : Dans ce cas, modifiez le paramètre localhost pour représenter le nom d'hôte ou l'adresse IP de votre serveur TEPS.

- `com.ibm.automationprovider.itm.soap.url=http://localhost:1920///cms/soap` - spécifie l'adresse URL d'ITM SOAP. La valeur par défaut est `http://localhost:1920///cms/soap`.

  Remarque : Dans ce cas, modifiez le paramètre localhost pour représenter le nom d'hôte ou l'adresse IP de votre serveur TEMS concentrateur, qui peut ou non se trouver sur le même hôte que votre TEPS (dans la plupart des environnements de production, TEMS et TEPS sont installés sur des serveurs distincts).

Remarque : Si vous avez configuré ITM CURI ou ITM SOAP sans utiliser les valeurs par défaut, ou si vous avez configuré une sécurité SSL sous ITM TEPS, ou les deux, vérifiez que les adresses URL spécifiées pour les propriétés `com.ibm.automationprovider.itm.curi.url` et `com.ibm.automationprovider.itm.soap.url` sont correctes.

Les valeurs des paramètres spécifiées dans le fichier `provider.properties` sont prioritaires sur les valeurs des paramètres définis à partir de la ligne de commande.

Fix Pack 5 Si vous avez l'intention d'exécuter une découverte sur RTEMS, assurez-vous que le paramètre "`KT1_TEMS_SECURE=YES`" est activé dans votre fichier d'environnement.

Enregistrement des fournisseurs de services d'automatisation d'exécution OSLC dans les services de registre de JAZZ SM (FRS)

Vous pouvez éventuellement enregistrer des fournisseurs de services d'automatisation d'exécution OSLC dans les services de registre de JAZZ SM. Choisissez l'une des méthodes suivantes :

- Ajoutez les paramètres suivants au fichier `provider.properties` :
  - `com.ibm.automationprovider.frs.url` - spécifie l'adresse URL FRS pour l'enregistrement du fournisseur de services d'automatisation d'exécution OSLC. L'adresse URL complète de la collection est obligatoire, par exemple `http://9.122.100.100:9083/oslc/pr/collection`.
  - `com.ibm.automationprovider.frs.user` - spécifie le nom d'utilisateur qui est utilisé pour la connexion à FRS.
  - `com.ibm.automationprovider.frs.password` - spécifie le mot de passe qui est utilisé pour la connexion à FRS.
  - `com.ibm.automationprovider.registration.initialdelay=5000` - indique le temps entre le démarrage du fournisseur de services d'automatisation d'exécution OSLC et la première tentative d'enregistrement dans FRS. La valeur par défaut exprimée en millisecondes est `5000`. Pour désactiver l'enregistrement, définissez la valeur à `-1`.
- Ajouter l'option `-f` dans la ligne de commande, par exemple `./automation_provider.sh -f`, et pendant l'installation du fournisseur, à l'invite, fournissez les paramètres requis.

Installation du fournisseur de services d'automatisation d'exécution OSLC sous IBM Tivoli Monitoring :

Pour installer un fournisseur de services d'automatisation d'exécution OSLC sous IBM Tivoli Monitoring (ITM), vous devez exécuter le script `automation_provider`. Vous pouvez installer le fournisseur de services d'automatisation d'exécution OSLC en mode interactif ou non interactif.

Procédure

Pour installer le fournisseur de services d'automatisation d'exécution OSLC, exécutez le script `automation_provider` suivant à partir de l'hôte ITM TEPS :

- Pour le système d'exploitation Linux :

```
TADDM_CD_ISO/itm-discovery-support/automation_provider.sh install
[-i <ITM-HOME>] [-t <TEMP-DIR>] [[-c <CONFIG-FILE> | [-h <TEPS-IP>]
 [-p <TEPS-PORT>]] [-f]
```

- Pour le système d'exploitation Windows :

```
TADDM_CD_ISO/itm-discovery-support/automation_provider.ps1 install
[-i <ITM-HOME>] [-t <TEMP-DIR>] [[-c <CONFIG-FILE> | [-h <TEPS-IP>]
 [-p <TEPS-PORT>]] [-f]
```

où :

-i <*ITM-HOME*>
: est le répertoire d'installation d'ITM TEPS, par exemple `/opt/IBM/ITM`.

-t <*TEMP-DIR*>
: est le répertoire de destination des fichiers temporaires. La valeur par défaut est `/var/log/automation_provider`.

-h <*TEPS-IP*>
: est l'adresse IP de l'hôte ITM TEPS.

-p <*TEPS-PORT*>
: est le port HTTP d'ITM TEPS.

-c <*CONFIG-FILE*>
: est la destination du fichier `provider.properties` qui contient la configuration du fournisseur de services d'automatisation d'exécution OSLC.

-f
: est un indicateur que vous pouvez utiliser pour être invité durant l'installation à fournir les paramètres requis pour enregistrer les fournisseurs de service d'automatisation d'exécution OSLC dans les services de registre de JAZZ SM.

Important : Tous les paramètres du script d'installation sont facultatifs. Vous pouvez les spécifier dans n'importe quel ordre.
Exemples:

```
automation_provider.sh install -t /tmp/log -i /opt/IBM/ITM -h 9.100.100.200 -p 15210
automation_provider.ps1 install -i /opt/IBM/ITM
```

- Vous pouvez installer le fournisseur de services d'automatisation d'exécution OSLC en mode non interactif. Procédez comme suit :
  1. Configurez le fichier `provider.properties`. Voir la section «Configuration du fichier provider.properties», à la page 209.
  2. Exécutez le script `automation_provider` à partir de l'hôte d'ITM TEPS :
     - Pour le système d'exploitation Linux :

```
automation_provider.sh install  -t /tmp/log
-i /opt/IBM/ITM -c /tmp/provider.properties
```

– Pour le système d'exploitation Windows :

```
automation_provider.ps1 install  -t /tmp/log
-i /opt/IBM/ITM -c /tmp/provider.properties
```

Remarque : Si vous avez configuré ITM CURI ou ITM SOAP sans utiliser les valeurs par défaut, ou si vous avez configuré une sécurité SSL sous ITM TEPS, ou si ces deux ont été réalisés, installez le fournisseur de services d'automatisation d'exécution OSLC en mode non interactif. Vérifiez que les adresses URL spécifiées pour les propriétés `com.ibm.automationprovider.itm.curi.url` et `com.ibm.automationprovider.itm.soap.url` sont correctes.

- Vous pouvez installer le fournisseur de services d'automatisation d'exécution OSLC en mode interactif. Pendant l'installation, fournissez les valeurs pour les paramètres requis comme indiqué dans la section «Configuration du fichier provider.properties», à la page 209.

Vérification de l'installation du fournisseur de services d'automatisation d'exécution OSLC :

Vous pouvez vérifier que le fournisseur de services d'automatisation d'exécution OSLC a été correctement installé sous IBM Tivoli Monitoring.

Procédure

1. Vérifiez qu'ITM TEMS dispose de tous les agents Windows, Linux ou UX en fonctionnement en exécutant les commandes suivantes :

   ```
   /opt/IBM/ITM /bin/tacmd login -u admin -p password -s localhost
   /opt/IBM/ITM /bin/tacmd listSystems
   ```

2. Assurez-vous que chaque ITM TEMS dispose d'un plan d'automatisation. Les plans doivent contenir des adresses IP des noeuds finaux d'ITM. Ouvrez les adresses Web suivantes dans votre navigateur Web :

   ```
   http://<ITM_TEPS>:<ITM_PORT>/itmautomationprovider
   http://<ITM_TEPS>:<ITM_PORT>/itmautomationprovider/services/plans
   ```

   Exemple

   ```
   http://9.100.200.100:15210/itmautomationprovider/services/plans
   ```

Vérification de l'état du fournisseur de services d'automatisation d'exécution OSLC :

Vous pouvez vérifier l'état de l'installation du fournisseur de services d'automatisation d'exécution OSLC sous ITM.

Procédure

Exécutez le script `automation_provider` suivant :

- Pour le système d'exploitation Linux :

  ```
  automation_provider.sh status [i- <ITM-HOME>] [t- <TEMP-DIR>]
  ```

- Pour le système d'exploitation Windows :

  ```
  automation_provider.ps1 status [i- <ITM-HOME>] [t- <TEMP-DIR>]
  ```

où :

i- *<ITM-HOME>*
est le répertoire d'installation d'ITM TEPS, par exemple `/opt/IBM/ITM`.

t- <*TEMP-DIR*>
est le répertoire de destination des fichiers temporaires. La valeur par défaut est `/var/log/automation_provider`.

Important : Tous les paramètres du script sont facultatifs. Vous pouvez les spécifier dans n'importe quel ordre.

Exemples

```
automation_provider.sh status
automation_provider.ps1 status -i /opt/IBM/ITM
automation_provider.sh status -t /tmp/log -i /opt/IBM/ITM
```

Désinstallation du fournisseur de services d'automatisation d'exécution OSLC :

Vous pouvez désinstaller le fournisseur de services d'automatisation d'exécution OSLC sous ITM en exécutant le script `automation_provider`.

Procédure

Exécutez le script `automation_provider` suivant :

- Pour le système d'exploitation Linux :
  `automation_provider.sh uninstall [i- <ITM-HOME>] [t- <TEMP-DIR>]`
- Pour le système d'exploitation Windows :
  `automation_provider.ps1 uninstall [i- <ITM-HOME>] [t- <TEMP-DIR>]`

où :

i- <*ITM-HOME*>
est le répertoire d'installation d'ITM TEPS, par exemple `/opt/IBM/ITM`.

t- <*TEMP-DIR*>
est le répertoire de destination des fichiers temporaires. La valeur par défaut est `/var/log/automation_provider`.

Important : Tous les paramètres du script sont facultatifs. Vous pouvez les spécifier dans n'importe quel ordre.

Exemples

```
automation_provider.sh uninstall
automation_provider.ps1 uninstall -i /opt/IBM/ITM
automation_provider.sh uninstall -t /tmp/log -i /opt/IBM/ITM
```

Configuration de la reconnaissance pour le fournisseur de services d'automatisation d'exécution OSLC sous ITM

Lorsque vous utilisez le fournisseur de services d'automatisation d'exécution OSLC sous ITM, vous pouvez configurer le processus de reconnaissance à l'aide des propriétés suivantes.

com.collation.discover.dwcount=32
La valeur par défaut est `32`.

Cette propriété est une propriété de serveur TADDM, qui définit le nombre d'unités d'exécution de tâche de reconnaissance.

Pour de meilleurs résultats, affectez la même valeur aux propriétés `com.collation.discover.dwcount` et `KT1_RPC_THREADS`.

com.ibm.automationprovider.kt1.concurenttasks.limit=100
La valeur par défaut est `100`.

Cette propriété est une propriété du fournisseur de services d'automatisation d'exécution OSLC sous ITM qui peut être éditée dans le fichier `provider.properties`. Elle définit le nombre de demandes simultanées que le fournisseur envoie à TEMS. Les demandes en trop sont placées en file d'attente au niveau du fournisseur.

Remarque : Ne modifiez la valeur de cette propriété que si une régulation supplémentaire est requise entre TADDM et TEMS ou que plus de 100 unités d'exécution de tâche KT1 sont définies.

KT1_RPC_THREADS=10
La valeur par défaut est `10`.

Il s'agit d'une propriété ITM TEMS qui peut être éditée dans le fichier `ITM_HOME/config/kbbenv.ini`. Elle définit le nombre d'unités d'exécution de tâche qui répondent aux demandes KT1.

Pour de meilleurs résultats, affectez la même valeur aux propriétés `KT1_RPC_THREADS` et `com.collation.discover.dwcount`.

Intégration de TADDM à d'autres produits via une automatisation OSLC

TADDM peut être intégré à d'autres produits via une automatisation OSCL (Open Services for Lifecycle Collaboration). TADDM se connecte à un fournisseur de services d'automatisation d'exécution OSLC qui fournit des données sur d'autres infrastructures de produits qui peuvent être reconnues par TADDM à l'aide de session d'automatisation OSLC.

La reconnaissance via l'utilisation d'un fournisseur de services d'automatisation d'exécution OSLC est un processus générique qui peut être étendu pour inclure la reconnaissance d'autres produits qui implémentent leurs propres fournisseurs de service d'automatisation d'exécution OSLC. Durant la reconnaissance, un port par hôte fournisseur de services d'automatisation d'exécution OSLC, par services de registre dans Jazz SM, ou pour les deux est ouvert. Il permet un meilleur contrôle de sécurité. .

Le tableau suivant répertorie des rubriques contenant davantage d'informations sur la reconnaissance via OSLC.

Tableau 42. Rubriques contenant plus d'informations sur la reconnaissance via OSLC.

Informations	Emplacement
Configuration de la reconnaissance	«Configuration pour reconnaissance sur une session d'automatisation OSLC», à la page 117
propriétés du serveur TADDM	«Propriétés pour une reconnaissance via une session d'automatisation OSLC», à la page 86
Détecteurs prenant en charge une reconnaissance via une session d'automatisation OSLC	Voir la rubrique *Détecteurs prenant en charge une reconnaissance via une session d'automatisation OSLC* dans le *Guide de référence des détecteurs* de TADDM.

Fournisseur de services d'automatisation d'exécution OSLC

Le fournisseur de services d'automatisation d'exécution OSLC permet de renseigner des données concernant les adresses IP des noeuds finaux gérés par

d'autres produits pour TADDM. Les données permettent de reconnaître des noeuds finaux via une session d'automatisation OSLC.

TADDM peut obtenir la destination du fournisseur de services d'automatisation d'exécution OSLC à partir des services de registre dans Jazz SM ou à partir du fichier `collation.properties`.

TADDM peut être connecté directement à plusieurs fournisseurs de service d'automatisation d'exécution OSLC et à une instance unique des services de registre dans Jazz SM, où plusieurs fournisseurs de service d'automatisation d'exécution OSLC peuvent être enregistrés. Chaque fournisseur de services d'automatisation d'exécution OSLC stocke des informations sur une instance d'un produit particulier avec lequel TADDM s'intègre, par exemple un concentrateur ITM.

Référence associée:

«Fournisseur de services d'automatisation d'exécution OSLC sous ITM», à la page 203

Le fournisseur de services d'automatisation d'exécution OSLC sous ITM est utilisé pour importer des données concernant les adresses IP des noeuds finaux gérés par IBM Tivoli Monitoring pour TADDM et pour reconnaître des noeuds finaux IBM Tivoli Monitoring via une session d'automatisation OSLC.

Configuration de TADDM pour utiliser un fournisseur de services d'automatisation d'exécution OSLC :

Pour être en mesure d'exécuter une reconnaissance via une session d'automatisation OSLC, vous devez configurer TADDM pour utiliser un fournisseur de services d'automatisation d'exécution OSLC.

Procédure

Pour configurer TADDM pour utiliser un fournisseur de services d'automatisation d'exécution OSLC, procédez comme suit :

1. Vérifiez que le fournisseur de services d'automatisation d'exécution OSLC est installé et fonctionne.
2. Connectez TADDM au fournisseur de services d'automatisation d'exécution OSLC. Il existe deux manières de le faire, directement ou via les services de registre de Jazz for Service Management. Vous pouvez combiner ces méthodes si vous êtes en présence de plusieurs fournisseurs de service d'automatisation d'exécution OSLC.
   - Pour connecter TADDM directement au fournisseur de services d'automatisation d'exécution OSLC, ajoutez les adresses des fournisseurs de service d'automatisation d'exécution OSLC à la propriété `com.ibm.cdb.topobuilder.integration.oslc.automationprovider` dans le fichier `collation.properties`.
   - Pour connecter TADDM au fournisseur de services d'automatisation d'exécution OSLC à l'aide des services de registres de Jazz for Service Management, activer la recherche TADDM des services de registre de Jazz SM des fournisseurs de service d'automatisation d'exécution OSLC. Procédez comme suit :
     a. Vérifiez que les services de registre de JAZZ SM fonctionnent.
     b. Vérifiez que les fournisseurs de service d'automatisation d'exécution OSLC sont connectés aux services de registre de Jazz SM.

c. Configurez l'une des propriétés suivantes dans le fichier `collation.properties` pour fournir une adresse pour les services de registre de Jazz SM :

```
com.ibm.cdb.topobuilder.integration.oslc.frsurl
com.ibm.cdb.topobuilder.integration.oslc.automation.frsurl
```

3. Redémarrez le serveur TADDM.

Résultats

Après avoir configuré TADDM, vous pouvez exécuter une reconnaissance via une session d'automatisation OSLC.

Référence associée:

«Propriétés pour une reconnaissance via une session d'automatisation OSLC», à la page 86
Ces propriétés s'appliquent à une reconnaissance via une session d'automatisation OSLC.

Interface de ligne de commande pour OSLCAutomationAgent

OSLCAutomationAgent permet de collecter des données provenant des fournisseurs de services d'automatisation d'exécution OSLC. Vous pouvez utiliser des commandes pour exécuter l'agent manuellement et pour actualiser ou mettre à jour les ensembles de portées qu'il crée.

Les adresses des fournisseurs de services d'automatisation d'exécution OSLC sont configurées dans le fichier `collation.properties` ou téléchargées à partir des services de registre dans Jazz SM ou les deux. L'agent se connecte à chaque fournisseur de services d'automatisation d'exécution OSLC pour obtenir la liste des plans d'automatisation compatibles avec TADDM. Les plans d'automatisation consistent en adresses IP que l'agent utilise pour mettre en mémoire cache et créer des ensembles de portées de reconnaissance. Par exemple, lorsque TADDM s'intègre à IBM Tivoli Monitoring, les plans d'automatisation consistent en adresses IP des serveurs TEMS ITM et des noeuds finaux (agents) gérés par IBM Tivoli Monitoring. L'agent OSLCAutomationAgent met en mémoire cache et crée des ensembles de portées avec des adresses IP des agents IBM Tivoli Monitoring. Chaque ITM TEMS dispose d'un ensemble de portées distinct.

L'agent OSLCAutomationAgent s'exécute périodiquement dans le groupe des agents d'intégration.

Vous pouvez utiliser les commandes suivantes sur l'agent OSLCAutomationAgent.

- Pour exécuter l'agent manuellement, utilisez la commande suivante.

  ```
  /taddm/dist/support/bin/runtopobuild.sh -a OSLCAutomationAgent
  ```

- Pour actualiser des ensembles de portées, utilisez la commande suivante :

  ```
  /taddm/dist/support/bin/runtopobuild.sh -a OSLCAutomationAgent -s true
  ```

  Remarque : Les ensembles de portées sont actualisés uniquement dans le cas de changements dans le plan d'automatisation du fournisseur d'automatisation ITM. Pour forcer l'actualisation des ensembles de portées, utilisez la commande suivante :

  ```
  /taddm/dist/support/bin/runtopobuild.sh -a OSLCAutomationAgent
  --forceScopeSetRefresh true
  ```

  Les ensembles de portées sont disponibles dans le panneau **Portées** de la console de gestion de reconnaissance.

- Pour afficher les ensembles de portées mis en mémoire cache, utilisez la commande suivante :

  ```
  /taddm/dist/support/bin/runtopobuild.sh -a OSLCAutomationAgent -d true
  /taddm/dist/support/bin/runtopobuild.sh -a OSLCAutomationAgent
   --displayCache true
  ```

  Les ensembles de portées sont affichés dans les fichiers journaux TADDM suivants :

  - <COLLATION_HOME>/dist/log/services/TopologyBuilder.log
  - <COLLATION_HOME>/dist/log/agents/OSLCAutomationAgent.log

  L'exemple suivant montre la sortie que vous pouvez trouver dans le fichier <COLLATION_HOME>/dist/log/agents/OSLCAutomationAgent.log :

  ```
  2014-07-22 11:42:54,660 TopologyBuilder [pool-1-thread-1]  DEBUG
  oslc.OSLCAutomationAgent - OSLCAutomationAgent:displaying cache
  2014-07-22 11:42:54,669 TopologyBuilder [pool-1-thread-1]  INFO
   oslc.OSLCAutomationAgent - <AGENT_IP_2> http://9.120.100.100:15210/
  itmautomationprovider/services/plans/2 1406009933764
  2014-07-22 11:42:54,669 TopologyBuilder [pool-1-thread-1]  INFO
   oslc.OSLCAutomationAgent - <AGENT_IP_2> http:///9.120.100.100:15210/
  itmautomationprovider/services/plans/2 1406009933764
  2014-07-22 11:42:54,675 TopologyBuilder [pool-1-thread-1]  DEBUG
   oslc.OSLCAutomationAgent - OSLCAutomationAgent:cache end
  ```

Concepts associés:

«Présentation du processus de génération de topologie», à la page 16
TADDM exécute le processus de génération de la topologie de façon régulière. Une fois ce processus terminé à la suite d'une reconnaissance ou d'une opération de chargement en bloc, la base de données TADDM risque de contenir des objets non synchronisés et les relations de topologie risquent d'être incomplètes.

Intégration de TADDM à IBM Tivoli Monitoring (ancienne méthode)

En fonction des tâches spécifiques à exécuter dans votre environnement informatique, vous pouvez utiliser les fonctions d'intégration disponibles entre IBM Tivoli Application Dependency Discovery Manager (TADDM) et IBM Tivoli Monitoring. Vous pouvez intégrer TADDM à IBM Tivoli Monitoring à l'aide d'un détecteur IBM Tivoli Monitoring Scope.

Nouvelle méthode d'intégration

Important : A partir de TADDM version 7.3.0, il est recommandé d'effectuer l'intégration à IBM Tivoli Monitoring 6.3 via une automatisation OSLC. L'ancienne méthode d'intégration à l'aide d'un détecteur IBM Tivoli Monitoring Scope est obsolète et sera retirée des prochaines éditions.

Pour en savoir plus sur l'intégration de TADDM à IBM Tivoli Monitoring via une automatisation OSLC, voir «Intégration de TADDM à IBM Tivoli Monitoring via une automatisation OSLC», à la page 202 et sur les détecteurs qui prennent en charge une reconnaissance via une automatisation OSLC, voir la rubrique *Détecteurs prenant en charge une reconnaissance via une automatisation OSLC* du *Guide de référence des détecteurs* de TADDM.

Ancienne méthode d'intégration

Toutes les sections qui suivent s'appliquent à l'ancienne méthode d'intégration. Vous pouvez encore l'utiliser mais sachez que cette méthode est obsolète et sera retirée des prochaines éditions.

Le tableau 42 met en corrélation certaines tâches que vous devez éventuellement exécuter avec les fonctions d'intégration ; les autres sections présentent ces fonctions.

Tableau 43. Tâches utilisateur avec les fonctions d'intégration correspondantes à utiliser

Tâche	Fonction d'intégration à utiliser
En savoir plus sur la disponibilité en affichant les paramètres du système d'exploitation, les paramètres des applications et l'historique des modifications des systèmes surveillés par IBM Tivoli Monitoring.	• «Reconnaissance à l'aide d'IBM Tivoli Monitoring» • «Lancement selon le contexte», à la page 220
Vérifier que la disponibilité des systèmes d'exploitation que TADDM reconnaît est surveillée.	• «Reconnaissance à l'aide d'IBM Tivoli Monitoring» • «Rapports sur la portée de la surveillance», à la page 220
Afficher la disponibilité et les performances des systèmes reconnus par TADDM.	• «IBM Tivoli Monitoring DLA», à la page 219 • «Rapports sur la portée de la surveillance», à la page 220
Surveiller une application métier pour les modifications de configuration.	• «Reconnaissance à l'aide d'IBM Tivoli Monitoring» • «Evénements de modification», à la page 220 • «Lancement selon le contexte», à la page 220

Reconnaissance à l'aide d'IBM Tivoli Monitoring

TADDM peut exécuter des reconnaissances de niveaux 1 et 2 et certaines reconnaissances de niveau 3 à l'aide d'une infrastructure IBM Tivoli Monitoring 6.2.1 ou ultérieure. TADDM reconnaît les éléments de configuration dans l'environnement IBM Tivoli Monitoring uniquement à l'aide des autorisations d'accès pour votre serveur Tivoli Enterprise Portal au lieu des autorisations d'accès pour chaque ordinateur surveillé par le serveur du portail.

TADDM optimise l'infrastructure de Tivoli Monitoring des deux façons suivantes :

- TADDM obtient la liste des noeuds finaux Tivoli Monitoring du serveur Tivoli Enterprise Portal Server pour générer des informations sur la reconnaissance de niveau 1 de base et pour créer des portées pour les reconnaissances de niveau 2 et 3, plus profondes.
- TADDM utilise l'infrastructure Tivoli Monitoring pour exécuter des commandes CLI sur des systèmes cible pour les détecteurs dans les reconnaissances de niveau 2 et 3 et pour capturer le résultat de ces commandes.

Cette fonction présente les avantages suivants :

- Déploiement rapide de TADDM dans des environnements Tivoli Monitoring existants.
- Pas besoin de serveur ancre ou passerelle TADDM.
- Inutile de définir des ensembles de portées contenant des ordinateurs à analyser. Seule une portée avec une entrée unique pour Tivoli Enterprise Portal Server est obligatoire.
- Inutile de définir une liste d'accès (autorisations d'accès au système d'exploitation) pour les cibles de reconnaissance.
- Une seule entrée de liste d'accès pour la connexion à l'interface graphique de Tivoli Enterprise Portal Server est obligatoire.

Tableau 44. Rubriques contenant des informations supplémentaires sur la reconnaissance avec IBM Tivoli Monitoring

Informations	Emplacement des informations
Configuration de la reconnaissance à l'aide d'IBM Tivoli Monitoring	«Configuration de la reconnaissance à l'aide d'IBM Tivoli Monitoring (ancienne méthode)», à la page 115
Propriétés du serveur TADDM s'appliquant à la reconnaissance avec IBM Tivoli Monitoring	«Propriétés de la reconnaissance à l'aide d'IBM Tivoli Monitoring (ancienne méthode)», à la page 84
• Détecteurs prenant en charge la reconnaissance à l'aide d'IBM Tivoli Monitoring • Détecteur IBM Tivoli Monitoring Scope, avec des informations sur sa configuration et sur l'identification et la résolution des problèmes pouvant se produire lors du déploiement ou de l'utilisation du détecteur	*Guide de référence des détecteurs* de TADDM

IBM Tivoli Monitoring DLA

L'adaptateur de bibliothèque de reconnaissance (DLA) IBM Tivoli Monitoring extrait des données de Tivoli Monitoring sur les systèmes informatiques et les bases de données surveillés par Tivoli Monitoring. La sortie du DLA est un fichier XML formaté qui contient ces composants et leurs relations. Cette sortie inclut aussi des données représentant les agents Tivoli Monitoring et des données employées pour lancer des vues de disponibilité depuis TADDM. Pour plus d'informations sur le chargement des données exportées de DLA dans TADDM, voir la rubrique *Programme de chargement en bloc* dans le *Guide d'utilisation* de TADDM.

Pour lancer l'adaptateur de bibliothèque de reconnaissance, procédez comme suit :

1. Générez un adaptateur de bibliothèque de reconnaissance (DLA) sous ITM comme indiqué dans la rubrique *Using the Tivoli Management Services Library Adapter* à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSTFXA_6.2.2.1/com.ibm.itm.doc_6.2.2fp1/discoverylibraryadapter_tms.htm?lang=en.
2. Copiez le fichier de sortie du DLA sur le système hôte de TADDM.
3. Utilisez le programme de chargement en bloc pour charger le DLA depuis ITM vers TADDM. Utilisez la commande suivante :

```
$COLLATION_HOME/bin/loadidml.sh -u nom_utilisateur
-p mot de passe -f chemin_DLA
```

Quand vous installez de nouveaux agents Tivoli Monitoring, ils peuvent offrir une prise en charge supplémentaire au DLA Tivoli Monitoring. Les agents fournissent des informations pour les rapports sur la portée de la surveillance ; la portée de la surveillance pour le rapport sur les systèmes d'exploitation ne requiert pas de DLA.

Quand vous installez un agent, vous devez activer la prise en charge de l'application correspondante pour qu'ils participent à la sortie générée par le DLA. Tous les agents ne prennent pas en charge le DLA Tivoli Monitoring.

Pour plus d'informations, reportez-vous à la documentation relative à la configuration de la prise en charge des application pour les agents non standard. Pour vérifier qu'un agent prend en charge le DLA Tivoli Monitoring, voir la documentation pour l'agent IBM Tivoli Composite Application Manager.

Rapports sur la portée de la surveillance

Les rapports sur la portée de la surveillance montrent des détails sur les différents composants de votre environnement. Vous pouvez générer un rapport pour des systèmes d'exploitation, des bases de données, des applications Microsoft, des serveurs VMware et des composants System p dans votre environnement. Ces composants sont surveillés par des agents IBM Tivoli Monitoring 6.1 ou ultérieur.

Pour plus d'informations sur les rapports de portée de la surveillance, voir le *Guide d'utilisation* de TADDM.

Evénements de modification

Vous pouvez configurer TADDM pour avertir IBM Tivoli Monitoring lorsque la modification d'une ressource reconnue est détectée.

Tableau 45. Rubriques contenant plus d'informations sur les événements de changement

Informations	Emplacement des informations
• Configuration de TADDM en vue de l'envoi des événements de modification • Configuration d'un fournisseur de données IBM Tivoli Monitoring • Configuration des événements de modification pour un système métier	«Envoi d'événements de modification à des systèmes externes», à la page 229

Lancement selon le contexte

Grâce au lancement en contexte, vous pouvez afficher des données TADDM dans les vues Tivoli Enterprise Portal d'IBM Tivoli Monitoring.

En configurant les vues de topologies devant s'afficher dans Tivoli Enterprise Portal, vous pouvez afficher une infrastructure physique, une infrastructure d'applications et des topologies système métier dans les vues de disponibilité Tivoli Enterprise Portal.

Tableau 46. Rubriques contenant plus d'informations sur le lancement selon le contexte

Informations	Emplacement des informations
URL obligatoires pour afficher les vues de topologies	«Configuration du lancement selon le contexte», à la page 226
Instructions pour configurer le lancement selon le contexte pour afficher les paramètres du système d'exploitation, les paramètres d'applications et l'historique des modifications pour les événements de modification entrants	«Création de liens détaillés dans les rapports sur les événements de modification de la configuration dans IBM Tivoli Monitoring», à la page 240

Enregistrement des éléments de configuration pour Context Menu Service et Data Integration Service

Si vous utilisez CMS (Context Menu Service) et DIS (Data Integration Service) pour activer les points de lancement inter-produit, vous devez enregistrer les éléments de configuration TADDM dans la base de données CMS/DIS.

Avant de commencer

Avant de pouvoir utiliser Context Menu Service et Data Integration Service, vous devez configurer la base de données CMS/DIS.

Pourquoi et quand exécuter cette tâche

Les éléments de configuration TADDM sont enregistrés dans la base de données CMS/DIS de deux manières :

- Enregistrement initial à l'aide du script d'enregistrement CMS/DIS
- Mises à jour automatiques périodiques par le générateur de topologie CMSDISAgent

Exécution de l'enregistrement initial

Pour terminer l'enregistrement initial des éléments de configuration TADDM dans le service de menu contextuel et dans le service d'intégration des données, vous devez exécuter manuellement le script **run_cms_dis_registration**. L'agent générateur de topologie CMSDISAgent met à jour l'enregistrement d'élément de configuration une fois l'enregistrement initial terminé.

Pourquoi et quand exécuter cette tâche

Si vous utilisez un déploiement de serveur de diffusion en continu, exécutez le script d'enregistrement sur le serveur de stockage principal. Si vous utilisez un déploiement de serveur de synchronisation, exécutez le script d'enregistrement sur le serveur de synchronisation.

Procédure

Pour terminer l'enregistrement initial des éléments de configuration TADDM, procédez comme suit :

1. A l'invite de commande, accédez au répertoire `$COLLATION_HOME/bin`.
2. Exécutez le script **run_cms_dis_registration** correspondant à votre système d'exploitation :
   - Systèmes Linux et UNIX :

```
./run_cms_dis_registration.sh [ register [guid] |
                                clean [guid [type_classe]] |
                                re-register-all | register-menu |
                                help ]
```

- Systèmes Windows :

```
run_cms_dis_registration.bat [ register [guid] |
                                clean [guid [type_classe]] |
                                re-register-all | register-menu |
                                help ]
```

Où :

register [*guid*]

Enregistre les données TADDM dans le service de menu contextuel et dans le service d'intégration des données. Vous pouvez éventuellement spécifier l'identificateur global unique (GUID) d'un objet de modèle à enregistrer.

La première fois que vous exécutez le script avec l'option `register` et qu'aucun GUID n'est spécifié, toutes les données TADDM sont enregistrées dans la base de données et tous les points de lancement sont enregistrés auprès du service de menu contextuel. Les exécutions ultérieures utilisant cette option enregistrent uniquement les modifications apportées à TADDM depuis l'exécution précédente. Il s'agit de l'option par défaut.

Si vous avez spécifié un GUID, seul l'objet de modèle associé à ce GUID est enregistré.

Remarque : L'enregistrement initial de toutes les données TADDM peut prendre un long moment.

clean [*guid* [*type_classe*]]

Annule l'enregistrement des données TADDM actuellement présentes dans la base de données.

Si vous ne spécifiez aucun GUID, l'enregistrement de toutes les données TADDM est annulé. Si vous spécifiez un GUID, seul l'enregistrement de l'objet de modèle associé à ce GUID est annulé. Si l'objet de modèle associé au GUID spécifié n'est plus disponible dans TADDM, vous devez également définir le type d'objet de modèle.

re-register-all

Annule l'enregistrement de toutes les données et de tous les points de lancement TADDM, puis répète l'enregistrement initial. Cette option revient à exécuter le script avec l'option `clean`, puis avec l'option `register`.

register-menu

Met uniquement à jour les définitions de menu enregistrées dans la base de données de service de menu contextuel. Utilisez cette option lorsque des données TADDM sont enregistrées mais que vous souhaitez uniquement mettre à jour les définitions de menu.

help

Affiche des informations d'aide sur le script.

Exemple

- Cet exemple enregistre toutes les données TADDM auprès du service de menu contextuel et du service d'intégration des données lors de la première exécution. Lors des exécutions ultérieures, il enregistre toutes les modifications apportées depuis la dernière exécution :

```
./run_cms_dis_registration.sh
```

- Cet exemple enregistre uniquement l'objet de modèle associé au GUID spécifié.
  ```
  ./run_cms_dis_registration.sh register 3950DF835FA0337A829D864415CC1384
  ```
- Cet exemple supprime toutes les données TADDM enregistrées :
  ```
  ./run_cms_dis_registration.sh clean
  ```
- Cet exemple supprime l'objet associé au GUID et au type d'objet de modèle spécifiés :
  ```
  ./run_cms_dis_registration.sh clean 3950DF835FA0337A829D864415CC1384
    LinuxUnitaryComputerSystem
  ```
- Cet exemple supprime toutes les données TADDM enregistrées, puis répète l'enregistrement :
  ```
  ./run_cms_dis_registration.sh re-register-all
  ```

Que faire ensuite

Si vous souhaitez ultérieurement exécuter à nouveau le script d'enregistrement, commencez par désactiver l'agent de générateur de topologie CMSDISAgent pour arrêter les mises à jour incrémentielles. Pour désactiver l'agent, éditez le fichier `$COLLATION_HOME/etc/collation.properties` et définissez la propriété suivante :

```
com.ibm.cdb.DisCmsIntegration.enabled=false
```

Une fois le script terminé, vous devez ensuite réactiver l'agent en définissant la propriété sur `true`.

Configuration de CMSDISAgent

CMSDISagent s'exécute périodiquement en tant qu'agent de générateur de topologie et met à jour l'enregistrement des éléments de configuration TADDM dans Context Menu Service et Data Integration Service en enregistrant les éléments de configuration nouveaux ou modifiés et en annulant l'enregistrement des éléments supprimés.

Pourquoi et quand exécuter cette tâche

S'il est activé, CMDDISAgent commence à s'exécuter une fois que vous avez terminé l'enregistrement initial des éléments de configuration TADDM à l'aide du script **`run_cms_dis_registration`**. Vous pouvez modifier la configuration de l'agent pour modifier le mode d'exécution de l'agent.

Procédure

- Pour activer ou désactiver CMSDISAgent, éditez le fichier `$COLLATION_HOME/etc/collation.properties` et définissez la propriété suivante :
  ```
  com.ibm.cdb.DisCmsIntegration.enabled=valeur
  ```

  où la *valeur* peut être égale à `true` ou `false`. Si elle est définie sur `true`, l'agent s'exécute périodiquement une fois que l'enregistrement initial est terminé. (Cette propriété n'affecte pas le fonctionnement du script **`run_cms_dis_registration`**, qui peut être exécuté à tout moment.)
- Pour personnaliser les éléments de configuration enregistrés dans la base de données, modifiez les fichiers suivants dans le répertoire `$COLLATION_HOME/etc/cmsdis` :

  `classtype-changehistory.list`
  : Répertorie les types d'objet de modèle des éléments de configuration pour lesquels TADDM prend en charge le lancement en contexte pour le rapport d'historique des modifications.

classtype-detailPanel.list
Répertorie les types d'objet de modèle des éléments de configuration pour lesquels TADDM prend en charge le lancement en contexte pour le panneau contenant les détails.

Vous pouvez supprimer tous les types d'objet de modèle non nécessaires aux autres produits pour lancer TADDM en contexte. N'ajoutez aucun autre type à ces fichiers, car TADDM risque de ne pas prendre en charge le lancement en contexte pour ces autres types. Après avoir modifié les fichiers de la liste des types de classe, désactivez l'agent, puis exécutez le script **run_cms_dis_registration** en indiquant l'option `re-register-all`.

Création d'un magasin de bibliothèque de reconnaissance

Un magasin de bibliothèque de reconnaissance est un répertoire ou dossier sur un ordinateur dans le centre de données ; il correspond à l'emplacement courant de tous les adaptateurs de bibliothèque de reconnaissance (DLA) pour écrire les fichiers XML contenant des informations sur les ressources. Les fichiers de données XML à charger en bloc dans un système TADDM sont placés dans ce magasin de bibliothèque de reconnaissance. Pour utiliser le programme de chargement en bloc, vous devez créer un magasin de bibliothèque de reconnaissance.

Avant de commencer

Un adaptateur de bibliothèque de reconnaissance (DLA) est un logiciel qui extrait des données d'une application source comme IBM Tivoli Monitoring ou IBM Tivoli Business Service Manager.

Chaque adaptateur de bibliothèque de reconnaissance écrit des fichiers XML contenant des informations sur les ressources dans un format XML particulier appelé IdML (Identity Markup Language). Les fichiers XML écrits au format IdML sont généralement appelés *livres*. Pour consulter la collection de livres Tivoli que la base de données TADDM peut charger avec des données à partir d'autres produits Tivoli, voir http://www.ibm.com/software/brandcatalog/ismlibrary/.

Les adaptateurs de bibliothèque de reconnaissance sont spécifiques à un produit, car chaque produit possède un mode d'accès distinct aux ressources de l'environnement. La configuration et l'installation d'un adaptateur de bibliothèque de reconnaissance sont différentes pour chaque application. En règle générale, les DLA sont installés sur un système ayant accès aux données d'une application particulière. Par exemple, le DLA de IBM Tivoli Monitoring est installé sur un ordinateur qui dispose d'un accès à la base de données du système de gestion d'entreprise IBM Tivoli Monitoring. Vous pouvez exécuter tous les DLA au moyen de l'interface de ligne de commande et en planifier l'exécution à l'aide d'un programme de planification de votre environnement (cron, par exemple).

Vous pouvez créer un DLA pour extraire des informations de bases de données ou de produits existants de votre environnement.

Pour plus d'informations sur la création d'un adaptateur de bibliothèque de reconnaissance et sur la spécification IdML, ou pour d'autres détails sur le magasin de bibliothèque de reconnaissance, voir le *Guide du développeur de logiciel de l'adaptateur de bibliothèque de reconnaissance* de TADDM.

Pourquoi et quand exécuter cette tâche

En général, le magasin de bibliothèque de reconnaissance se trouve sur le serveur TADDM. Si vous ne le configurez pas sur le serveur TADDM, vous devez vous assurer que le programme de chargement en bloc TADDM qui s'exécute sur ce serveur TADDM peut accéder au magasin. D'autres applications peuvent s'exécuter sur l'ordinateur hébergeant le magasin de bibliothèque de reconnaissance.

Procédure

Pour créer le magasin de bibliothèque de reconnaissance, procédez comme suit :

1. Créez un répertoire pour stocker les fichiers XML sur un ordinateur, avec un nom distinct (par exemple, `c:\IBM\DLFS`). Vous pouvez éventuellement créer des sous-répertoires dans le magasin principal de bibliothèque de reconnaissance pour chaque adaptateur utilisé.
2. Configurez un serveur FTP (File Transfer Protocol) avec au moins un ID utilisateur. Cet ID utilisateur doit disposer des droits suivants: accès en écriture, en renommage et en lecture au répertoire dans lequel les fichiers de bibliothèque de reconnaissance XML sont stockés. Si vous n'utilisez pas FTP pour transférer les fichiers XML au magasin de bibliothèque de reconnaissance, vérifiez que l'outil et l'ID utilisateur que vous employez pour exécuter l'outil ont des droits d'écriture dans le répertoire du magasin de bibliothèque de reconnaissance.
3. Vérifiez que les différents adaptateurs de bibliothèques ont accès au nom du système (nom d'hôte) qui héberge le magasin de bibliothèque de reconnaissance. La plupart des adaptateurs de bibliothèque de reconnaissance copient les fichiers XML dans ce magasin.
4. Assurez-vous que les différents adaptateurs de bibliothèque de reconnaissance disposent de l'ID utilisateur et du mot de passe permettant de se connecter au serveur FTP.
5. Si l'adaptateur de bibliothèque de reconnaissance n'utilise pas le protocole FTP, copiez les fichiers XML (livres) auxquels le programme de chargement en bloc doit avoir accès dans ce répertoire partagé. Le répertoire partagé doit être accessible par le programme de chargement en bloc.

   Il n'incombe pas aux rédacteurs et à l'administrateur d'insérer les livres dans le magasin de bibliothèque de reconnaissance. Configurez par exemple un travail cron pour envoyer les livres IdML produits au magasin de bibliothèque de reconnaissance via le protocole FTP.

Que faire ensuite

Si vous créez un magasin de bibliothèque de reconnaissance et vous souhaitez configurer une base de données TADDM destinée à contenir les livres de l'adaptateur de bibliothèque de reconnaissance, vous pouvez utiliser une unité locale du serveur de domaine comme magasin de bibliothèque de reconnaissance en réseau. Ce répertoire doit être défini dans le fichier `$COLLATION_HOME/etc/bulkload.properties` sur le serveur de domaine où les données ont été chargées. Si plusieurs serveurs de domaine existent, configurez le programme de chargement en bloc correct pour accéder au répertoire partagé correspondant. Le programme de chargement en bloc ne supprime pas les fichiers XML du magasin de bibliothèque de reconnaissance. Vous devez conserver les fichiers dans le magasin de bibliothèque de reconnaissance. Vérifiez que l'espace disque est suffisant sur le serveur pour placer ces fichiers dans le répertoire. Si de nouveaux fichiers XML sont fréquemment ajoutés au répertoire, vous devez régulièrement le vider.

Avec un déploiement de serveur de synchronisation, vous devez choisir l'une des options suivantes :

- Si les ressources référencées dans un livre sont contenues dans les définitions de portée définies sur un serveur de domaine, chargez ce livre sur le serveur de domaine respectif.
- Si les ressources référencées dans un livre ne figurent ***pas*** dans les définitions de portée définies sur un serveur de domaine, chargez tous les livres dans le serveur de synchronisation.

Configuration du lancement selon le contexte

Pour des informations plus détaillées sur les composants dans votre environnement, vous pouvez lancer des vues TADDM depuis d'autres applications Tivoli. Pour configurer votre application afin de lancer des vues TADDM selon le contexte, vous devez indiquer une URL.

Vues que vous pouvez lancer depuis d'autres applications Tivoli

A partir d'autres applications Tivoli, vous pouvez lancer les vues du portail de gestion de données. Vous pouvez aussi lancer le rapport sur les détails et l'historique des modifications pour un élément de configuration concret.

Dans les vues du portail de gestion de données, vous trouverez plus d'informations sur les regroupements de composants suivants :

- Applications métier
- Services métier
- Collections

Si le serveur TADDM et l'application d'où TADDM est lancé ne sont pas configurés pour une connexion unique, une fenêtre de connexion unique s'ouvre. Avant d'afficher plus d'informations dans le portail de gestion de données, vous devez entrer un nom d'utilisateur et un mot de passe.

Définition de l'URL permettant de lancer des vues TADDM

Pour lancer des vues TADDM en contexte à partir d'autres applications Tivoli, vous devez indiquer une URL.

Le format de l'URL pour un lancement en contexte est :

Protocol`://`*TADDMHostname*`:`*TADDMPort*`/`*ContextRoot*`/?`*queryString*

La liste suivante présente les valeurs valides pour chaque variable au format d'URL :

Protocol
Protocole Web à utiliser. Les valeurs valides sont `http` et `https`.

TADDMHostname
Nom d'hôte du serveur TADDM auquel se fait le lancement.

TADDMPort
Numéro de port du serveur TADDM auquel se fait le lancement. La valeur par défaut est `9430`.

ContextRoot
Les valeurs suivantes sont valides :

`cdm/servlet/LICServlet`
Chemin d'accès relatif au servlet Java déployé sur le serveur Apache

Tomcat pour TADDM 7.3.0, et sur le serveur du profil Liberty WAS pour TADDM versions 7.3.0.1 et ultérieures.

cdm/queryHomePage.do
Chemin d'accès relatif à la page d'accueil des requêtes lorsqu'elle est lancée à partir d'IBM Tivoli Monitoring à l'aide d'une connexion unique et en indiquant un texte à rechercher.

queryString
Contient des paramètres de paire nom-valeur délimités par des séparateurs. Le format d'une paire nom-valeur est `nom=valeur`. Utilisez `=` pour séparer les noms des valeurs, et `&` pour séparer les paires.

La liste suivante présente les paires nom-valeur valides pouvant être utilisées dans la variable *queryString* :

view
Indique que vous voulez afficher l'historique des modifications.

La seule valeur valide est `changehistory`.

days_previous
Indique la période (nombre de jours passés) pour laquelle montrer l'historique des modifications d'un élément de configuration concret.

La valeur valide est un entier positif.

hoursback
Indique la période (nombre de jours passés) pour laquelle montrer l'historique des modifications d'un élément de configuration particulier.

La valeur valide est un entier positif.

guid
Indiquez l'identificateur global unique pour un élément de configuration.

Pour le serveur de domaine et le serveur de synchronisation, le tableau 47, à la page 228 répertorie les valeurs admises pour le paramètre `graph` et indique si le paramètre `guid` est facultatif ou obligatoire selon la valeur de graphique respective.

Si le paramètre `graph` est indiqué avec l'une des valeurs suivantes, le paramètre `guid` est facultatif :

- `businessapplications`
- `applicationinfrastructure`
- `physicalinfrastructure`

Si le paramètre `graph` est indiqué avec un autre type de graphique de topologie, le paramètre `guid` est obligatoire.

La valeur valide est une représentation de chaîne valide d'un identificateur global unique, comme illustré dans l'exemple suivant :

```
BA2842345F693855A3165A4B5F0D8BDE
```

Vous devez indiquer un seul GUID pour chaque demande d'URL pour le lancement selon le contexte.

graph
Indique le type de diagramme de topologie à lancer.

Si vous indiquez aussi un élément de configuration en précisant son identificateur global unique dans le paramètre `guid`, l'élément de configuration demandé est sélectionné s'il se trouve dans le graphique de topologie mentionné dans ce paramètre `graph`.

Pour le serveur de domaine et le serveur de synchronisation, le tableau 47 répertorie les valeurs admises pour le paramètre `graph` et indique si le paramètre `guid` est facultatif ou obligatoire selon la valeur de graphique respective.

Tableau 47. Valeurs de graphique valides et leurs relations au paramètre `guid`

	Valeur valide	**Le paramètre `guid` est-il facultatif ou obligatoire avec cette valeur de graph ?**
Serveur de domaine	`businessapplications`	Facultatif
	`applicationinfrastructure`	Facultatif
	`physicalinfrastructure`	Facultatif
	Pour des objets de collection personnalisés : • `ba_infrastructure`	Obligatoire
Serveur de synchronisation	`businessapplications`	Facultatif
	`physicalinfrastructure`	Facultatif
	Pour des objets de collection personnalisés : • `ba_infrastructure`	Obligatoire

Remarque : Les autres types de graphique qui ont été utilisés dans des éditions précédentes de TADDM pour rendre des entités de regroupement particulières par GUID sont obsolètes. Toutefois, pour assurer la compatibilité avec des versions antérieures, si vous indiquez un type de graphique ancien avec un GUID, la demande est redirigée vers le niveau type de topologie.

`username`
Indique le nom d'utilisateur employé pour se connecter à TADDM.

`password`
Indique le mot de passe employé pour se connecter à TADDM.

`launchsource`
La seule valeur valide est `ITM`. Elle est toujours utilisée avec la paire nom-valeur `searchtext=`*`terme_à_rechercher`*.

La recherche est limitée aux éléments de configuration de type ComputerSystem et TMSAgent figurant dans le fichier de configuration `$COLLATION_HOME/etc/cdm/xml/itm_query_components.xml`.

A partir des résultats de la page d'accueil des requêtes, vous pouvez ouvrir les pages suivantes pour chaque élément de configuration répertorié :

- Panneau Historique des modifications
- Panneau Détails
- Portail de gestion de la reconnaissance en affichant le panneau Détails

`searchtext`
Définit le terme à rechercher. Toujours utilisé avec la paire nom-valeur `launchsource=ITM`.

Exemples de définition de l'URL

Les exemples suivants montrent comment définir l'URL pour lancer des vues TADDM :

URL permettant de lancer le portail de gestion de données sans devoir entrer des informations d'autorisation distinctes

```
http://home.taddm.com:9430/cdm/servlet/LICServlet?username=administrator
&password=adminpwd&guid=BA2842345F693855A3165A4B5F0D8BDE
```

Si vous utilisez une connexion sécurisée, vous devez utiliser les autorisations d'accès uniquement dans l'URL pour le lancement en contexte car le nom d'utilisateur et le mot de passe ne sont pas chiffrés.

Adresse URL permettant de lancer la fenêtre de la page d'accueil des requêtes pour IBM Tivoli Monitoring lorsqu'une connexion unique est utilisée et que vous recherchez un élément de configuration correspondant au texte à rechercher.

```
http://home.taddm.com:9430/cdm/queryHomePage.do?launchsource=itm&searchtext=127.0.0.1
```

Adresse URL pour afficher la topologie d'une collection personnalisée indiquée par le paramètre `guid`

```
http://home.taddm.com:9430/cdm/servlet/LICServlet?username=administrator
&password=adminpwd&graph=ba_infrastructure&guid=BA2842345F693855A3165A4B5F0D8BDE
```

Envoi d'événements de modification à des systèmes externes

Vous pouvez configurer TADDM pour avertir un système de gestion d'événements externes lorsque la modification d'une ressource reconnue est détectée.

Pour envoyer des événements de modification depuis TADDM, un ou plusieurs des systèmes de gestion d'événements suivants doivent être installés :

- IBM Tivoli Monitoring 6.2.1 Fixpack 2 ou version ultérieure
- IBM TivoliNetcool/OMNIbus, y compris la sonde EIF (Event Integration Facility)

Pour connaître les versions prises en charge des produits, accédez à la section «Versions prises en charge», à la page 201.

Au terme d'une reconnaissance, TADDM vérifie les modifications apportées aux éléments suivis par des systèmes de gestion d'événements externes. Si des modifications sont détectées, elles sont envoyées directement à IBM Tivoli Netcool/OMNIbus et à IBM Tivoli Monitoring à l'aide de l'agent universel.

L'agent universel convertit les notifications reçues en événements asynchrones et transmet les données au composant IBM Tivoli Enterprise Monitoring Server d'IBM Tivoli Monitoring. IBM Tivoli Monitoring Server stocke les événements et les utilise pour évaluer des situation. Les événements sont ensuite envoyés à IBM Tivoli Enterprise Portal pour affichage.

Les serveurs IBM Tivoli Netcool/OMNIbus traitent les événements reçus en fonction des règles internes et les affichent.

Pour configurer l'envoi d'événements de modification de TADDM à des systèmes de gestion d'événements externes, vous devez activer les événements de modification dans TADDM et configurer chaque destinataire externe pour gérer les événements entrants comme approprié.

Configuration de TADDM en vue de l'envoi des événements de modification

Pour envoyer des événements de modification, vous devez configurer TADDM avec les informations sur les systèmes de gestion d'événements auxquels vous voulez faire ces envois.

Pourquoi et quand exécuter cette tâche

Selon le type de votre déploiement TADDM, apportez les modifications suivantes sur les serveurs TADDM suivants :

- Dans un déploiement de serveur de domaine, apportez les modifications au le serveur de domaine.
- Dans un déploiement de serveur de synchronisation, apportez les modifications au serveur de synchronisation.
- Dans un déploiement de serveur de diffusion en continu, apportez les modifications au serveur de stockage principal.

Procédure

Pour activer l'envoi des informations sur les événements de modification, procédez comme suit :

1. Pour activer les événements de modification, dans le fichier `$COLLATION_HOME/etc/collation.properties`, définissez la propriété suivante : `com.ibm.cdb.omp.changeevent.enabled=true`
2. Pour configurer les ressources faisant l'objet d'un suivi des modifications et à quels systèmes de gestion d'événements les événements sont envoyés, éditez le fichier `$COLLATION_HOME/etc/EventConfig.xml`.

   Pour plus d'informations sur le format que vous devez utiliser pour définir des informations dans le fichier `EventConfig.xml`, voir «Configuration du module de gestion des événements de modification TADDM OMP», à la page 231.

   Lorsque vous mettez TADDM à niveau, le fichier `EventConfig.xml` de la version précédente de TADDM est conservé, de telle sorte que vous ne perdez pas les paramètres personnalisés que vous aviez configurés. Des informations sur les nouvelles fonctions et sur leur utilisation sont disponibles dans le fichier `$COLLATION_HOME/etc/EventConfigDefault.xml`. Le fichier `eventconfigdefault.xml` sert uniquement de référence. Si vous souhaitez utiliser l'une des nouvelles fonctions, vous devez mettre à jour le fichier `eventconfig.xml` en fonction des exemples appropriés présentés dans `eventconfigdefault.xml`.
3. Si vous avez défini un système de gestion d'événements IBMTivoliNetcool/OMNIbus dans le fichier `EventConfig.xml`, créez un fichier de propriétés EIF correspondant pour ce type de système. Pour ce faire, procédez comme suit :
   a. Créez un fichier de propriétés `$COLLATION_HOME/etc/omnibus.eif.properties`.
   b. Personnalisez le fichier `omnibus.eif.properties`. Pour plus d'informations sur la personnalisation d'un fichier de propriétés EIF, voir *Configuring support for TADDM events in your integrated environment* (configuration de la prise en charge des événements TADDM dans votre environnement intégré) disponible à l'emplacement http://www-01.ibm.com/support/knowledgecenter/SSSHTQ_7.4.0/com.ibm.netcool_OMNIbus.doc_7.4.0/omnibus/wip/install/task/omn_con_ext_configuringtaddmevents.html?lang=en dans la documentation d'IBM Tivoli Netcool/OMNIbus.

Configuration du module de gestion des événements de modification TADDM OMP :

Pour permettre l'envoi d'événements de modification, vous devez modifier le fichier `EventConfig.xml` pour définir des programmes d'écoute d'événement et des destinataires.

Programmes d'écoute d'événement

Vous pouvez définir un programme d'écoute en indiquant les critères nécessaires pour une demande TADDM. Les objets sélectionnés par la requête sont vérifiés pour y rechercher des modifications après chaque reconnaissance. Il peut exister plusieurs programmes d'écoute. Pour qu'un événement soit transmis, il doit exister à la fois un programme d'écoute et un groupe de destinataires correspondant.

Utilisez le format suivant pour définir un programme d'écoute :

```
<listener object="[OBJECT_TYPE]"
          enabled="true|false">
          sendCauses="true|false"
          sendOriginGuid="true|false">
   <alert recipient="[RECIPIENT_SYSTEM_NAME]"/>
   <attribute name="[ATTRIBUTE_NAME]" operator="[OPERATOR]">
     <value>
     [ATTRIBUTE_VALUE]
     </value>
   </attribute>
   <causeFilter object="[CAUSEFILTER_OBJECT_TYPE]"
               sendOriginGuid="true|false"/>

 </listener>
```

où :

[OBJECT_TYPE]
: est un type d'objet de modèle représenté dans TADDM, par exemple ComputerSystem ou ITSystem. Pour obtenir d'autres exemples, reportez-vous au dictionnaire de données de TADDM disponible à l'emplacement `http://`*`taddmserverhost`*`:9430/cdm/datadictionary/model-object/index.html`.

enabled
: est un attribut qui permet l'envoi des événements. Cet attribut doit avoir la valeur `true` pour que le programme d'écoute soit actif.

sendCauses
: est un attribut optionnel qui détermine si le programme d'écoute envoie des événements pour les modifications qui ont été propagées à l'objet de modèle. Par exemple, si une modification sur un système d'exploitation Windows entraîne la modification d'un objet ComputerSystem et que l'attribut `sendCauses` a la valeur `true` pour un programme d'écoute de type ComputerSystem, ce programme d'écoute envoie un événement pour notifier le changement à la fois à l'objet ComputerSystem et au système d'exploitation Windows. La valeur par défaut de l'attribut `sendCauses` est `false`.

sendOriginGuid
: est un attribut facultatif utilisé avec l'attribut `sendCauses`. Quand l'attribut `sendOriginGuid` a la valeur `true`, un objet qui correspond au programme d'écoute est considéré comme l'origine logique des changements propagés à l'objet. Les événements liés aux changements propagés qui sont envoyés

contiennent l'identifiant unique de l'objet d'origine. Par exemple, si la modification apportée à un objet ConfigFile entraîne la modification d'un objet ComputerSystem et que les attributs `sendCauses` et `sendOriginGuid` ont tous deux la valeur `true` pour un programme d'écoute de type ComputerSystem, l'événement lié au changement de ConfigFile contient l'identifiant unique de l'objet ComputerSystem en plus de l'identifiant unique de l'objet ConfigFile. Cette fonction est uniquement disponible pour les destinataires d'événement Netcool/OMNIbus. La valeur par défaut de l'attribut `sendOriginGuid` est `false`.

[RECIPIENT_SYSTEM_NAME]
est un destinataire d'alerte. Voir «Destinataires des événements», à la page 234.

[ATTRIBUTE_NAME]
est le nom d'un attribut de `[OBJECT_TYPE ]` qui est analysé.

[OPERATOR]
indique le nom d'opérateur d'une requête MQML de TADDM. Les valeurs possibles sont les suivantes :

Tableau 48. Noms d'opérateur d'une requête MQL TADDM.

Opérateur	Equivalent MQL dans TADDM
contains-with	contains
ends-with	ends-with
equals	equals
greater-or-equal	>=
greater-than	>
less-or-equal	<=
less-than	<
not-equals	not-equals
starts-with	starts-with

[ATTRIBUTE_VALUE]
correspond à la valeur comparée à l'attribut.

<causeFilter>
est un attribut qui permet de filtrer les types d'objets des événements de cause qui sont transmis lorsque l'attribut `sendCauses` est activé. Si vous activez cet attribut, seuls les événements de cause du type d'objet indiqué sont envoyés. Toutefois, les événements propagés sont toujours envoyés, par exemple, ceux qui correspondent au type d'objet spécifié dans le programme d'écoute. Si l'attribut `causeFilter` n'est pas spécifié, tous les événements de cause détectés par le programme d'écoute sont envoyés.

Par exemple, la modification d'un objet WindowsService cause une modification du système d'exploitation Windows et, par voie de conséquence, de l'objet ComputerSystem. Si vous affectez à l'attribut `causeFilter` la valeur WindowsService, seuls les changements de ComputerSystem et WindowsService apparaissent, pas celui du système d'exploitation Windows.

Quand vous définissez l'attribut `causeFilter`, vous pouvez aussi affecter une valeur à l'attribut `sendOriginGuid` si vous le souhaitez. Par défaut, l'attribut `causeFilter` hérite des paramètres de l'attribut `sendOriginGuid` du programme d'écoute parent de l'attribut `causeFilter`. Quand vous utilisez

l'attribut sendOriginGuid dans un attribut causeFilter, cela ne remplace que la valeur de l'attribut causeFilter définie pour le programme d'écoute.

Si vous voulez modifier des objets comme WindowsService ou ConfigFile, dont les changements sont propagés à des objets de plus haut niveau comme ComputerSystem, il est préférable de surveiller ces objets en combinant les attributs sendCauses et causeFilter plutôt que de le faire avec un programme d'écoute séparé.

[CAUSEFILTER_OBJECT_TYPE]
est le nom de classe de l'objet, tel qu'il est défini dans le CDM. Vous pouvez utiliser le nom complet, par exemple com.collation.platform.model.topology.sys.windows.WindowsService, ou le nom abrégé, par exemple WindowsService.

Exemples de programme d'écoute d'événement

Dans l'exemple suivant, toute modification détectée dans un objet ComputerSystem dont le nom de domaine complet contient la chaîne "mycompany" est signalée au destinataire "enterprise-eventhost-itm".

```
    <listener object="ComputerSystem"
enabled="true">
      <alert recipient="enterprise-eventhost-itm"/>
      <attribute name="fqdn" operator="contains-with">
        <value>
         mycompany
        </value>
      </attribute>
    </listener>
```

Dans l'exemple suivant, les modifications apportées à tous les objets d'un type donné sont détectées.

```
      <attribute name="guid" operator="not-equals">
        <value>
         0
        </value>
      </attribute>
```

Dans l'exemple suivant, toute modification détectée dans un objet du type ComputerSystem est signalée au destinataire "enterprise-eventhost-omnibus".

```
    <listener object="ComputerSystem"
enabled="true">
      <alert recipient="enterprise-eventhost-omnibus"/>
      <attribute name="guid" operator="not-equals">
        <value>
         0
        </value>
      </attribute>
    </listener>
```

Dans l'exemple suivant, seules les modifications causées par une modification d'un objet ConfigFile sur un système informatique Linux sont signalées.

```
    <listener object="ITSystem" enabled="true" sendCauses="true">
      <alert recipient="enterprise-eventhost-itm"/>
      <attribute name="name" operator="ends-with">
      <value>
        ShoppingCart
      </value>
```

```
    </attribute>
    <causeFilter object="ConfigFile" />
    <causeFilter object="LinuxUnitaryComputerSystem" />
  </listener>
```

Destinataires des événements

Un destinataire d'événement est une instance d'IBM Tivoli Monitoring ou OMNIBus pouvant recevoir des événements de modification envoyés par le module de gestion des événements de modification. Lorsque des modifications sont détectées par les programmes d'écoute des modifications, des notifications sont envoyées aux destinataires. Vous pouvez définir simultanément plusieurs destinataires du même type ou de types différents. Pour qu'un événement soit transmis, il doit exister à la fois un programme d'écoute et un groupe de destinataires correspondant.

Utilisez le format suivant pour définir un destinataire :

```
<recipient name="[RECIPIENT_NAME]" type="[RECIPIENT_TYPE]">
  <address>[RECIPIENT_FQDN]</address>
  <port>[EVENT_ROUTING_PORT]</port>
  <config>[PATH_TO_EIF_CONFIGURATION]</config>
</recipient>
```

où :

[RECIPIENT_NAME]
: est le nom du système défini comme destinataire dans le programme d'écoute.

[RECIPIENT_TYPE]
: est le type de logiciel utilisé pour la réception des événements. Les types pris en charge sont les suivants :
  - `itm` : IBM Tivoli Monitoring 6 avec Universal Agent POST Data Provider
  - `omnibus` : Netcool/OMNIbus avec adaptateur EIF

[RECIPIENT_FQDN]
: (IBM Tivoli Monitoring uniquement) nom de domaine complet du système hôte où réside Universal Agent

[EVENT_ROUTING_PORT]
: (IBM Tivoli Monitoring uniquement) port utilisé, valeur d'Universal Agent POST Data Provider indiquée dans `KUMENV` sous la forme `KUMP_POST_DP_PORT`

[PATH_TO_EIF_CONFIGURATION]
: (OMNIBUS uniquement) chemin d'accès à la configuration de la fonction d'intégration d'événements (EIF), lu à partir du fichier des propriétés. Utilisez le chemin d'accès absolu du fichier.

Exemples de destinataire d'événement

L'exemple suivant montre comment définir un destinataire d'événement Netcool/OMNIbus.

```
<recipient name="enterprise-eventhost-omnibus" type="omnibus">
  <config>/opt/IBM/taddm/dist/etc/omnibus.eif.properties</config>
</recipient>
```

L'exemple suivant montre comment définir un destinataire d'événement IBM Tivoli Monitoring.

```
<recipient name="enterprise-eventhost-itm" type="itm">
  <address>itm-ua.mycompany.com</address>
  <port>7575</port>
</recipient>
```

Configuration d'IBMTivoliNetcool/OMNIbus

Vous pouvez configurer IBMTivoliNetcool/OMNIbus version 7.3 ou ultérieure pour recevoir des événements de changement envoyés par TADDM. Vous pouvez regrouper et personnaliser les données d'événements apparaissant dans les versions antérieures de Tivoli Netcool/OMNIbus et définir une logique de gestion des événements.

Avant de commencer

Pour configurer IBM Tivoli Netcool/OMNIbus version 7.3 ou ultérieure pour recevoir des événements de changement que TADDM envoie, voir la rubrique *Activation de la prise en charge pour des événements TADDM* dans la documentation IBM Tivoli Netcool/OMNIbus à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html?lang=en. La documentation de Tivoli Netcool/OMNIbus inclut aussi des informations sur le fichier `tivoli_eif_taddm.rules`. Ce fichier renferme la logique pour traiter des détails de changements de configuration détectés lors d'une reconnaissance TADDM.

Dans un environnement où l'informatique à haute disponibilité ou de reprise est utilisée, TADDM peut être configuré pour prendre en charge la reprise automatique. Cette prise en charge se produit quand des événements TADDM sont envoyés à Tivoli Netcool/OMNIbus. Vous pouvez indiquer des adresses EIF principales et secondaires ainsi que les ports associés dans le fichier de propriétés EIF. L'exemple suivant montre à quel endroit ajouter ces propriétés :

```
# Nom de l'hôte où se trouve le palpeur EIF NetCool/OMNIbus.  Entrez jusqu'à 8 emplacements.
# Les emplacements doivent être séparés par une virgule.
# L'événement est envoyé au premier palpeur disponible dans la liste.
# Exemple :
#     ServerLocation=netcool.mycompany.com,netcool2.mycompany.com
ServerLocation=netcool.mycompany.com,netcool2.mycompany.com

# Port sur lequel le palpeur EIF NetCool/OMNIbus écoute.
# Il doit exister une entrée de port pour chaque palpeur indiqué sous ServerLocation.
# Exemple :
#     ServerPort=9998,9998
ServerPort=9998,9998
```

Chaque adresse de palpeur doit avoir le port associé indiqué dans la propriété *ServerPort*. Si le port n'est pas indiqué pour chaque adresse de palpeur, une erreur se produit à l'envoi de l'événement. Quand un événement ne peut pas être envoyé au port principal, il est envoyé au premier port disponible dans la liste. Vous pouvez entrer jusqu'à 8 adresses dans la propriété *ServerLocation*.

Pourquoi et quand exécuter cette tâche

Dans les versions d'IBMTivoliNetcool/OMNIbus antérieures à la version 7.3, le comportement par défaut concerne tous les événements d'un module d'événements à combiner en un seul événement, avec l'attribut Count défini pour afficher le nombre d'événements figurant dans celui combiné. La procédure ci-dessous explique comment modifier ce comportement par défaut.

Procédure

1. Sur le serveur TADDM, ouvrez le fichier suivant pour l'éditer : `$COLLATION_HOME/etc/omnibus.eif.properties`
2. Définissez les valeurs des propriétés TADDMEvent_Slot suivantes:

```
TADDMEvent_Slot_object_name=$TADDM_OBJECT_NAME
TADDMEvent_Slot_change_type=$TADDM_CHANGE_TYPE
TADDMEvent_Slot_change_time=$TADDM_CHANGE_TIME
TADDMEvent_Slot_class_name=$TADDM_CLASS_NAME
TADDMEvent_Slot_attribute_name=$TADDM_ATTRIBUTE_NAME
TADDMEvent_Slot_old_value=$TADDM_OLD_VALUE
TADDMEvent_Slot_new_value=$TADDM_NEW_VALUE
TADDMEvent_Slot_host=$TADDM_HOST
TADDMEvent_Slot_port=$TADDM_PORT
TADDMEvent_Slot_guid=$TADDM_GUID
TADDMEvent_Slot_origin=$TADDM_ORIGIN
```

Que faire ensuite

Si vous rencontrez des problèmes lors de la configuration d'IBM Tivoli Netcool/OMNIbus, voir la rubrique sur les *problèmes liés à l'intégration de TADDM avec d'autres produits* dans le document d'*identification et de résolution des problèmes de TADDM*.

Configuration d'un fournisseur de données IBM Tivoli Monitoring

Vous pouvez configurer le fichier d'initialisation de l'agent universel pour définir un nouveau fournisseur de données.

Avant de commencer

Si vous utilisez Tivoli Monitoring version 6.2.2 ou une version antérieure, vérifiez que le fichier de configuration `KUMPOST` ne contient aucune tabulation ni aucun espace.

Procédure

Pour configurer un fournisseur de données IBM Tivoli Monitoring, procédez comme suit :

Si vous exécutez l'agent universel sur un système Windows, procédez comme suit :

1. Sur le système Windows sur lequel l'agent universel est installé, cliquez sur **Démarrer** > **IBM Tivoli Monitoring** > **Gérer les services Tivoli Monitoring**.
2. Cliquez avec le bouton droit sur l'agent universel et cliquez sur **Reconfigurer**.
3. Dans les deux fenêtres Configuration avancée de l'agent, cliquez sur **OK**.
4. Pour mettre à jour le fichier d'initialisation de l'agent universel, cliquez sur **Oui**. Le fichier KUMENV est ouvert dans l'éditeur de texte système.
5. Définissez la valeur KUMA_STARTUP_DP à `POST`:

   ```
   KUMA_STARTUP_DP=POST
   ```

   Remarque : Si l'agent universel est déjà configuré pour utiliser un autre fournisseur de données, séparez ces valeurs par des virgules, comme illustré dans l'exemple suivant :

   ```
   KUMA_STARTUP_DP=ASFS,POST
   ```
6. Ajoutez les informations sur le paramètre POST au fichier KUMENV :

```
*--------------------------------------*
* TADDM POST DP Parameters *
*--------------------------------------*
KUMP_POST_DP_PORT=7575
KUMP_POST_GROUP_NAME=TADDM
KUMP_POST_APPL_TTL=14400
```

7. Sauvegardez le fichier KUMENV et fermez-le.
8. Pour configurer l'agent, cliquez sur **Oui**.
9. Dans la fenêtre Gérer les services Tivoli Enterprise Monitoring, cliquez sur **Universal Agent** > **Démarrer**.
10. Dans l'éditeur de texte système, créez un fichier texte. Entrez les informations suivantes dans le fichier :

```
//APPl CONFIGCHANGE
//NAME dpPost E 3600
//ATTRIBUTES ';'
Post_Time T 16 Caption{Time}
Post_Origin D 32 Caption{Origination}
Post_Ack_Stamp D 28 Caption{Event time stamp}
Comp_Type D 512 Caption{Component type}
Comp_Name D 512 Caption{Component name}
Comp_Guid D 512 Caption{Component GUID}
Change_Type D 512 Caption{Change type}
Chg_Det_Time D 512 Caption{Change detection time}
Chg_Attr D 512 Caption{Changed attribute}
Srv_Addr D 512 Caption{TADDM server}
Srv_Port D 16 Caption{TADDM port}
```

11. Sauvegardez le fichier en tant que %ITM_HOME%\TMAITM6\metafiles\KUMPOST.

    Remarque : Vérifiez que vous entrez le nom du fichier en majuscules (KUMPOST).
12. Ouvrez une invite de commande Windows et naviguez jusqu'au dossier %ITM_HOME%\TMAITM6.
13. Exécutez le programme KUMPCON.exe pour valider et importer le métafichier KUMPOST.
14. Dans la fenêtre Gérer les services Tivoli Monitoring, cliquez avec le bouton droit sur l'agent universel et sélectionnez **Recycler**.

Si vous exécutez l'agent universel sur un système Linux ou UNIX, procédez comme suit :

1. Reconfigurez l'agent universel à l'aide de la commande suivante :

   ```
   itmcmd config –A um
   ```

   Quand un message vous demande le fournisseur de données, entrez POST.

   Remarque : Si l'agent universel est déjà configuré pour utiliser un autre fournisseur de données, séparez ces deux valeurs par une virgule (par exemple ASFS,POST).
2. Faites une copie de sauvegarde du fichier um.ini dans le répertoire $ITM_HOME/config et ajoutez les entrées suivantes à la copie d'origine du fichier :

   ```
   # TADDM POST DP Parameters
   KUMP_POST_DP_PORT=7575
   KUMP_POST_GROUP_NAME=TADDM
   KUMP_POST_APPL_TTL=14400
   ```
3. Dans le répertoire $ITM_HOME/*interp*/um/metafiles, créez un fichier texte. Entrez les informations suivantes dans le fichier :

```
//APPl CONFIGCHANGE
//NAME dpPost E 3600
//ATTRIBUTES ';'
Post_Time T 16 Caption{Time}
Post_Origin D 32 Caption{Origination}
Post_Ack_Stamp D 28 Caption{Event time stamp}
Comp_Type D 512 Caption{Component type}
Comp_Name D 512 Caption{Component name}
Comp_Guid D 512 Caption{Component GUID}
Change_Type D 512 Caption{Change type}
Chg_Det_Time D 512 Caption{Change detection time}
Chg_Attr D 512 Caption{Changed attribute}
Srv_Addr D 512 Caption{TADDM server}
Srv_Port D 16 Caption{TADDM port}
```

4. Sauvegardez le fichier en tant que KUMPOST.

   Remarque : Vérifiez que vous entrez le nom du fichier en majuscules (KUMPOST).

5. Redémarrez l'agent universel à l'aide des commandes suivantes :

   ```
   itmcmd agent stop um
   ```

   ```
   itmcmd agent start um
   ```

6. Pour valider et régénérer le métafichier KUMPOST, procédez comme suit :
   a. Exécutez la commande $ITM_HOME/bin/um_console avec les paramètres suivants :

      ```
      um_console -h <ITM directory>
      ```

   b. Sur la ligne de commande, entrez le texte suivant :

      ```
      validate KUMPOST
      ```

      Des messages similaires aux suivants s'affichent :

      ```
      KUMPS001I Console input accepted.
      KUMPV025I Processing input metafile /opt/IBM/ITM//lx8266/um/metafiles/KUMPOST
      KUMPV026I Processing record 0001 -> //APPl CONFIGCHANGE
      KUMPV148I Note: APPL names starting with letters A-M are designated for
      Best Practices and Business Partner UA solutions.
      KUMPV026I Processing record 0002 ->     //NAME dpPost E 3600
      KUMPV026I Processing record 0003 ->     //ATTRIBUTES ';'
      KUMPV026I Processing record 0004 -> Post_Time T 16 Caption{Time}
      KUMPV026I Processing record 0005 -> Post_Origin D 32 Caption{Origination}
      KUMPV026I Processing record 0006 -> Post_Ack_Stamp D 28 Caption{Event time stamp}
      KUMPV026I Processing record 0007 -> Comp_Type D 512 Caption{Component type}
      KUMPV026I Processing record 0008 -> Comp_Name D 512 Caption{Component name}
      KUMPV026I Processing record 0009 -> Comp_Guid D 512 Caption{Component GUID}
      KUMPV026I Processing record 0010 -> Change_Type D 512 Caption{Change type}
      KUMPV026I Processing record 0011 -> Chg_Det_Time D 512 Caption{Change detection time}
      KUMPV026I Processing record 0012 -> Chg_Attr D 512 Caption{Changed attribute}
      KUMPV026I Processing record 0013 -> Srv_Addr D 512 Caption{TADDM server}
      KUMPV026I Processing record 0014 -> Srv_Port D 16 Caption{TADDM port}
      KUMPV000I Validation completed successfully
      KUMPV090I Application metafile validation report saved in file
      /opt/IBM/ITM//lx8266/um/metafiles/KUMPOST.rpt.
      ```

   c. Lorsque vous êtes invité à effectuer l'opération souhaitée sur le métafichier, entrez le texte suivant :

      ```
      Refresh
      ```

   d. Entrez Yes pour confirmer.

Que faire ensuite

Pour vérifier que la configuration de l'agent universel a abouti, consultez le rapport sur les événements de modification dans Tivoli Enterprise Portal.

Pour ouvrir le rapport des événements de modification à l'aide d'IBM Tivoli Monitoring 6.2.1 ou une version ultérieure, procédez comme suit :

1. Accédez à l'agent universel configuré pour envoyer et recevoir des notifications d'événements à partir de TADDM.
2. Développez le noeud CONFIGCHANGE.
3. Cliquez sur le noeud **DPPOST**.

Création des situations de modification de la configuration dans IBM Tivoli Monitoring

Vous pouvez utiliser la fonction Situation de Tivoli Enterprise Portal pour surveiller les événements de modification et déclencher des situations basées sur les informations d'un événement de modification.

Procédure

Pour créer une situation de modification de la configuration dans IBM Tivoli Monitoring, procédez comme suit :

Pour créer une situation de modification de la configuration dans IBM Tivoli Monitoring 6.2.1, procédez comme suit :

1. Dans le panneau Navigateur d'IBM Tivoli Enterprise Portal, accédez à l'agent universel configuré pour envoyer et recevoir des notifications d'événements provenant de TADDM.
2. Développez le noeud CONFIGCHANGE.
3. Cliquez avec le bouton droit de la souris sur le noeud DPPOST. Cliquez sur **Situations**.
4. Dans la fenêtre des «situations pour *nom_noeud*», cliquez avec le bouton droit sur la zone **Universal Data Provider**. Cliquez sur **Créer un nouveau**. La fenêtre de création d'une situation ou règle s'affiche.
5. Dans la zone **Nom**, entrez le nom de la situation. Par exemple, `ConfigurationChanged`.
6. Dans la zone **Description**, entrez la description de la situation. Par exemple, `Une modification de l'objet suivi a été détectée par TADDM`.
7. Dans la liste **Application surveillée**, sélectionnez **Universal Data Provider**.
8. Vérifiez que la case **Correlate Situations across Managed Systems** est décochée.
9. Cliquez sur **OK**. La fenêtre «Sélectionner une condition» s'affiche.
10. Dans la liste **Groupe d'attributs**, sélectionnez **DPPOST**.
11. Dans la liste **Elément d'attribut**, sélectionnez **Nom de composant**.
12. Cliquez sur **OK**. L'onglet **Formule** pour la situation s'affiche.
13. Configurez la situation pour qu'elle se déclenche quand le nom du composant correspond à celui de la ressource dans l'environnement que vous voulez surveiller.
14. Cliquez sur **OK**.

Pour créer une situation de modification de la configuration dans IBM Tivoli Monitoring 6.2.2 ou une version ultérieure, procédez comme suit :

1. Dans le panneau Navigateur d'IBM Tivoli Enterprise Portal, accédez à l'agent universel configuré pour envoyer et recevoir des notifications d'événements provenant de TADDM.
2. Développez le noeud CONFIGCHANGE.

3. Cliquez avec le bouton droit de la souris sur le noeud DPPOST. Cliquez sur **Situations**.
4. Dans la fenêtre des «situations pour *nom_noeud*», cliquez sur la zone de **création d'une situation**. La fenêtre de création d'une situation s'affiche.
5. Dans la zone **Nom**, entrez le nom de la situation. Par exemple, `ConfigurationChanged`.
6. Dans la zone **Description**, entrez la description de la situation. Par exemple, `Une modification de l'objet suivi a été détectée par TADDM`.
7. Dans la liste **Application surveillée**, sélectionnez **Universal Data Provider**.
8. Cliquez sur **OK**. La fenêtre «Sélectionner une condition» s'affiche.
9. Dans la liste **Groupe d'attributs**, sélectionnez **DPPOST**.
10. Dans la liste **Elément d'attribut**, sélectionnez **Nom de composant**.
11. Cliquez sur **OK**. L'onglet **Formule** pour la situation s'affiche.
12. Configurez la situation pour qu'elle se déclenche quand le nom du composant correspond à celui de la ressource dans l'environnement que vous voulez surveiller.
13. Cliquez sur **OK**.
14. Dans le volet de navigation d'IBM Tivoli Enterprise Portal, cliquez avec le bouton droit sur le noeud contenant le rapport sur les événements de modification. Cliquez sur **Situations**.
15. Dans la fenêtre des «situations pour *nom_noeud*», cliquez avec le bouton droit de la souris sur la situation **ConfigurationChanged** que vous avez créée et cliquez sur l'option permettant de **démarrer une situation**.

Résultats

Lorsque des événements de modification de la configuration sont reçus, leur nom de composant est vérifié. Si le nom du composant correspond à celui indiqué dans la formule de la situation, la situation configurée est déclenchée.

Création de liens détaillés dans les rapports sur les événements de modification de la configuration dans IBM Tivoli Monitoring

Vous pouvez créer des liens dans un tableau de rapport vers un espace de travail qui affiche l'historique des modifications et des détails directement depuis le serveur TADDM. Ces liens fournissent des informations plus détaillées que celles figurant dans un rapport.

Procédure

Pour créer un lien, dans un rapport sur les événements de modification de la configuration, à des informations plus détaillées sur ces événements, procédez comme suit :

1. Pour créer un espace de travail dans lequel afficher les informations, procédez comme suit :
   a. Dans le panneau Navigateur, cliquez avec le bouton droit sur le noeud devant contenir l'espace de travail. Cliquez sur **Fichier** > **Enregistrer l'espace de travail en tant que**. La fenêtre Enregistrer l'espace de travail en tant que s'ouvre.
   b. Dans la zone **Nom**, entrez le nom de l'espace de travail. Par exemple, `ConfigChangeDetails`.

c. Dans la zone **Description**, entrez une description de l'espace de travail. Par exemple, `Espace de travail générique pour le tableau des événements de modification`.
d. Cochez la case **Uniquement sélectionnable en tant que cible d'un Lien espace de travail**.
e. Cliquez sur **OK**.

2. Pour configurer l'espace de travail à l'aide d'IBM Tivoli Monitoring 6.2.1 ou d'une version ultérieure, procédez comme suit :
   a. Configurez l'espace de travail pour obtenir un panneau de navigateur et deux panneaux d'explorateur.
   b. Cliquez sur **Editer** > **Propriétés**.
   c. Dans le panneau Navigateur, sélectionnez la première instance de **Guide de démarrage**.
   d. Dans le panneau Style, sélectionnez **Utiliser l'emplacement fourni**.
   e. Cliquez sur **OK**.
   f. Dans la zone **Emplacement** de l'un des deux panneaux de l'explorateur, entrez l'URL de la vue Historique des modifications dans TADDM. Une fois l'URL entrée sur une seule ligne, n'appuyez pas sur **Entrée**.

      ```
      http://$taddm_server$:$taddm_port$/cdm/servlet/
      LICServlet?view=changehistory&hoursback=10000&console=web&guid=$taddm_guid$
      ```

      Le paramètre `hoursback` indique le nombre d'heures pendant lesquelles les événements de modification sont affichés. Par exemple, si vous paramétrez `hoursback` sur 6, tous les événements de modification s'étant produits dans les 6 dernières heures s'affichent.
   g. Dans le panneau Navigateur, sélectionnez la seconde instance de **Guide de démarrage**.
   h. Dans le panneau Style, sélectionnez **Utiliser l'emplacement fourni**.
   i. Cliquez sur **OK**.
   j. Dans la zone **Emplacement** de le second panneau d'explorateur, entrez l'URL de la vue de détails sur les objets dans TADDM. Une fois l'URL entrée sur une seule ligne, n'appuyez pas sur **Entrée**.

      ```
      http://$taddm_server$:$taddm_port$/cdm/servlet/LICServlet?console=web
      &guid=$taddm_guid$
      ```
   k. Pour sauvegarder le nouvel espace de travail, cliquez sur **Fichier** > **Save**.

   Juste après avoir entré l'URL dans la zone **Emplacement**, n'appuyez pas sur **Entrée**, mais sauvegardez l'espace de travail.
3. Ouvrez IBM Tivoli Enterprise Portal. Dans le panneau Rapport, cliquez avec le bouton droit sur une ligne dans le tableau**Rapport**.
4. Cliquez sur **Lien vers** > **Assistant Liens**. La page d'accueil de l'assistant Lien Espace de travail s'affiche.
5. Cliquez sur **Créer un nouveau lien**. Cliquez sur **Suivant**. La page Nom du lien de l'assistant Lien Espace de travail s'affiche.
6. Dans la zone **Nom**, entrez le nom du lien. Par exemple, `Afficher les détails`.
7. Dans la zone **Description**, entrez une description du lien. Par exemple, `Lien vers des détails`.
8. Cliquez sur **Suivant**. La page Type de lien de l'assistant Lien Espace de travail s'affiche.

9. Cliquez sur **Absolu**. Cliquez sur **Suivant**. La page Espace de travail cible de l'assistant Lien Espace de travail s'affiche.
10. Dans le panneau Navigateur, sélectionnez le noeud contenant l'espace de travail créé. Dans le panneau Espace de travail, sélectionnez l'espace de travail créé.
11. Cliquez sur **Suivant**. La page Paramètres de l'assistant Lien Espace de travail s'affiche.
12. Vous devez ajouter trois symboles : "taddm_server", "taddm_port" et "taddm_guid". Pour ajouter un symbole, procédez comme suit :
    a. Cliquez sur **Ajouter un symbole**. La fenêtre Ajouter un symbole s'affiche.
    b. Dans la zone **Symbole**, entrez le nom du symbole.
    c. Cliquez sur **OK**.
13. Vous devez lier chaque symbole créé à un attribut représentant la colonne correcte dans le rapport.
    - Liez le symbole "taddm_server" à l'attribut du TADDM server.
    - Liez le symbole "taddm_port" au numéro de port de la console Web TADDM.
    - Liez le symbole "taddm_guid" à l'attribut Component GUID.

    Pour lier un symbole à un attribut, procédez comme suit :
    a. Dans la page Paramètres de l'assistant Lien Espace de travail, sélectionnez le symbole que vous voulez lier à une colonne du rapport.
    b. Cliquez sur **Modifier une expression**. La fenêtre Editeur d'expression s'ouvre.
    c. Cliquez sur **Symbole**. La fenêtre Symboles s'ouvre.
    d. Naviguez jusqu'à **Attributs** et sélectionnez l'attribut que vous voulez lier au symbole. Cliquez sur **OK**.
    e. Dans la fenêtre Editeur d'expression, cliquez sur **OK**. La page Paramètres de l'assistant Lien Espace de travail s'affiche.
14. Cliquez sur **Suivant**. La page Récapitulatif de l'assistant Lien Espace de travail s'affiche.
15. Cliquez sur **Terminer**.

Résultats

Si votre rapport sur les événements de modification comportent des événements actifs, une icône de lien apparaît à côté de chaque ligne du tableau. Pour passer à l'espace de travail cible, cliquez sur l'icône de lien et sélectionnez **Afficher les détails**. Dans la ligne, les valeurs sont remplacées par des symboles. Dans l'espace de travail, les panneaux Historique des modifications et de détails sur les objets sont lancés en contexte.

Configuration des événements de modification pour un système métier

Vous pouvez utiliser la fonctionnalité d'événements de modification pour envoyer un événement de modification chaque fois que change le système métier.

Pourquoi et quand exécuter cette tâche

Par défaut, TADDM n'indique pas un système métier comme changé si l'un des ordinateurs dont il dépend a changé.

Procédure

Pour permettre l'envoi d'événements de modification pour des systèmes métier, procédez comme suit :

1. Ouvrez le fichier `$COLLATION_HOME/etc/propagationserver.xml` dans l'éditeur approprié.
2. Dans la section Système informatique, pour les éléments de relation de l'application et du système métier, définissez la valeur de l'attribut `enabled` à `true`. Par exemple :

```
<relationship enabled="true" source="sys.ComputerSystem" attribute="groups"
target="app.Application" targetAttribute="true"
collectionType="app.FunctionalGroup" radius="1"/>

<relationship enabled="true" source="sys.ComputerSystem" attribute="components"
target="sys.BusinessSystem" targetAttribute="true"/>
```

3. Redémarrez TADDM.
4. Créez un programme d'écoute pour le système métier dans la configuration d'événements de modification `$COLLATION_HOME/etc/EventConfig.xml`. Dans l'exemple suivant, le destinataire des événements est `mycompany-itm`, et le nom du système métier est `MyBiz`.

```
<listener object="ITSystem" enabled="true">
 <alert recipient="mycompany-itm"/>
 <attribute name="name" operator="equals">
  <value>MyBiz</value>
 </attribute>
</listener>
```

Planification des travaux à l'aide d'IBM Tivoli Workload Scheduler

Vous pouvez utiliser IBM Tivoli Workload Scheduler pour planifier des travaux dans TADDM. IBM Tivoli Workload Scheduler est un outil d'automatisation des logiciels constituant l'élément central de la gestion et de la surveillance automatisées de la charge de travail.

Utilisez IBM Tivoli Workload Scheduler 8.5.1 ou une version ultérieure. Vous devez installer le gestionnaire de domaine maître et l'agent de tolérance aux pannes sur le serveur TADDM. Pour plus d'informations sur l'installation et la configuration de Tivoli Workload Scheduler, voir http://www-01.ibm.com/support/knowledgecenter/SSGSPN_8.5.1.1/com.ibm.tivoli.itws.doc_8.5.1.1/ic-homepage.html?lang=en. Les objets de planification sont gérés par le composeur de ligne de commande et sont stockés dans Tivoli Workload Scheduler.

Les travaux Tivoli Workload Scheduler utilisent le script `invokejob.sh` pour exécuter l'opération requise. Le script `invokejob.sh` est fourni par l'installation TADDM.

Les paramètres suivants sont communs à toutes les utilisations de ce script :

Obligatoire : -u *utilisateur*
: Cette valeur définit l'utilisateur qui exécute la commande API.

Obligatoire : -p *mot_de_passe*
: Cette valeur définit le mot de passe qui authentifie l'utilisateur.

Obligatoire : --profile *profil*
: Cette valeur définit le profil de reconnaissance.

Facultatif : -H *hôte*
Cette valeur définit le nom d'hôte du serveur. Le nom par défaut est `localhost`. Si vous utilisez le paramètre **-T**, vous devez également spécifier le paramètre **-H**.

Facultatif : -P *port*
Cette valeur définit le port du serveur TADDM. La valeur par défaut est `9433`.

Facultatif : -v *version*
Cette valeur définit le nom ou le numéro de la version. La valeur par défaut est `0`.

Facultatif : -t *délai d'expiration*
Cette valeur définit le temps écoulé avant l'interruption automatique de l'exécution du travail.

Facultatif : -T | --truststorefile *magasincléscertifiées*
Cette valeur indique l'emplacement du fichier de magasin de clés certifiées, `jssecacerts.cert`, avec un certificat pour la connexion au serveur TADDM. Ce paramètre est requis pour la connexion sécurisée à TADDM. Si vous utilisez ce paramètre, vous devez également spécifier le paramètre **-H**.

Pour planifier un travail, procédez comme suit :

1. Dans Tivoli Workload Scheduler, entrez le fichier de définition du travail TADDM dans un fichier d'édition. L'exemple suivant illustre un modèle de définition de travail :

   ```
   WORKSTATION_ID#TADDM_JOB
    SCRIPTNAME "./opt/IBM/taddm/dist/bin/invokejob.sh -u
   ^NOM_UTILISATEUR_TADDM^ -p ^MOT_DE_PASSE_TADDM^ commande [paramètres]"
    STREAMLOGON taddmuser
    TASKTYPE UNIX
    RECOVERY STOP
   ```

   ^*NOM_UTILISATEUR_TADDM*^ et ^*MOT_DE_PASSE_TADDM*^ sont des variables qui doivent être définies dans Tivoli Workload Scheduler. Ces variables sont mappées vers des valeurs stockées dans la base de données. Pour des raisons de sécurité, utilisez des variables, notamment lors du codage des mots de passe, pour vous assurer que ces valeurs ne soient pas visibles en tant que texte.
2. Utilisez le composeur pour ajouter le fichier d'édition à la base de données.
3. Ajoutez le travail à un flot de travaux et planifiez l'exécution de ce flot. L'agent IBM Tivoli Workload Scheduler démarre et surveille l'action du script `invokejob.sh`.

Planification d'un travail de reconnaissance

L'exemple suivant exécute une reconnaissance sur la portée 127.0.0.1 :

```
dist/bin/invokejob.sh -u USER -p PASSWORD --timeout 60000 discover start
--profile  "Level 3 Discovery" 127.0.0.1
```

L'exemple suivant exécute une reconnaissance sur l'ensemble de portées MyScopeSet, qui doit déjà exister dans la liste des portées :

```
dist/bin/invokejob.sh -u USER -p PASSWORD --timeout 60000 discover start
--profile "Level 3 Discovery" MyScopeSet
```

Dans les exemples précédents, le dernier paramètre définit la portée ou l'ensemble de portées à inclure lors de l'exécution de la reconnaissance. Le paramètre **profile** est obligatoire. Le paramètre **name**, qui définit le nom de l'exécution de la reconnaissance, est facultatif.

La commande suivante est un exemple de la marche à suivre pour arrêter une reconnaissance en cours d'exécution :

```
dist/bin/invokejob.sh -u USER -p PASSWORD --timeout 60000 discover stop
```

La commande **discover stop** n'accepte aucun autre argument.

Planification d'un travail de synchronisation de domaine

L'exemple suivant illustre la syntaxe et les options de ligne de commande permettant au script TADDM `invokejob.sh` d'exécuter une synchronisation de domaine dans un déploiement de serveur de synchronisation :

```
dist/bin/invokejob.sh -u USER -p PASSWORD --timeout 60000 sync start TestDomain
```

Les commandes **sync start** et **sync stop** requièrent un argument correspondant au nom de domaine pour lequel la synchronisation doit démarrer ou être arrêtée.

Intégration de TADDM à IBM Tivoli Business Service Manager

Selon les tâches spécifiques que vous devez réaliser dans votre environnement informatique, vous pouvez utiliser les fonctionnalités d'intégration qui sont disponibles entre TADDM et IBM Tivoli Business Service Manager. Pour utiliser ces fonctions, vous devez disposer du correctif provisoire 3 d'IBM Tivoli Business Service Manager 4.2.1, mais aucune configuration supplémentaire de TADDM n'est requise.

Mise à jour de l'état de cycle de vie des applications métier

Vous pouvez utiliser l'état de cycle de vie pour filtrer les objets en vue de leur synchronisation dans IBM Tivoli Business Service Manager à partir de TADDM. Vous pouvez utiliser le programme **BusinessServiceLifecycle** pour répertorier les informations relatives à une application métier ou pour définir l'état de cycle de vie d'une application métier.

L'application IBM Tivoli Business Service Manager ITsystems inclut uniquement des applications métier. C'est pour cette raison que le programme **BusinessServiceLifecycle** ne prend en charge que les applications métier.

Le programme **businessservicelifecycle** se trouve à l'emplacement suivant :

- Pour les systèmes d'exploitation Linux et UNIX, le script `businessservicelifecycle` se trouve dans le répertoire `$COLLATION_HOME/bin`.
- Pour les systèmes d'exploitation Windows, le fichier de traitement `BusinessServiceLifecycle.bat` se trouve dans le dossier `%COLLATION_HOME%\bin`.

Utilisez le programme **BusinessServiceLifecycle** avec les options de ligne de commande suivantes :

```
BusinessServiceLifecycle -u nom_utilisateur_TADDM -p mot_de_passe_TADDM -l | -s GUID état
```

Utilisez l'option `-l` pour répertorier les informations sur le cycle de vie de l'application métier ou utilisez l'option `-s` avec un paramètre GUID et un paramètre de code d'état pour définir un état de cycle de vie. Il est impossible d'utiliser simultanément l'option `-l` et l'option `-s`.

Le tableau suivant recense les codes d'état valides :

Tableau 49. Codes d'état

Code	Etat
0	Inconnu
1	Autre
2	Ordonné
3	Reçu
4	En test
5	Testé
6	Installé
7	Activé
8	Désactivé
9	Maintenance
10	Retiré
11	Archivé
12	Accepté
13	Compilation
14	Développement
15	Brouillon
16	Inventaire
17	Hors ligne
18	Postproduction
19	Production
20	Prêt à la production
21	Sunset
22	Valider

Intégration de TADDM à Jazz for Service Management

TADDM prend en charge l'intégration aux plateformes Open Services for Lifecycle Collaboration (OSLC). OSLC, lorsqu'il est utilisé avec TADDM, vous permet d'obtenir des données de reconnaissance présentées sous la forme de définitions de ressources standard. La plateforme Jazz for Service Management est un outil d'intégration IBM qui repose sur les spécifications de la communauté ouverte OSLC.

Jazz for Service Management fournit un point unique de configuration et d'administration pour tous les produits Tivoli et bien d'autres. Jazz for Service Management montre une vue de bout en bout des ressources informatiques, de l'application et des relations commerciales.

Communication REST OSLC TADDM

Le service Representational State Transfer (REST) TADDM fournit une intégration OSLC dans un certain nombre de flux REST OSLC. Le service spécifie les types de média renvoyés lorsqu'il est exécuté et décrit les aspects de sécurité connectés au service.

Common Resource Type Vocabulary (CRTV) est un modèle de données défini par la communauté OSLC et IBM pris en charge par TADDM, avec le modèle de données commun Tivoli (Common Data Model, CDM). La prise en charge de TADDM pour OSLC rend les données de reconnaissance CDM disponibles sous la forme de ressources définies par CRTV.

Interface REST OSLC :

Une interface REST est disponible dans TADDM pour Open Services Lifecycle Collaboration (OSLC). Vous pouvez utiliser l'interface REST OSLC pour obtenir des informations relatives aux éléments de configuration enregistrés, à leurs attributs et à l'historique des changements.

Vous pouvez obtenir des informations sur les attributs d'élément de configuration uniquement si les attributs sont pris en charge par Common Resource Type Vocabulary (CRTV) ou TADDM vocabulary.

Chaque requête valide doit contenir un identificateur global unique identifiant l'élément de configuration concret.

Il existe deux types de service :

Service de configuration
Ce service fournit une interface permettant d'extraire des attributs étendus pour une ressource CRTV.

Service d'historique des changements
Ce service offre une interface permettant d'extraire un historique des changements pour une durée ou une ressource CRTV spécifiée.

Pour chaque service, il est possible d'afficher les trois types de contenu suivants :

- Représentation RDF
- Affichage compact OSLC
- Affichage HTML

L'URL suivante est l'adresse de base :

`http[s]://`*`taddm_host`*`:`*`port`*`/cdm/oslc/`*`provider_name`*`/`*`ci_guid`*

où

- *port* est le port sur lequel le serveur Tomcat (TADDM 7.3.0) ou le serveur du profil Liberty WAS (TADDM versions 7.3.0.1 et ultérieures) est en mode écoute. La valeur par défaut est 9430.
- *provider_name* est associé à l'une des deux valeurs suivantes, en fonction du service que vous souhaitez utiliser :
  - `configuration`
  - `changehistory`
- *ci_guid* est l'ID de l'élément de configuration dans TADDM

Pour afficher l'aperçu HTML pour un élément de configuration, utilisez l'URL suivante :

- `http[s]://`*`taddm_host`*`:`*`port`*`/cdm/oslc/`*`provider_name`*`/`*`ci_guid`*`/preview`

L'interface REST OSLC accepte uniquement les demandes HTTP GET. Vous pouvez utiliser l'en-tête Accept HTTP pour spécifier le type de contenu renvoyé.

Pour afficher la vue compacte OSLC pour l'élément de configuration donné, spécifiez l'en-tête Accept suivant :

```
application/x-oslc-compact+xml
```

Pour afficher la représentation RDF de l'élément de configuration donné, spécifiez l'en-tête Accept suivant :

```
application/rdf+xml
```

Il s'agit du comportement par défaut lorsqu'aucune valeur n'est fournie pour l'en-tête Accept.

Affichage compact OSLC :

L'affichage compact OSLC est une représentation XML de ressource cible.

L'affichage compact OSLC est un aperçu fourni par l'interface REST (Representational State Transfer Rational) OSLC. Pour afficher un aperçu de ressource cible, une représentation des ressources, tel que défini dans la spécification OSLC, doit être fournie par le fournisseur.

Pour utiliser une représentation de la ressource, émettez une requête HTTP GET vers l'identificateur URI de la ressource cible avec l'en-tête Access `application/x-oslc-compact+xml`.

Si le fournisseur prend en charge le mécanisme de prévisualisation, il répond par une représentation compacte incluant les informations que le client peut utiliser pour afficher les liens et un aperçu de la ressource cible.

Aperçu HTML Jazz for Service Management :

Jazz for Service Management Registry Services offre une interface utilisateur HTML pour distribuer des informations sur les éléments enregistrés à partir des systèmes externes connectés.

Tous les éléments contenant des données fournies par TADDM contiennent un aperçu HTML offrant une présentation rapide des données de l'élément sélectionnées directement à partir d'un serveur TADDM.

TADDM fournit Jazz for Service Management avec un service de flux à l'adresse suivante :

```
http[s]://nom_hôte:port/cdm/oslc/configuration/guid/preview
```

où *nom_hôte* et *port* sont le nom d'hôte et le numéro de port du serveur TADDM et où *guid* est l'identificateur d'élément unique.

L'URL affiche une page contenant une présentation de l'élément sélectionné. La page s'affiche automatiquement dans l'interface utilisateur de Jazz for Service Management.

Le contenu de la page est semblable à l'onglet General (Général) de la vue Inventory Summary Details (Détails du récapitulatif de l'inventaire) du portail de gestion de données TADDM.

Sécurité :

Il est possible de configurer TADDM afin que l'accès aux flux fourni par l'interface REST OSLC requière l'authentification.

Pour accéder à l'interface REST, vous devez vous authentifier à l'aide de l'une des méthodes suivantes :

Authentification HTTP de base
Les données d'identification doivent être placées dans l'en-tête de requête d'autorisation. La valeur de cet en-tête doit se conformer aux règles d'authentification HTTP de base.

Connexion unique
En cas de connexion unique, toutes les requêtes envoyées à l'interface REST doivent contenir un jeton LTPA (Lightweight Third-Party Authentication). Pour vérifier le jeton, TADDM doit être configuré pour utiliser WebSphere Virtual Member Manager (VMM) comme référentiel d'utilisateur.

Pour plus d'informations sur la configuration de VMM, voir «Configuration du serveur TADDM en vue de l'utilisation des référentiels fédérés WebSphere», à la page 28.

Pour que les flux demandés soient affichés sans authentification, la propriété suivante du fichier `collation.properties` doit être configurée avec une URL valide des services de registre :

`com.ibm.cdb.topobuilder.integration.oslc.frsurl`

Puis, un nom d'utilisateur et un mot de passe pré-configurés sont utilisés si aucune donnée d'identification valide n'est incluse dans la demande.

Le nom d'utilisateur et le mot de passe sont extraits du fichier descripteur de déploiement `web.xml` de l'application Common Data Model. Vous pouvez configurer cette personnalisation à l'aide des paramètres init OSLCFilter suivants :

OSLC_LOGIN_OFF
Si ce paramètre est défini sur `true`, le nom d'utilisateur et le mot de passe spécifiés par les paramètres OSLC_USER et OSLC_PASSWORD sont utilisés lorsque les demandes entrantes ne possèdent pas de données d'identification valides propres.

Si ce paramètre est défini sur `false`, la demande entrante doit contenir des données d'identification valides.
La valeur par défaut est `true`.

OSLC_USER
Ce paramètre est défini sur le nom d'utilisateur utilisé quand aucune donnée d'identification valide n'est incluse dans la demande. Si nécessaire, vous pouvez modifier le nom d'utilisateur utilisé.

La valeur par défaut est `administrator`.

OSLC_PASSWORD
Ce paramètre est défini sur le mot de passe utilisé quand aucune donnée d'identification valide n'est incluse dans la demande. Si vous modifiez le mot de passe de l'administrateur à l'aide de l'interface utilisateur TADDM, vous devez mettre à jour la valeur du mot de passe définie par ce paramètre.

La valeur par défaut est `collation`.

Exportation de données vers les services de registre à l'aide d'OSLCAgent

Vous pouvez utiliser l'agent de topologie OSLCAgent pour exporter des informations sur l'élément de configuration (EC) vers les services de registre.

OSLCAgent est une solution automatisée pour l'exportation de données entre TADDM et les services de registre. L'agent effectue périodiquement les tâches suivantes :

- Recherche d'objets pouvant être enregistrés dans les services de registre
- Traduction de ces objets en messages au format RDF
- Publication de ces objets à l'aide du protocole HTTP

OSLCAgent appartient au groupe Integration. L'intervalle de temps entre les exécutions est spécifié dans l'entrée suivante du fichier `collation.properties` :

`com.ibm.cdb.topobuilder.groupinterval.integration`

OSLCAgent peut agir en tant que fournisseur de configuration et en tant que fournisseur d'historique des changements. Ces deux rôles peuvent être activés séparément. Pour activer le rôle de fournisseur de configuration, définissez la propriété sur `true`:

`com.ibm.cdb.topobuilder.integration.oslc.enable.configurationsp`

Pour activer le rôle de fournisseur d'historique des changements, définissez la propriété sur `true` :

`com.ibm.cdb.topobuilder.integration.oslc.enable.changehistorysp`

Pour configurer OSLCAgent afin qu'il se connecte aux services de registre, vous devez indiquer l'adresses de ces services et accédez aux les détails de saisie.

Configurez l'adresses des services de registre dans la propriété suivante :

`com.ibm.cdb.topobuilder.integration.oslc.frsurl`

Indiquez l'adresse des services de registre dans le format suivant :

protocol`://`*fqdn_ou_ip_ou_nomhôte*`:`*port*

Par exemple, `http://192.0.2.24:9081`

Remarque : Le nom de domaine complet (FQDN) ou le nom d'hôte complet est préféré aux adresses IP afin d'assurer la cohérence avec d'autres produits et éviter les problèmes d'intégration. Toutefois, si tous les autres produits utilisés avec TADDM utilisent les adresses IP, vous devez spécifier l'adresse IP. S'il n'y a pas de produits utilisés avec TADDM, il est préférable d'utiliser le FQDN pour le cas où d'autres produits seraient ajoutés par la suite.

Créez une entrée de liste d'accès de type **Integration/Registry Service**. Indiquez le nom d'utilisateur et le mot de passe pour les services de registre.

Vous pouvez régler le mode de fonctionnement d'OSLCAgent à l'aide des propriétés suivantes :

com.ibm.cdb.topobuilder.integration.oslc.maxtimeperrun
Cette propriété spécifie la durée maximale (en minutes) durant laquelle OSLCAgent est autorisé à s'exécuter. Pour chaque fournisseur, cette durée

peut être dépassée d'une durée équivalente au temps requis pour les tâches envoyées vers le pool avant l'événement de délai d'attente. Si la propriété n'est pas configurée ou si elle est définie sur `-1`, la durée autorisée pour une exécution unique d'OSLCAgent est illimitée.

com.ibm.cdb.topobuilder.integration.oslc.jobspoolsize
Cette propriété indique le nombre maximal de travaux simultanés que vous êtes autorisé à exécuter. Chaque travail enregistre un élément de configuration unique. Si la propriété n'est pas configurée, la valeur par défaut est `10`.

com.ibm.cdb.topobuilder.integration.oslc.frshttptimeout
Cette propriété spécifie le délai de la connexion HTTP en millisecondes. La valeur par défaut est `5000`.

com.ibm.cdb.topobuilder.integration.oslc.frsfailfastafter
Cette propriété indique le nombre d'expirations du délai de connexion HTTP après lequel un agent considère les services de registre non disponibles et arrête les tentatives de connexion. La valeur par défaut est `5`.

com.ibm.cdb.topobuilder.integration.oslc.unregisterableIPs
Cette propriété spécifie les adresses IP qui ne doivent pas être enregistrées car elles sont privées et peuvent entraîner la surfusion des enregistrements de ressource. Cette propriété peut contenir des expressions régulières. La valeur par défaut est
`127.0.0.1,01111111000000000000000000000001,0:0:0:0:0:0:0:1,`
`00000000000000000000000000000000000000000000000000000000000000000`
`00000000000000000000000000000000000000000000000000000000000000000`
`000000000001`.

com.ibm.cdb.topobuilder.integration.oslc.unregisterableFQDNs
Cette propriété spécifie les noms de domaine complets qui ne doivent pas être enregistrés car ils sont privés et peuvent entraîner la surfusion des enregistrements de ressource. Cette propriété peut contenir des expressions régulières. La valeur par défaut est
`localhost.localdomain,localhost,loopback6(.?\u005c\w*)*`.

com.ibm.cdb.topobuilder.integration.oslc.enablecrtvtype.*CRTVType*
Cette propriété indique que les processus OSLCAgent traitent uniquement les éléments de configuration d'un type CRTV (Common Resource Type Vocabulary) particulier. Si elle est activée, l'enregistrement, la mise à jour et l'annulation de l'enregistrement sont uniquement possibles pour les éléments de configuration de type CRTV.

Par exemple, le paramètre

```
com.ibm.cdb.topobuilder.integration.oslc.enablecrtvtype.ComputerSystem=true
```

indique que seuls les systèmes informatiques sont traités.

Les types CRTV suivants sont autorisés :

- Système informatique
- Base de données
- Fix Pack 2 SAPSystem
- ServiceInstance
- Module logiciel
- SoftwareServer

com.ibm.cdb.topobuilder.integration.oslc.history.days_previous

Cette propriété définit le nombre de jours d'historique des modifications disponibles avec l'adresse URL de lancement en contexte. La valeur par défaut est 5.

Vous pouvez utiliser la propriété `days_previous` pour contrôler l'espace de stockage et le temps de traitement requis pour gérer les informations de l'historique des modifications.

L'adresse URL de lancement en contexte apparaît dans l'aperçu de l'historique des changements OSLC.

Si la valeur est supérieure à 0, le paramètre `days_previous` est appliqué à l'adresse URL de lancement en contexte pour limiter l'affichage de l'historique des modifications.

Si la valeur est inférieure ou égale à 0, l'adresse URL de lancement en contexte ne contient pas le paramètre `days_previous` et vous pouvez voir l'intégralité de l'historique des modifications de l'élément de configuration.

Interface de ligne de commande pour OSLCAgent

Vous pouvez utiliser l'interface de ligne de commande OSLCAgent pour exporter manuellement les informations relatives à un élément de configuration vers Registry Services.

Pour OSLCAgent, vous pouvez transmettre une combinaison de commandes et de commutateurs au script ou fichier de traitement `runtopobuild`. Chaque commande et commutateur présente un format court à une lettre et un format plus long et descriptif. Vous pouvez combiner tous les formats de commande et de commutateur.

Les commandes suivantes sont disponibles :

- `-R | –refreshAll true|false`

  Cette commande enregistre tous les éléments de configuration admissibles, même s'ils ont déjà été enregistrés.
- `-r | -refreshGuid` *`guid`*

  Cette commande enregistre l'élément de configuration ayant le GUID spécifié, même s'il a déjà été enregistré.
- `-l | -refreshIgnored true|false`

  Si un EC est reconnu à une position qui n'est pas assez profonde, ses règles de nommage sont éventuellement inexactes. Par défaut, OSLCAgent ignore ces EC. Cette commande force OSLCAgent à traiter à nouveau ces EC.

Pour indiquer des actions spécifiques, vous pouvez transmettre un commutateur avec n'importe quelle commande. Deux types de commutateurs sont disponibles.

Vous pouvez utiliser les commutateurs suivants pour activer ou désactiver le traitement de types CRTV spécifiques :

- `-c | --enableComputerSystem true|false`
- `-d | --enableDatabase true|false`
- `-i | --enableServiceInstance true|false`
- `-m | --enableSoftwareModule true|false`
- `-s | --enableSoftwareServer true|false`

Par exemple, si vous ne voulez pas enregistrer à nouveau les systèmes informatiques, utilisez les commutateurs `-c false`.

Vous pouvez utiliser les commutateurs suivants pour activer ou désactiver la configuration et modifier les rôles d'historique :

- `-h | --enableChangeHistoryProvider true|false`
- `-p | --enableConfigurationProvider true|false`

Par exemple, si vous ne voulez pas effectuer de nouvel enregistrement pour mettre à jour l'historique des changements, utilisez les commutateurs `-h false`.

Si vous voulez utiliser les valeurs par défaut en cas de non transmission d'une commande ou d'un commutateur lors de l'exécution du script ou fichier de traitement `runtopobuild`, configurez les propriétés suivantes dans le fichier `collation.properties` :

- `com.ibm.cdb.topobuilder.integration.oslc.refreshAll=true|false`
- `com.ibm.cdb.topobuilder.integration.oslc.refreshGuid=`*`guid`*
- `com.ibm.cdb.topobuilder.integration.oslc.enablecrtvtype.`*`crtv_type`*

Pour une liste complète des paramètres et commutateurs disponibles, accédez à `$COLLATION_HOME/support/bin` et exécutez le script ou fichier de traitement `runtopobuild` avec le commutateur `-H`. Par exemple,

```
./runtopobuild.sh -H
```

Enregistrement des éléments de configuration avec Registry Services

Cette rubrique répertorie les éléments de configuration (EC) reconnus par TADDM et interrogés pour enregistrement avec Registry Services. Elle présent aussi les attributs définis, ainsi que des informations détaillées sur le mappage.

Si un élément de configuration particulier n'est pas enregistré, chaque unité d'exécution d'enregistrement produit des informations de journal expliquant pourquoi l'élément de configuration n'est pas enregistré. La liste des attributs de règle de nommage non définis figure dans le journal. Pour configurer le niveau de journalisation correct, définissez la valeur de propriété suivante dans le fichier `collation.properties` :

```
com.collation.log.level.vm.Topology=DEBUG
```

Les attributs suivants sont communs pour chaque type CRTV :

Identificateur global unique
: Définissez-le à l'aide de la valeur GUID de l'élément de configuration.

name Définissez-le à l'aide de la valeur de l'attribut name, label ou displayName.

description
: Définissez-le à l'aide de la valeur de l'attribut description.

lastDiscoveredTime
: Définissez-le à l'aide de la valeur de l'attribut lastModifiedTime.

SoftwareServer

Le type CRTV SoftwareServer contient les classes et les attributs TADDM suivants :

- WebSphereServer
  - host

  - node
  - node.cell
- Db2Instance
  - home
  - host
- MQQueueManager
  - displayName | label | name
- AppServer
  - displayName | label | name
  - host
- CommunityServer
  - displayName | label
- SametimeServer
  - displayName | label
- MeetingServer
  - displayName | label
- SpecialityServer
  - displayName | label | name
- AgentManager
  - displayName | label
- SharePointRole
  - displayName | label | name

Les attributs TADDM sont mappés aux attributs CRTV de la façon suivante :

Attribut TADDM	Attribut CRTV	Autres informations
PrimarySAP	crtv:serverAccessPoint	La ressource serviceAccessPoint est enregistrée avec la ressource IpAddress vers laquelle elle pointe, à l'aide de crtv:ipAddress.
version	crtv:version	
vendorName	crtv:manufacturer	
host	crtv:runsOn	crtv:runsOn pointe vers ComputerSystem
home	crtv:instancePath	Pour DatabaseServer et Db2Instance uniquement.
dataPath	crtv:instancePath	Pour MQQueueManager uniquement.

rdf:type est défini sur l'une des valeurs suivantes :

- `J2EEServer`
- `WebSphereServer`
- `IBMHTTPServer`
- `WebServer`
- `Db2Instance`
- `OracleInstance`

- `MQQueueManager`
- `WebServer`
- `DatabaseInstance`
- `CICSRegion`

Système informatique

Le type CRTV ComputerSystem contient les classes et les attributs TADDM suivants :

- ComptuerSystem

  L'une des combinaisons d'attributs suivantes est définie :
  - systemId &VMID
  - systemId
  - serialNumber & model & manufacturer &VMID
  - serialNumber & model & manufacturer
  - systemBoardUUID
  - ipInterfaces

Les attributs TADDM sont mappés aux attributs CRTV de la façon suivante :

Attribut TADDM	Attribut CRTV	Autres informations
label ou displayName	crtv:name	
OSVersion ou OSRunning	crtv:version	
hostSystem	crtv:dependsOn	
fqdn	crtv:fqdn	
name	crtv:shortHostname	Si un nom est défini et qu'il s'agit d'un nom d'hôte valide. Pour SunSPARCComputerSystem uniquement.
ipInterface	crtv:ipAddress	Tous les noms de domaine complets pour ces adresses IP sont fusionnés dans crtv:fqdn.

crtv:type est défini avec les valeurs suivantes

- `Generic`
- `SunFire`
- `SunSPARC`
- `SystemP`
- `Unitary`
- `Virtual`
- `WPAR`

Pour LinuxUnitaryComputerSystem, des attributs supplémentaires sont mappés de la façon suivante :

Attribut TADDM	Attribut CRTV	Autres informations
manufacturer	crtv:manufacturer	
model	crtv:model	
serialNumber	crtv:serialNumber	
VMID	crtv:vmid	Si CPUType et Model sont définis : • Pour intel, VMID est défini sur `null` et une tentative est exécutée pour définir crtv:systemBoardUUID avec systemBoardUUID ou convertedUUID. • Pour power, CS est ignoré si VMID y est défini.

Pour SunSPARCUnitaryComputerSystem, des attributs supplémentaires sont mappés de la façon suivante :

Attribut TADDM	Attribut CRTV	Autres informations
systemId	crtv:hostid	
VMID	crtv:vmid	

Pour tous les autres systèmes informatiques, des attributs supplémentaires sont mappés de la façon suivante :

Attribut TADDM	Attribut CRTV	Autres informations
manufacturer	crtv:manufacturer	
model	crtv:model	
serialNumber	crtv:serialNumber	
VMID	crtv:VMID	Si OSRunning est défini sur `WindowsOperatingSystem`, VMID est défini sur `null`. Si OSRunning est défini sur `HpUx`, VMID, model et serialNumber sont définis sur `null`.
systemBoardUUID ou convertedUUID	crtv:systemBoardUUID	
worldWideName	crtv:hostid	Pour FCSwitch, TapeLibrary et TapeMediaChanger uniquement.

Base de données

Le type CRTV Database contient les classes et les attributs TADDM suivants :

- Db2Database
  - name | displayName
- IDSDatabase
  - name | displayName

- IMSDatabase
  - name | displayName
- OracleDatabase
  - name | displayName
- SqlServerDatabase
  - name | displayName
- SybaseDatabase
  - name | displayName
- DominoDatabase
  - name | displayName

Les attributs TADDM sont mappés aux attributs CRTV de la façon suivante :

Attribut TADDM	Attribut CRTV	Autres informations
name	crtv:name	
fileName	crtv:name	Pour DominoDatabase uniquement.
parent	crtv:dbInstance	

ServiceInstance

Selon la compatibilité activée ou non avec des versions antérieures, le type CRTV ServiceInstance contient les classes et attributs TADDM suivants :

- Si la compatibilité avec des versions antérieures est activée :
  - BusinessSystem
    - name
  - Application
    - name
  - ServiceInstance
    - name
  - ServiceInfrastructure
    - name
  - SAPSystem
    - SAPSystemSID | systemHome
- Si la compatibilité avec des versions antérieures est désactivée :
  - CustomCollection (avec le type „BusinessApplication” uniquement)
    - collectionId

Les attributs TADDM sont mappés aux attributs CRTV de la façon suivante :

Attribut TADDM	Attribut CRTV	Autres informations
name	crtv:name	
SAPSystemSID:systemHome	crtv:name	Lorsque ni name ni displayName ne sont définis. Pour SAPSystem uniquement.
parentGUID ou NULL	crtv:parentServiceInstance	

Attribut TADDM	Attribut CRTV	Autres informations
collectionId	crtv:name	

Module logiciel

Le type CRTV SoftwareModule contient les classes et les attributs TADDM suivants :

- SoftwareModule
  - fileName
  - name
  - parent.name
- MQQueue
  - name
  - queueManager

Les attributs TADDM sont mappés aux attributs CRTV de la façon suivante :

Attribut TADDM	Attribut CRTV	Autres informations
parent	deployedTo	
fileName	crtv:fileName	

rdf:type est défini sur l'une des valeurs suivantes

- `J2EEApplication`
- `MQQueue`

Identification et résolution des problèmes liés à OSLC

Cette rubrique décrit les problèmes courants dans OSLC et propose des solutions à ces problèmes.

L'URL TADDM configurée n'inclut pas de numéro de port

Problème

La propriété de l'URL TADDM qui est configurée dans le fichier `collation.properties`, `taddmURL`, doit inclure un numéro de port.

Si la propriété n'est pas configurée avec un numéro de port, vous devez mettre à jour l'URL de TADDM pour inclure un numéro de port, effacer les informations sur Registry Services ou des fournisseurs spécifiques, ainsi que supprimer les horodatages de TADDM.

Solution

Pour mettre à jour l'URL TADDM afin qu'elle inclue un numéro de port, effectuez les étapes suivantes :

1. Dans le fichier `collation.properties`, définissez la propriété `taddmURL` de la manière suivante :
   `taddmURL=http://`*`serveur`*`.`*`domaine`*`:`*`port`*
2. Sur l'ordinateur où Registry Services est installé, procédez comme suit :
   a. Accédez à `/opt/IBM/JazzSM/registry/etc`.
   b. Dans le fichier `CLI.properties`, configurez des données d'identification pour les propriétés suivantes :
      - ds.jdbc.user

- ds.jdbc.password
- appserver.user
- appserver.password

c. Accédez à `/opt/IBM/WebSphere/AppServer/bin`.

d. Exécutez le script `stopServer.sh` pour arrêter le serveur d'applications WebSphere.

```
./stopServer.sh server_name -user user_name -p password
```

par exemple,

```
./stopServer.sh server1 -user wasadmin -p passw0rd
```

e. Accédez à `/opt/IBM/JazzSM/registry/bin`.

f. Exécutez le script `frs.sh` avec les paramètres appropriés :

```
./frs.sh uninstall -type db -properties ../etc/CLI.properties
```

g. Assurez-vous que la base de données a été supprimée. Faute de quoi, exécutez les commandes suivantes :

```
db2 drop db db_name
db2 create db db_name
```

où *db_name* est le nom de la base de données Registry Services.

h. Accédez à `/opt/IBM/JazzSM/registry/bin`.

i. Exécutez le script `frs.sh` avec les paramètres appropriés :

```
./frs.sh install -type db -properties ../etc/CLI.properties
```

j. Accédez à `/opt/IBM/WebSphere/AppServer/bin`.

k. Exécutez le script `startServer.sh` pour démarrer le serveur d'applications WebSphere.

```
./startServer.sh server_name -user user_name -p password
```

par exemple,

```
./startServer.sh server1 -user wasadmin -p passw0rd
```

l. Exécutez le script `frs.sh` avec les paramètres appropriés :

```
./frs.sh uninstall -type container -properties ../etc/CLI.properties
```

m. Exécutez le script `frs.sh` avec les paramètres appropriés :

```
./frs.sh install -type container -properties ../etc/CLI.properties
```

Vous pouvez supprimer un élément de Registry Services pour un fournisseur déterminé à l'aide de la commande suivante :

```
./frs.sh deleteProvider -providerUrl url - properties cli.properties
```

3. Sur l'ordinateur contenant la base de données TADDM, effectuez les étapes suivantes :

a. Accédez au répertoire `$COLLATION_HOME/support/bin`.

b. Exécutez le script ou fichier de traitement par lots `runtopobuild` avec les paramètres appropriés, par exemple :

```
./runtopobuild.sh -a OSLCAgent -R
```

Tivoli Directory Integrator

A l'achat d'IBM Tivoli Application Dependency Discovery Manager (TADDM), vous recevez Tivoli Directory Integrator, qui vous permet d'intégrer TADDM à d'autres sources de données.

Documentation de Tivoli Directory Integrator dans le Knowledge Center
http://www-01.ibm.com/support/knowledgecenter/SSCQGF_7.1.0/KC_ditamaps/welcome.html?lang=en

Scénarios d'intégration de TADDM dans le wiki Tivoli Application Dependency Discovery Manager
https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Application%20Dependency%20Discovery%20Manager/page/Integration%20Scenarios

Compatibilité des entités métier avec des versions antérieures

Une nouvelle fonction a été introduite pour permettre l'intégration entre TADDM et des produits qui lisent des données issues de TADDM à l'aide de DataApi ou directement à partir de la base de données de TADDM en utilisant SQL. IBM Tivoli Business Service Manager (TBSM), IBM SmartCloud Control Desk (SCCD), Tivoli Directory Integrator (TDI) sont des exemples de tels produits. Le modèle de données Application métier actuel s'appuie sur l'interface CustomCollection, qui n'a rien de commun avec les anciennes interfaces Application et ITSystem. La nouvelle fonction permet une intégration à d'autres produits sans avoir à apporter de modifications à ces systèmes.

Dans les versions futures de TBSM et de SCCD, le modèle Application métier sera présenté avec de nouvelles fonctionnalités. L'objectif consiste à générer de précédentes entités métier qui sont des copies d'instances de collections personnalisées.

La nouvelle fonction qui offre une compatibilité avec des versions antérieures, se compose des fonctionnalités suivantes.

Etape supplémentaire lors de l'exécution de `BizAppsAgent`
L'étape supplémentaire génère des entités métier (services, application, collection) compatibles avec des versions antérieures pour chaque collection personnalisée qui est générée par l'agent.

Pour activer cette étape, une nouvelle propriété a été ajoutée au fichier `collation.properties` : `com.ibm.cdb.serviceinfrastructure.earlier.ver.compatibility`. La valeur par défaut de cette propriété est *TRUE* pour le scénario de mise à niveau et *FALSE* pour le scénario d'installation fraîche.

Prise en charge d'OSLC
L'agent OSLC a été modifié et est en mesure d'enregistrer d'anciennes entités métier ou de nouvelles collections personnalisées. Lorsque l'indicateur de compatibilité est défini à *TRUE*, des anciennes entités métier sont enregistrées. Sinon, des collections personnalisées sont utilisées pour produire un contenu pour JazzSM (Jazz for Service Management).

Dans le futur, une rechargement complet des entités métier sera requis si l'intégration du produit commence à charger des données en utilisant de nouveaux objets de modèle (collections et noeuds personnalisés). D'anciennes applications métier (applications) et de nouvelles applications métier (collections personnalisées) ne peuvent pas avoir le même identificateur global unique. Pour éviter des doublons, avant de charger une nouvelle collection personnalisée, les utilisateurs doivent avoir supprimé les anciennes applications métier.

Création de groupes fonctionnels

Contrairement aux anciennes applications métier, les nouvelles applications métier ne possèdent pas de groupes fonctionnels. Cependant, une nouvelle fonctionnalité tierce a été introduite pour servir des objectifs similaires. Afin de garantir la compatibilité avec des versions antérieures, pour chaque niveau unique, un groupe fonctionnel portant un nom correspondant au nom du niveau est créé.

Pour plus d'informations, voir la rubrique *Niveaux d'applications métier* dans le *Guide d'utilisation* de TADDM.

Intégration de BigFix

Fix Pack 5

IBM a travaillé au développement d'un support dans TADDM pour reconnaître des serveurs/machines sécurisés sans utiliser d'ancres et de passerelles et qui repose sur l'utilisation de l'infrastructure BigFix.

Remarque : Quand un chemin d'accès est affiché comme chemin relatif, ce chemin d'accès est supposément relatif à `$COLLATION_HOME (/opt/ibm/taddm/dist)` ou `%COLLATION_HOME% (E:\ibm\taddm\dist)`.

Introduction

IBM/Aricent a travaillé au développement d'un support dans TADDM pour reconnaître des serveurs/machines sécurisés sans utiliser d'ancres et de passerelles et qui repose sur l'utilisation de l'infrastructure BigFix.

Remarque : Quand un chemin d'accès est affiché comme chemin relatif, ce chemin d'accès est supposément relatif à `$COLLATION_HOME (/opt/ibm/taddm/dist)` ou `%COLLATION_HOME% (E:\ibm\taddm\dist)`.

Objectif :

TADDM utilise des ancres et des passerelles pour reconnaître les machines, les applications et le réseau qui se trouvent derrière un pare-feu. L'utilisation des ancres/passerelles peut être évitée à l'aide des outils de contrôle IBM Netcool (ITM). L'intégration de TADDM à l'architecture BigFix permet également d'éviter l'utilisation des ancres et des passerelles. L'architecture BigFix se compose du serveur BigFix (serveur BES) et de plusieurs noeuds finaux BigFix (clients BES) où les clients BES sont les machines sécurisées accessibles au moyen du serveur BES. L'infrastructure BigFix peut être réutilisée/utilisée automatiquement pour exécuter les packages de script TADDM sur les clients BES par l'intermédiaire du serveur BES.

Voici les avantages clés de cette intégration pour les administrateurs de TADDM :

1. Possibilité de reconnaître des zones protégées par un pare-feu sans ancres.
2. Possibilité de réutiliser l'architecture BigFix (par exemple, les ports sécurisés ouverts) pour accéder aux noeuds finaux et d'économiser du temps de configuration pour reconnaître les mêmes cibles à l'aide de la méthode TADDM standard.
3. Alignement sur la direction stratégique pour les détecteurs basés sur script de TADDM.
4. Intervention requise minime de l'administrateur de TADDM.

5. Fournit une méthode alternative pour reconnaître les machines des zones protégées par un pare-feu sans utiliser l'intégration de TADDM à ITM.

Référence :

Documentation de TADDM

Le tableau suivant montre les versions prises en charge des produits auxquels TADDM peut être intégré.

Pour plus d'informations sur les produits que vous intégrez à TADDM, consultez leur documentation respective :

- Knowledge Center de TADDM 7.3 et des détecteurs (documentation officielle) http://www-01.ibm.com/support/knowledgecenter/SSPLFC_7.3.0/com.ibm.taddm.doc_7.3/welcome_page/kc_welcome-444.html?lang=en
- Détecteurs de TADDM 7.3 et systèmes cible pris en charge https://www.ibm.com/developerworks/community/groups/service/html/communityview?communityUuid=7d5ebce8-2dd8-449c-a58e-4676134e3eb8#fullpageWidgetId=Wea1cb2531f10_4ccd_99d7_6ab0334cb21f&file=e70bf323-31f1-45ba-8992-4cb491feab4a
- TADDM - Configuration de la reconnaissance de scripts asynchrones (ASD) https://www.ibm.com/support/knowledgecenter/SSPLFC_7.3.0/com.ibm.taddm.doc_7.3/SensorGuideRef/r_cmdb_async_script_sensors.html#sensorsthatcanbescripted
- Guide de configuration d'IBM BigFix https://www.ibm.com/support/knowledgecenter/SSPLFC_7.3.0/com.ibm.taddm.doc_7.3/SensorGuideRef/r_cmdb_async_script_sensors.html#sensorsthatcanbescripted
- Site Web de support de TADDM http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliApplicationDependencyDiscoveryManager.html
- Wiki de TADDM https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Application%20Dependency%20Discovery%20Manager/page/Home Il s'agit d'une bonne source d'informations à jour et de meilleures pratiques pour TADDM. Ajoutez cette page à vos favoris et familiarisez-vous avec celle-ci.
- Forum de TADDM http://www.ibm.com/developerworks/forums/forum.jspa?forumID=1547&categoryID=15&ca=drs-fo
- Demande à la Communauté d'amélioration http://www.ibm.com/developerworks/rfe/?BRAND_ID=90 Cette communauté doit être sollicitée pour demander des améliorations du produit directement aux développeurs IBM.

Architecture de la solution :

L'intégration de TADDM à BigFix repose sur l'extension et l'automatisation du comportement actuel de la Reconnaissance de scripts asynchrones (Asynchronous Script Discovery ou ASD) qui nécessite l'intervention manuelle de l'administrateur de TADDM. Cette intégration utilise la connectivité que l'infrastructure BigFix fournit aux machines de zones situées derrière un pare-feu pour exécuter la reconnaissance au moyen des packages de script TADDM.

Dans ASD, l'administrateur de TADDM doit effectuer les étapes suivantes manuellement :

1. Exécuter un script sur le serveur TADDM pour créer un package de reconnaissance qui inclut tous les détecteurs à exécuter sur la cible.

2. Transférer ce package vers le système cible.
3. Exécuter le package de reconnaissance sur le système cible.
4. Retransférer le fichier de résultats généré sur le système cible vers le serveur TADDM.

Avec la solution actuelle, les étapes manuelles ont été automatisées et la solution se nomme donc désormais Reconnaissance de scripts asynchrones automatisée (Automated Asynchronous Script Discovery ou AASD). Il suffit à l'administrateur de TADDM d'exécuter un script pour démarrer la reconnaissance sur le serveur TADDM et des étapes de redémarrage seront effectuées automatiquement.

Etapes dans BigFix Discovery :

Détails des étapes de la reconnaissance BigFix

Etape 1 : Script d'intégration de BigFix

Le script « runBigFixDiscovery.sh » a été développé pour démarrer la reconnaissance de scripts asynchrones automatisée (AASD) à partir du serveur de reconnaissance TADDM. Le script peut être exécuté à la demande. Ce script utilise la Portée de reconnaissance et le nom du Profil de reconnaissance (outre les données d'identification d'accès à BigFix) et prend en charge les modes ci-dessous :

- Mode RECONNAÎTRE : pour lancer la reconnaissance BigFix
- Mode SONDAGE : pour sonder les résultats de la reconnaissance BigFix
- Mode NETTOYAGE : pour une purge à la demande des packages de résultats de reconnaissance du serveur racine BES
- Mode RECONNAÎTRE À NOUVEAU : pour réexécuter la reconnaissance précédente

a) Créer un package de détecteurs AASD

- Le profil de reconnaissance indiqué est utilisé pour extraire la liste de détecteurs et seul un sous-ensemble de détecteurs scriptés valides est considéré pour la création d'un package de scripts AASD. Consultez l'Annexe D pour obtenir la liste complète de tous les détecteurs scriptés pris en charge par TADDM, fonction qui ne prend en charge qu'un sous-ensemble de ces détecteurs pris en charge en mode ASD standard.
- Les autres détecteurs non scriptés du profil de reconnaissance sont ignorés
- Le package ASSD fonctionne sur tous les systèmes d'exploitation ; par conséquent, certains détecteurs peuvent échouer sur les noeuds finaux de BigFix en son absence
- Le package de script AASD généré est téléchargé sur le serveur racine BigFix à l'aide de l'API REST /api/upload

b) Créer une tâche BigFix

- La portée de reconnaissance indiquée est utilisée pour créer le fichier XML de « Langage de pertinence », lequel est compris par BigFix
- Le fichier XML de la tâche BigFix est généré avec le « Langage de pertinence » et le « Script d'action » factice
- Générez le titre de la tâche en fonction de la date-heure en cours
- Utilisez l'API REST /api/tasks/custom/TADDM pour créer une tâche BigFix sous le site personnalisé nommé « TADDM » sur le serveur BigFix

c) Démarrer la tâche BigFix

- Utilisez <Action_fixlet_sourcée> pour exécuter l'action de la tâche BigFix créée ci-dessus
- L'API REST /api/actions de BigFix permet de démarrer l'exécution du « Script d'action » sur le noeud final cible

Etape 2 : Exécution du script

- Lors de l'exécution du « Script d'action », le package AASD de TADDM sera décompressé et les scripts de détecteur (basés sur le profil de reconnaissance) qu'il contient seront exécutés sur les noeuds finaux de BigFix

Etape 3 : Collecter le fichier zip

- A la fin de l'exécution du « Script d'action », le package de résultats généré sur le client BES suite à l'exécution du package AASD de TADDM sera copié sur le serveur racine BES

Etape 4 : Réimporter les résultats sur TADDM

- TADDM interrogera continuellement la base de données du serveur BigFix pour rechercher le fichier de résultats téléchargé sur le serveur BES
- Si la base de données indique la présence de nouveaux fichiers de résultats, TADDM émettra une demande HTTP pour extraire les fichiers de résultats chiffrés, les déchiffrer et les sauvegarder
- TADDM traitera ensuite ces fichiers de résultats en fonction de la portée et du profil configurés et stockera les objets reconnus dans la base de données

Intégration de TADDM à Bigfix (Disponibilité limitée)

L'édition en Disponibilité limitée de la solution de reconnaissance TADDM étendue de BigFix se concentre sur l'exécution de bout en bout de la fonction de reconnaissance pour les systèmes d'exploitation Windows, Linux, AIX et Solaris et les détecteurs associés (pour plusieurs noeuds finaux) avec une prise en charge de la communication SSL entre TADDM et BigFix par le biais des API REST BigFix. La reconnaissance peut être lancée sur le serveur de reconnaissance TADDM et les résultats de reconnaissance seront extraits automatiquement et visibles sur l'interface graphique de TADDM

Suppositions :

Les suppositions suivantes ont été prises en considération dans l'exécution de la reconnaissance :

1. Le serveur BigFix et les clients disposent de la version mentionnée dans la section 2.1.

2. Les clients BigFix disposent des droits appropriés pour exécuter le script de la tâche/action de reconnaissance téléchargé par le serveur BigFix.

3. L'utilisateur de la base de données SQL de BigFix configuré dans collation.properties doit disposer d'un accès en lecture à la base de données BFEnterprise.

4. Les packages de scripts de détecteur exécutés par l'intermédiaire des agents BigFix auront besoin d'un accès en écriture au répertoire temporaire configuré (par exemple : « C:\Windows\Temp »). Le répertoire temporaire peut être configuré dans collation.properties et son chemin de répertoire ne doit pas contenir d'espaces.

5. Le nettoyage du package de demande de script n'est pas traité sur le serveur de reconnaissance TADDM et il est supposé que l'administrateur le gérera.

6. Puisque l'intégration de TADDM à BigFix repose sur l'infrastructure ASD existante dans TADDM, les caractéristiques de performance de cette intégration se baseront sur des tests de performances de l'infrastructure ASD.

7. Seul « taddmusr » peut être utilisé pour exécuter le script de reconnaissance BigFix sur le serveur de reconnaissance TADDM, l'utilisateur racine ne sera pas autorisé.

8. Nettoyage du serveur racine Bigfix : le nettoyage sera appelé à chaque démarrage de TADDM mais aussi périodiquement selon la durée configurée (com.collation.bigfix.root.cleanup.interval = 1 jour par défaut). Cette action supprimera les fichiers de résultats plus anciens que la période configurée (com.collation.bigfix.root.cleanup.days = 5 jours par défaut).

9. Nettoyage du serveur TADDM : tous les fichiers de résultats créés/copiés sur le serveur TADDM pendant la reconnaissance seront nettoyés et ceux dont le nom contient « taddmasd » et se termine par « _DONE » seront traités. (Au moins un des seuils indiqués dans l'annexe A, puce 6 doit être configuré pour activer le nettoyage sur le serveur TADDM).

10. Nettoyage du noeud final : le nettoyage du noeud final de reconnaissance est activé par défaut et peut être contrôlé en configurant le paramètre de propriété ci-dessous :

- a) Un paramètre « com.collation.bigfix.endpoint.cleanup » ayant pour valeur « N » désactivera le nettoyage sur le noeud final de reconnaissance.

Prérequis :

Avant de démarrer la reconnaissance à partir du serveur TADDM, les prérequis suivants doivent être remplis :

1. Sélectionnez ASDSensor, ASDPingSensor et Generic Server Sensor et décochez PingSensor, PortSensor et SessionSensor de manière obligatoire lors de la création du profil de reconnaissance.

2. Toutes les étapes de configuration indiquées dans la section 2.3 ont été effectuées.

3. Le script d'action Bigfix a utilisé la commande powershell native pour décompresser le package de demande sur le noeud final Windows et la commande tar native sur Linux

Remarque : En fonction d'un besoin spécifique, il est possible de personnaliser le langage ActionScript. Cette personnalisation est prise en charge lorsque le fichier modifiable par le client ActionScript_Pre_Post.txt situé dans le dossier `$COLLATION_HOME/etc/` est mis à jour, entre autres, autoriser le téléchargement et l'utilisation d'un logiciel de décompression personnalisé (distribution de l'exécutable sur le serveur racine BigFix). Un exemple de fragment est fourni ci-dessous :

```
%WIN_PRE_START%
if {not exists file "C:\Windows\System32\unzip.exe"}
prefetch unzip.exe sha1:e1652b058195db3f5f754b7ab430652ae04a50b8
size:167936 http://10.160.161.199:52311/Uploads/Unzip/unzip.exe
```

```
// Make sure that environment is set appropriately and "unzip"
utility is available in the windows PATH
copy "__Download\unzip.exe" "C:\Windows\System32\unzip.exe"

endif
%WIN_PRE_END%

%WIN_POST_START%
%WIN_POST_END%

%LIN_PRE_START%
%LIN_PRE_END%
...
```

4. L'utilisateur exécutant la reconnaissance devra disposer de droits de lecture/écriture pour le dossier de résultats.

5. L'espace disque, la capacité de traitement et la mémoire doivent être suffisants pour répondre aux demandes et aux packages de résultats traités sur le serveur TADDM, le serveur racine BigFix et les cibles.

6. L'agent BigFix (ordinateur de noeud final) doit être configuré en indiquant une valeur suffisante pour le paramètre « _BESClient_ArchiveManager_MaxArchiveSize » afin de permettre les téléchargements de résultats au serveur racine BigFix.

7. La portée et le profil corrects doivent être définis (voir la section 4.1 pour la définition de la portée et du profil).

8. Le nom de site « TADDM » doit être configuré et existant sur le serveur BigFix.

9. Toutes les conditions préalables nécessaires aux scripts de détecteur ASD standards s'appliquent également en cas de reconnaissance BigFix.

- a) L'exécutable Powershell doit être correctement installé et configuré en cas de reconnaissance impliquant un noeud final Windows 2003.

Limitations :

Les limitations suivantes sont liées à l'édition actuelle :

1. Toute cible de reconnaissance spécifiée pendant la reconnaissance et non accessible depuis le serveur racine BigFix ne sera pas visible dans l'historique de reconnaissance.

2. Les détecteurs PingSensor, PortSensor et SessionSensor sont activés automatiquement lorsque d'autres détecteurs sont sélectionnés et activés, et doivent être désactivés manuellement lors de la création du profil de reconnaissance.

3. Le nettoyage des packages de demande sur le serveur de reconnaissance TADDM ou le serveur racine BigFix n'est pas pris en charge par nature. On considère qu'elle peut être utilisée pendant la nouvelle reconnaissance (déclenchée par le mode Reconnaître à nouveau).

4. La nouvelle reconnaissance n'est prise en charge qu'à partir du même serveur de reconnaissance TADDM sur lequel la reconnaissance initiale a été lancée.

5. Il s'agit d'une édition en Disponibilité limitée, ce qui signifie que la traduction et le support de documentation en ligne, entre autres, ne sont pas disponibles.

6. La reconnaissance de serveurs personnalisés n'est pas prise en charge par l'intégration de BigFix.

Configuration :

Suivez les étapes mentionnées dans cette section pour définir la configuration souhaitée.

Configurations de base pour Bigfix Discovery :

1. Définissez les propriétés obligatoires suivantes dans $COLLATION_HOME/etc/collation.properties

a) Paramètres de la fonction d'intégration de BigFix

```
com.collation.bigfix.enabled=true
```

b) Paramètres du serveur BigFix

- com.collation.bigfix.host=<IP ou nom de domaine complet du serveur BigFix>
- com.collation.bigfix.port=<N° de port>
- com.collation.bigfix.uid=<ID utilisateur pour accéder à la console du serveur BigFix>
- com.collation.bigfix.pwd=<mot de passe pour accéder à la console du serveur BigFix>

c) Paramètres de la base de données BigFix

- com.collation.bigfix.db.type=<MSSQL/DB2>
- com.collation.bigfix.db.host=<IP ou nom de domaine complet de la base de données du serveur BigFix>
- com.collation.bigfix.db.port=<Port sur lequel TADDM se connectera à la base de données BigFix>
- com.collation.bigfix.db.dbname=<nom de la base de données BigFix>
- com.collation.bigfix.db.domain=<Domaine utilisateur> Paramètre facultatif : obligatoire seulement quand l'authentification basée sur Windows est configurée pour la base de données BigFix>
- com.collation.bigfix.db.uid=<ID utilisateur permettant d'accéder à la base de données BigFix>
- com.collation.bigfix.db.pwd=<Mot de passe permettant d'accéder à la base de données BigFix>

d) Paramètres de l'unité d'exécution du traitement des résultats

- com.ibm.cdb.discover.asd.ProcessUnreachableIPs=true
- com.ibm.cdb.discover.asd.autodiscovery.enabled=true

2. Définissez les propriétés suivantes dans $COLLATION_HOME/etc/collation.properties seulement si la configuration SSL est activée sur le serveur BigFix :

e) Certificat BigFix

- com.collation.bigfix.certificate.type=<PKCS12/JKS>
- com.collation.bigfix.certificate.file=<Chemin d'accès complet au fichier certificat>
- com.collation.bigfix.certificate.pwd=<Mot de passe pour utiliser le certificat>

Remarque : Des propriétés supplémentaires autres que ces propriétés obligatoires peuvent être configurées. Consultez l'Annexe A pour obtenir la liste complète des propriétés et leurs détails.

Remarque : Les certificats générés avec un champ de mot de passe vide ne sont pas pris en charge.

3. Exécutez le script « encryptprops.sh » pour chiffrer les propriétés (consultez l'Annexe C pour vérifier leformat nécessaire pour l'exécution de ce script). Autrement, des scripts de reconnaissance (runBigFixDiscovery.sh/.bat) échoueront en affichant une erreur d'arguments manquants ou non valides (référez-vous à l'Annexe E pour des détails sur le code d'erreur) puisque les mots de passe non chiffrés ne sont pas acceptés.

4. Créez le dossier COLLATION_HOME/var/asdd pour stocker les fichiers de résultats dans TADDM. Si le dossier var/asdd ne doit pas être utilisé, il faut définir la propriété « com.ibm.cdb.discover.asd.AsyncDiscoveryResultsDirectory » en indiquant le dossier spécifique dans lequel l'administrateur veut que les fichiers de résultats soient stockés.

5. Redémarrez TADDM.

6. Créez un profil de reconnaissance avec les détecteurs obligatoires mentionnés dans la section 2.1. Le profil doit avoir des détecteurs obligatoires en plus des autres détecteurs reconnus.

7. Créez une portée de reconnaissance avec un ou plusieurs noeuds finaux cible BigFix où la reconnaissance doit être exécutée.

Autre configuration :

Un nom de site « TADDM » doit être créé sur le serveur BigFix.

1. Ouvrez la « Console BigFix » -> accédez à l'onglet « Outils » -> sélectionnez « Créer un site personnalisé » -> entrez le nom de site « TADDM ».

2. Cliquez sur « TADDM » -> sélectionnez l'onglet « Abonnement d'ordinateur » -> abonnez des ordinateurs en fonction des besoins (tous les ordinateurs auxquels le serveur BigFix veut se connecter par le biais de TADDM doivent être inclus).

Conseils relatifs au fichier journal et au traitement des incidents :

Si un incident se produit pendant la reconnaissance, il est possible de vérifier les éléments suivants. Vérifiez que tous les prérequis sont remplis et respectés :

Serveur de reconnaissance TADDM

- Vérifier les journaux pour le script d'exécution Bigfix Discovery
  - `$COLLATION_HOME/log/BigFixDiscovery.log`
- Vérifier dans les journaux que le Fichier de résultats atteint ou non le serveur TADDM :
  - `$COLLATION_HOME/log/services/ApiServer.log` (effectuez une recherche avec les mots clés « BigfixDiscoveryServerController » et « AASDiscoveryServerController »)

Serveur racine BigFix

Vérifier le statut de la reconnaissance et de l'exécution d'action à l'aide de la `Console IBM BigFix` sur le **serveur racine BigFix**

1. Ouvrez la **Console IBM Bigfix**.
2. Sélectionnez **Site** (Personnalisé -> TADDM) -> **Fixlets** et **Tâches**.
3. Sélectionnez **Tâche** (donnée pendant l'exécution du script).
4. Accédez à **Détails** et **Historique des actions**.
5. Sélectionnez **Historique des actions spéciales** -> **Ordinateurs signalés**.
6. Vérifiez le statut et **cliquez deux fois** dessus pour une exécution ligne par ligne.
7. Cliquez sur **OK** pour revenir à la fenêtre Profils de reconnaissance.

Agent BigFix/Cible de la reconnaissance

- Vérifiez que le fichier de résultats se trouve dans le dossier `%wintemp%"/taddm7.3.0.4/asd` (seulement lorsque la propriété com.collation.bigfix.endpoint.cleanup est définie sur « N »)
- Le fichier `allErrors.txt` (se trouvant dans `%wintemp%"/taddm7.3.0.4/asd`) peut être mis en référence pour toutes erreurs survenues pendant l'exécution du script des détecteurs

Exécution de Bigfix Discovery :

Exécution de Bigfix Discovery

Création de la portée :

Ouvrez l'interface graphique du serveur TADDM pour créer une portée de reconnaissance. La portée doit inclure tous les noeuds finaux cible deBigFix. Les noeuds finaux cible peuvent être définis comme hôtes individuels ou en indiquant la portée de domaine/réseau.

Création d'un profil :

Un profil de reconnaissance doit être créé à l'aide de l'interface graphique du serveur TADDM. Le profil doit inclure les détecteurs correspondant aux applications que l'administrateur veut faire reconnaître par TADDM. Voir la section 2.1 pour plus d'informations sur les détecteurs qui doivent obligatoirement être inclus/exclus du profil de reconnaissance créé.

Exécution du script :

Pour exécuter la reconnaissance, le script « runBigFixDiscovery.sh » doit être exécuté dans COLLATION_HOME/bin. Le script peut être exécuté dans 4 modes : « reconnaissance », « sondge », « nettoyage » et « nouvelle reconnaissance ». En mode reconnaissance, la reconnaissance est démarrée. En mode sondage, le statut actuel de la reconnaissance sera extrait. En mode nettoyage, le nettoyage des fichiers de résultats sera déclenché sur le serveur racine BigFix, et en mode nouvelle reconnaissance, la reconnaissance exécutée précédemment peut être exécutée de nouveau.

1. Mode reconnaissance-

TADDM fournit Jazz for Service Management avec un service de flux à l'adresse suivante :

```
./runBigFixDiscovery.sh -d -o <output dir> -s <scope> -p <profile>
Where,
-d – for discovery mode
-o - output directory where discovery package would be created
-s – input scope, having BigFix endpoints target that are to be discovered.
-p – input profile, having sensors to be run
```

Une fois la commande exécutée en mode reconnaissance, la reconnaissance démarre. Cela affichera le statut des étapes effectuées et donnera un ID d'« Action ». Cette Action peut être utilisée en mode sondage pour vérifier le statut de l'action sur chaque noeud final de BigFix

Remarque :

- L'« ID d'action » créé pour la reconnaissance (affiché dans la sortie de la console, par exemple 2090 dans l'exemple ci-dessous) peut être réutilisé à des fins de sondage.
- Conservez le nom de la tâche BigFix nouvellement créée (« Nom de tâche » affiché dans la sortie de la console, par exemple 20180130125432) associée à la portée et au profil indiqués qui peut être réutilisé pour une nouvelle reconnaissance.

2. Mode sondage-

```
./runBigFixDiscovery.sh -p -r <répétition> -i <ID d'action>

Where,
-p – for poll mode
-r – no of times polling will be done to BigFix server
-i - Action id obtained from discovery mode command.
```

3. Mode nettoyage-

```
./runBigFixDiscovery.sh -c -d <Nombre de jours>
Where,
-c – for cleanup mode
-d – Files older than specified number of days to be removed
```

4. Mode nouvelle reconnaissance

```
./runBigFixDiscovery.sh  -r/--rediscover -i <Nom de tâche>
Where,
-r – for rediscover mode
-i – TASK NAME corresponding to the previous discovery, that needs to be run again
```

Remarque : Des détails supplémentaires sur cette commande incluant toutes les options possibles sont exposés dans l'Annexe B et un exemple pour exécuter la commande est décrit dans l'Annexe C.

Traitement des résultats de la reconnaissance :

Le mode sondage de la commande « runBigFixDiscovery.sh » donne le statut de l'action exécutée sur chaque noeud final BigFix. En fonction du statut, le fichier de résultats sera créé et traité.

1. Une fois l'action terminée avec succès sur le noeud final, un fichier de résultats pour ce noeud final sera importé dans le dossier de résultats configuré (par défaut var/asdd. Voir la section 2.3.1 pour la configuration du dossier de résultats).

2. Une fois l'action terminée avec succès sur le noeud final, un fichier de résultats pour ce noeud final sera importé dans le dossier de résultats configuré (par défaut var/asdd. Voir la section 2.3.1 pour la configuration du dossier de résultats).

3. Une fois les fichiers de résultats traités avec succès, le résultat sera disponible sur l'interface graphique de TADDM dans l'onglet Historique.

4. Les données de résultat traitées seront stockées dans la base de données TADDM et seront disponibles sur le portail de gestion de données ou le PSS de TADDM.

Scénario d'incident possible :

En cas d'incident au cours du mode reconnaissance, sondage, nettoyage ou nouvelle reconnaissance, il est possible d'effectuer les vérifications suivantes :

1. Confirmez que tous les prérequis mentionnés dans la section 2.2 sont respectés :

2. Vérifiez les journaux de TADDM dans le chemin :
- `$COLLATION_HOME/log/BigFixDiscovery.log` – pour les journaux de reconnaissance et d'exécution de script
- `$COLLATION_HOME/log/services/ApiServer.log` – pour les journaux d'extraction et d'analyse des résultats

3. Vérifiez si les journaux du serveur BigFix et la console BigFix contiennent des statuts d'échec.

4. Les journaux d'exécution **Bigfix ActionScript** peuvent être vérifiés au cas où le « **Sondage d'action** » serait en échec en raison du « **Serveur racine** » et du « **Noeud final** ».

Annexe A. Propriétés Collation.Properties utilisées dans l'intégration

1. Fonction BigFix activée

Tableau 50.

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation. bigfix.enabled	true/false	Si la valeur est true, la fonction BigFix sera activée. Après avoir défini cette propriété sur true, un redémarrage de TADDM est nécessaire.	O

2. Serveur BigFix

Tableau 51.

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation. bigfix.host	IP ou nom de domaine complet	IP ou nom de domaine complet du serveur BigFix	O
com.collation. bigfix.port	<N° de port> Par défaut = 52311	Port à travers lequel TADDM enverra la requête au serveur BigFix.	N
com.collation. bigfix.uid	<id utilisateur>	ID utilisateur permettant d'accéder à la console du serveur BigFix.	O

Tableau 51. (suite)

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation. bigfix.pwd	<mot de passe>	Mot de passe permettant d'accéder à la console du serveur BigFix. Sera stocké sous forme chiffrée.	O
com.collation. bigfix.connectTo	<période> Par défaut = 20 sec	TADDM attendra pendant cette période exprimée en secondes avant le dépassement du délai d'attente de la connexion HTTP ou de l'API Rest.	N
com.collation. bigfix.responseTo	<période> Par défaut = 20 sec	TADDM attendra pendant cette période exprimée en secondes avant le dépassement du délai d'attente de la réponse HTTP.	N
com.collation. bigfix.site.type	<type de site> Par défaut = personnalisé	Type du site sur le serveur BigFix auquel TADDM se connectera.	N
Visibility.Control. Automation	<nom de site>Par défaut = TADDM	Nom du site sur le serveur BigFix auquel TADDM se connectera.	N
com.collation. bigfix. aasdpkgmaxsize	<taille du package de demande> Par défaut = 1024	Taille maximale autorisée du package de demande généré par le script de reconnaissance BigFix.	N

3. Certificat du serveur BigFix

Tableau 52.

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation. bigfix.certificate.type	<PKCS12/JKS> Par défaut = JKS	Type de certificat client pris en charge.	N
com.collation. bigfix.certificate.file	<Chemin>	Emplacement du fichier de certificat client.	N
com.collation. bigfix.certificate.pwd	<Mot de passe>	Mot de passe du certificat client	N

4. Base de données du serveur BigFix

Tableau 53.

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation. bigfix.db.type	MSSQL ou DB2	Type de base de données utilisé par le serveur BigFix ; MSSQL pour un serveur BigFix sur Windows ou DB2 pour un serveur BigFix sur Linux.	O
com.collation. bigfix.db.host	IP ou nom de domaine complet	IP ou nom de domaine complet de la base de données BigFix	O
com.collation. bigfix.db.port	<N° de port>	Port sur lequel TADDM se connectera à la base de données BigFix.	O
com.collation. bigfix.db.dbname	<nom de base de données>	Nom de la base de données BigFix.	O
com.collation. bigfix.db.domain	<domaine utilisateur>	Domaine de l'utilisateur, obligatoire en cas d'authentification basée sur Windows.	N
com.collation. bigfix.db.domain	<id utilisateur>	ID utilisateur permettant d'accéder à la base de données BigFix.	O
com.collation. bigfix.db.pwd	<mot de passe>	Mot de passe permettant d'accéder à la base de données BigFix ; sera stocké sous forme chiffrée.	O

3. Vérifiez si les journaux du serveur BigFix et la console BigFix contiennent des statuts d'échec.

Remarque :

- En cas d'interruption de la connexion entre TADDM et la base de données, TADDM essaiera de se reconnecter au moyen du paramètre « com.collation.bigfix.result.wait ».
- En cas de modification des paramètres ci-dessus, un redémarrage de TADDM est nécessaire.

5. TADDM - Extraction de résultats/Unité d'exécution de traitement

Tableau 54.

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation. bigfix.result.wait	<valeur en seconde> Par défaut = 60 sec	Lorsque la propriété « com.collation.bigfix.enabled » est activée, l'unité d'exécution d'Extraction des résultats est générée afin d'extraire périodiquement les fichiers de résultats de reconnaissance à partir du serveur BigFix. L'« unité d'exécution d'Extraction des résultats » extraira les packages de résultats du serveur BigFix selon la périodicité (exprimée en secondes) configurée.	N
com.ibm.cdb. discover.asd. autodiscovery.enabled	True/false	Si la valeur est true, l'unité d'exécution pourra traiter les fichiers de résultats ASD stockés	O
com.ibm.cdb. discover.asd. ProcessUnreachableIPs	True/false	L'unité d'exécution traitera le résultat ASD pour les cibles qui sont inaccessibles.	O
com.ibm.cdb. discover.asd. AsyncDiscovery ResultsDirectory	Chemin par défaut = var/asdd	Chemin d'accès où les fichiers de résultats doivent être conservés. Le chemin d'accès est configurable mais défini sur var/asdd par défaut.	N
com.ibm.cdb. discover.asd. autodiscovery. asdScope	<nom de portée> Par défaut = ASD	L'unité d'exécution sélectionnera la cible mentionnée dans cette portée pour traiter le fichier de résultats. Si cette propriété n'est pas mentionnée, la portée par défaut ASD sera traitée.	N
com.ibm.cdb. discover.asd. autodiscovery. asdProfile	<nom de profil> Par défaut = ASD	L'unité d'exécution sélectionnera les détecteurs mentionnés dans ce profil pour traiter le fichier de résultats. Si cette propriété n'est pas mentionnée, le profil par défaut ASD sera traité.	N
com.ibm.cdb. discover.asd. autodiscovery. filesThreshold	<seuil de fichiers> Par défaut = 20	Nombre de fichiers minimum requis par unité d'exécution pour commencer leur traitement. L'unité d'exécution traitera le résultat si le seuil de fichier ou le seuil de durée est atteint.	N
com.ibm.cdb. discover.asd. autodiscovery. timeThreshold	<seuil de durée> Par défaut = 60sec	Seuil de durée au delà duquel l'unité d'exécution traitera les fichiers de résultats, même si le seuil de fichier n'est pas atteint.	N

Remarque : 1. Les résultats de BigFix Discovery arriveront de manière asynchrone sur le serveur TADDM et dès que l'une des propriétés (com.ibm.cdb.discover.asd.autodiscovery.filesThreshold, com.ibm.cdb.discover.asd.autodiscovery.timeThreshold) est atteinte, un groupe de

fichiers de résultats disponibles sera alors traité, ce qui créera une nouvelle entrée « Historique des reconnaissances ». Ces propriétés seront ajustées selon les exigences spécifiques pour contrôler le nombre d'entrées de l'« Historique des reconnaissances ».

6. Nettoyage

Tableau 55.

N° série	Ressources	Serveur TADDM		Serveur racine BES		Noeud final BES	
		Création	Nettoyage	Création	Nettoyage	Création	Nettoyage
1.	Package de demande	O	N[1]	O	N[2]	O	O
2.	Tâche	-	-	O	O[4]	-	-
3.	Action	-	-	O	O[3]	-	-
4.	Package de résultats	O	O	O	O	O	O
5.	Ensemble de fichiers	-	-	-	-	O	O

Remarque :

- Le nettoyage du package de demande sur le serveur TADDM n'est pas pris en charge
- Le nettoyage du package de demande sur le serveur racine BES n'est pas pris en charge. (Le package de demande peut être réutilisé pendant la nouvelle reconnaissance)
- Seules les actions qui ont été créées par TADDM et ont l'état Expiré pourront faire l'objet d'un nettoyage (excepté l'action créée avec le nom TADDMCLEANUP).
- Les tâches créées par TADDM ne seront supprimées que si toutes les actions associées à ces tâches ont déjà été supprimées.
- Les tâches créées par TADDM ne seront supprimées que si toutes les actions associées à ces tâches ont déjà été supprimées.
  - Pour exclure une tâche spécifique et ses actions associées du nettoyage (pour la prise en charge d'une nouvelle reconnaissance), il est possible d'utiliser le paramètre retainBigFixTask.sh/.bat en suivant les détails ci-dessous :

  Utilisation : ./retainBigFixTask.sh <nom_tâche> <activer/désactiver>

Nettoyage sur le serveur TADDM

Tableau 56.

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation.bigfix.taddm.cleanup.volume	<taille limite avec suffixe>	<Taille limite au delà de laquelle les anciens fichiers traités sont supprimés (par exemple, 50 Mo, 2 Go, etc.)>	N
com.collation.bigfix.taddm.cleanup.time	<durée limite avec suffixe>	<Permet d'identifier les fichiers traités plus anciens que les unités configurées (par exemple, 1 j, 5 h, 30 min, etc.)>	N

Tableau 56. (suite)

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation. bigfix.taddm. cleanup.runtime	Nombre de minutes	L'unité d'exécution de nettoyage de TADDM attendra pendant le nombre de minutes configuré après l'exécution.	N

Remarque :

- Le nettoyage des fichiers de résultats sur le serveur TADDM ne sera effectué que si au moins une des propriétés (com.collation.bigfix.taddm.cleanup.volume, com.collation.bigfix.taddm.cleanup.time) est configurée.

Nettoyage sur le noeud final

Tableau 57.

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation. bigfix.endpoint. cleanup	<O ou N> <Par défaut = O>	Si la valeur est O, le fichier zip du package de demande, le répertoire du package de demande extrait et le fichier zip du package de résultats nouvellement créé seront supprimés du point final	N

Nettoyage sur le serveur racine BigFix

Tableau 58.

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation. bigfix.root. cleanup.interval	<nombre de jours> <Par défaut = 1>	Fréquence d'exécution de la tâche de nettoyage pour supprimer les packages de résultats, les tâches et les actions à l'état Expiré du serveur racine BES.	N
com.collation. bigfix.root. cleanup.days	<nombre de jours> <Par défaut = 5>	Les fichiers de résultats plus anciens que le nombre de jours donné pourront être supprimés.	N

7. Pertinence personnalisée

Tableau 59.

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation. bigfix.relevance. appendscope	true/false <Par défaut = true>	Si la valeur est true, la requête de Pertinence personnalisée sera utilisée en plus de la portée indiquée Si la valeur est false, seule la requête de Pertinence personnalisée sera utilisée, à la place de la portée indiquée	N
com.collation. bigfix. relevance	True/false	Requête de pertinence permettant d'identifier un ensemble de noeuds finaux pour la reconnaissance donnée.	N

8. Paramètres de chemin temporaire du package BigFix

Tableau 60.

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation. bigfix.action. enable.os	<script d'action pour le système d'exploitation configuré><Par défaut = Windows, AIX, Linux, SunOS>	Le script d'action du système d'exploitation configuré sera inclus dans le langage des scripts d'action de Bigfix	N
com.collation. bigfix.temp. Windows	Chemin d'accès au package de demande<Par défaut = C:\Windows\ Temp>	Chemin d'accès qui sera utilisé pour le package de demande ASD. *Remarque : le caractère “\” doit être utilisé comme caractère “\\” dans un chemin d'accès Windows.	N
com.collation. asd.temp.Windows	Chemin d'accès au package de résultats <Par défaut = C:\Windows\ Temp>	Chemin d'accès qui sera utilisé pour les packages de résultats ASD.	N
com.collation. asd.temp.Unix	Chemin d'accès au package de résultats <Par défaut = /tmp>	Chemin d'accès qui sera utilisé pour les packages de résultats ASD.	N
com.collation. bigfix.temp.Linux	Chemin d'accès au package de résultats <Par défaut = /tmp>	Chemin d'accès qui sera utilisé pour le package de demande ASD.	N
com.collation. bigfix.temp. SunOS	Chemin d'accès au package de résultats <Par défaut = /tmp>	Chemin d'accès qui sera utilisé pour le package de demande ASD.	N

Tableau 60. (suite)

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation. bigfix.temp. AIX	Chemin d'accès au package de résultats <Par défaut = /tmp>	Chemin d'accès qui sera utilisé pour le package de demande ASD.	N

Remarque : En fonction du chemin d'accès temporaire configuré ci-dessus, le dossier sera créé sur des noeuds finaux cible s'il n'existe pas. Par exemple, sur Windows 2003, le chemin d'accès temporaire par défaut « C:\Windows\Temp\ » sera utilisé et ce dossier sera créé pendant la reconnaissance.

Annexe B. Paramètre de script pour différents modes

./runBigFixDiscovery.sh : outil TADDM permettant d'exécuter une reconnaissance BigFix étendue ou d'analyser une action de reconnaissance existante.

Mode : RECONNAÎTRE

utilisation : bin/runBigFixDiscovery.sh -d/--discover [-c <arg>] [-freq <arg>] [-h] [-intr <arg>] -o <arg> -p <arg> -s <arg>

où,

Tableau 61.

-c,--compressMethod <arg>	[Par défaut : ZIP] Valeurs possibles : [ZIP, TAR].
-freq,--frequency <arg>	[Par défaut : 1] Nombre de fois que la reconnaissance doit être exécutée.
-h,--help	afficher l'aide.
-intr,--interval <arg>	[Par défaut : P1D] Intervalle de temps entre les réexécutions de la reconnaissance. Valeurs prises en charge : [PT15M, PT30M, PT1H, PT2H, PT4H, PT6H, PT8H, PT12H, P1D, P2D, P3D, P5D, P7D, P15D, P30D].
-o,--output <arg>	OBLIGATOIRE : répertoire de sortie dans lequel le package de reconnaissance Bigfix sera généré.
-p,--profile <arg>	OBLIGATOIRE : Le nom de profil sera utilisé pour que la création du package de reconnaissance inclue des détecteurs.
-s,--scope	OBLIGATOIRE : nom/s Portée/GroupePortée (Séparés par des virgules. Noms d'enveloppe entre guillemets qui contiennent des espaces).

Mode : SONDER

utilisation : bin/runBigFixDiscovery.sh -p/--poll [-h] -i <arg> [-r <arg>] [-t <arg>]

où,

Tableau 62.

-d,--detail <arg>	[Par défaut : true] Résultat d'interrogation pour chaque noeud final
-h,--help	afficher l'aide.
-r,--repeat <arg>	[Par défaut : 1] Nombre d'interrogations pour obtenir le statut d'action
-i,--id <arg>	OBLIGATOIRE : ID action à INTERROGER
-t,--timeout <arg>	[Par défaut : 1] Intervalle entre deux SONDAGES consécutifs en secondes.

Mode : NETTOYER

utilisation : bin/runBigFixDiscovery.sh -c/--cleanup [-d <arg>] [-h]

où,

Tableau 63.

-h,--help	afficher l'aide.
-d,--days <arg>	[Par défaut : 5] Nettoyer les fichiers de résultats dont l'ancienneté est supérieure au nombre de jours spécifié

Mode : RECONNAÎTRE À NOUVEAU

utilisation : bin/runBigFixDiscovery.sh -r/--rediscover [-freq <arg>] [-h] [-intr <arg>]

où,

Tableau 64.

-freq,--frequency <arg>	[Par défaut : 1] Nombre de fois où la reconnaissance doit être exécutée
-h,--help	afficher l'aide.
-intr,--interval <arg>	[Par défaut : P1D] Intervalle de temps entre les réexécutions de la reconnaissance. Valeurs prises en charge : [PT15M, PT30M, PT1H, PT2H, PT4H, PT6H, PT8H, PT12H, P1D, P2D, P3D, P5D, P7D, P15D, P30D].

5. TADDM - Extraction de résultats/Unité d'exécution de traitement

Tableau 65.

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation. bigfix.result.wait	<valeur en seconde> Par défaut = 60 sec	Lorsque la propriété « com.collation.bigfix.enabled » est activée, l'unité d'exécution d'Extraction des résultats est générée afin d'extraire périodiquement les fichiers de résultats de reconnaissance à partir du serveur BigFix. L'« unité d'exécution d'Extraction des résultats » extraira les packages de résultats du serveur BigFix selon la périodicité (exprimée en secondes) configurée.	N
com.ibm.cdb. discover.asd. autodiscovery. enabled	True/false	Si la valeur est true, l'unité d'exécution pourra traiter les fichiers de résultats ASD stockés	O
com.ibm.cdb. discover.asd. ProcessUnreachableIPs	True/false	L'unité d'exécution traitera le résultat ASD pour les cibles qui sont inaccessibles.	O
com.ibm.cdb. discover.asd. AsyncDiscovery ResultsDirectory	Chemin par défaut = var/asdd	Chemin d'accès où les fichiers de résultats doivent être conservés. Le chemin d'accès est configurable mais défini sur var/asdd par défaut.	N
com.ibm.cdb. discover.asd. autodiscovery. asdScope	<nom_portée> Par défaut = ASD	L'unité d'exécution sélectionnera la cible mentionnée dans cette portée pour traiter le fichier de résultats. Si cette propriété n'est pas mentionnée, la portée par défaut ASD sera traitée.	N
com.ibm.cdb. discover.asd. autodiscovery. asdProfile	<nom_profil> Par défaut = ASD	L'unité d'exécution sélectionnera les détecteurs mentionnés dans ce profil pour traiter le fichier de résultats. Si cette propriété n'est pas mentionnée, le profil par défaut ASD sera traité.	N
com.ibm.cdb. discover.asd. autodiscovery. filesThreshold	<seuil_fichier> Par défaut = 20	Nombre de fichiers minimum requis par unité d'exécution pour commencer leur traitement. L'unité d'exécution traitera le résultat si le seuil de fichier ou le seuil de durée est atteint.	N

Tableau 65. (suite)

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.ibm.cdb. discover.asd. autodiscovery. timeThreshold	<seuil_durée> Par défaut = 60 sec	Seuil de durée au delà duquel l'unité d'exécution traitera les fichiers de résultats, même si le seuil de fichier n'est pas atteint.	N

Remarque : 1. Les résultats de BigFix Discovery arriveront de manière asynchrone sur le serveur TADDM et dès que l'une des propriétés (com.ibm.cdb.discover.asd.autodiscovery.filesThreshold, com.ibm.cdb.discover.asd.autodiscovery.timeThreshold) est atteinte, un groupe de fichiers de résultats disponibles sera alors traité, ce qui créera une nouvelle entrée « Historique des reconnaissances ». Ces propriétés seront ajustées selon les exigences spécifiques pour contrôler le nombre d'entrées de l'« Historique des reconnaissances ».

6. Nettoyage

Tableau 66.

N° série	Ressources	Serveur TADDM		Serveur racine BES		Noeud final BES	
		Création	Nettoyage	Création	Nettoyage	Création	Nettoyage
1.	Package de demande	O	N[1]	O	N[2]	O	O
2.	Tâche	-	-	O	O[4]	-	-
3.	Action	-	-	O	O[3]	-	-
4.	Package de résultats	O	O	O	O	O	O
5.	Ensemble de fichiers	-	-	-	-	O	O

Remarque :

- Le nettoyage du package de demande sur le serveur TADDM n'est pas pris en charge
- Le nettoyage du package de demande sur le serveur racine BES n'est pas pris en charge. (Le package de demande peut être réutilisé pendant la nouvelle reconnaissance)
- Seules les actions qui ont été créées par TADDM et ont l'état Expiré pourront faire l'objet d'un nettoyage (excepté l'action créée avec le nom TADDMCLEANUP).
- Les tâches créées par TADDM ne seront supprimées que si toutes les actions associées à ces tâches ont déjà été supprimées.
- Les tâches créées par TADDM ne seront supprimées que si toutes les actions associées à ces tâches ont déjà été supprimées.
  - Pour exclure une tâche spécifique et ses actions associées du nettoyage (pour la prise en charge d'une nouvelle reconnaissance), il est possible d'utiliser le paramètre retainBigFixTask.sh/.bat en suivant les détails ci-dessous :

  Utilisation : ./retainBigFixTask.sh <nom_tâche> <activer/désactiver>

Nettoyage sur le serveur TADDM

Tableau 67.

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation. bigfix.taddm. cleanup.volume	<taille limite avec suffixe>	<Taille limite au delà de laquelle les anciens fichiers traités sont supprimés (par exemple, 50 Mo, 2 Go, etc.)>	N
com.collation. bigfix.taddm. cleanup.time	<durée limite avec suffixe>	<Permet d'identifier les fichiers traités plus anciens que les unités configurées (par exemple, 1 j, 5 h, 30 min, etc.)>	N
com.collation. bigfix.taddm. cleanup.runtime	Nombre de minutes	L'unité d'exécution de nettoyage de TADDM attendra pendant le nombre de minutes configuré après l'exécution.	N

Remarque :

- Le nettoyage des fichiers de résultats sur le serveur TADDM ne sera effectué que si au moins une des propriétés (com.collation.bigfix.taddm.cleanup.volume, com.collation.bigfix.taddm.cleanup.time) est configurée.

Nettoyage sur le noeud final

Tableau 68.

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation. bigfix.endpoint. cleanup	<O ou N><Par défaut = O>	Si la valeur est O, le fichier zip du package de demande, le répertoire du package de demande extrait et le fichier zip du package de résultats nouvellement créé seront supprimés du point final	N

Nettoyage sur le serveur racine BigFix

Tableau 69.

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation. bigfix.root. cleanup.interval	<nombre de jours> <Par défaut = 1>	Fréquence d'exécution de la tâche de nettoyage pour supprimer les packages de résultats, les tâches et les actions à l'état Expiré du serveur racine BES.	N
com.collation. bigfix.root. cleanup.days	<nombre de jours> <Par défaut = 5>	Les fichiers de résultats plus anciens que le nombre de jours donné pourront être supprimés.	N

7. Pertinence personnalisée

Tableau 70.

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation. bigfix.relevance. appendscope	true/false <Par défaut = true>	Si la valeur est true, la requête de Pertinence personnalisée sera utilisée en plus de la portée spécifiée Si la valeur est false, seule la requête de Pertinence personnalisée sera utilisée à la place de la portée spécifiée	N
com.collation. bigfix.relevance	True/false	Requête de pertinence permettant d'identifier un ensemble de noeuds finaux pour la reconnaissance donnée.	N

8. Paramètres de chemin temporaire du package BigFix

Tableau 71.

Nom de la propriété	Valeurs possibles	Description	Obligatoire
com.collation. bigfix.action. enable.os	<script d'action pour le système d'exploitation configuré> <Par défaut = Windows, AIX, Linux, SunOS>	Le script d'action du système d'exploitation configuré sera inclus dans le langage des scripts d'action de Bigfix	N
com.collation. bigfix.temp. Windows	Chemin d'accès au package de demande <Par défaut = C:\Windows\Temp>	Chemin d'accès qui sera utilisé pour le package de demande ASD. *Remarque : le caractère “\” doit être utilisé comme caractère “\\” dans un chemin d'accès Windows.	N
com.collation. asd.temp. Windows	Chemin d'accès au package de résultats <Par défaut = C:\Windows\Temp>	Chemin d'accès qui sera utilisé pour les packages de résultats ASD.	N
com.collation. asd.temp. Unix	Chemin d'accès au package de résultats <Par défaut = /tmp>	Chemin d'accès qui sera utilisé pour les packages de résultats ASD.	N
com.collation. bigfix.temp. Linux	Chemin d'accès au package de résultats <Par défaut = /tmp>	Chemin d'accès qui sera utilisé pour le package de demande ASD.	N
com.collation. bigfix.temp. SunOS	Chemin d'accès au package de résultats <Par défaut = /tmp>	Chemin d'accès qui sera utilisé pour le package de demande ASD.	N
com.collation. bigfix.temp. AIX	Chemin d'accès au package de résultats <Par défaut = /tmp>	Chemin d'accès qui sera utilisé pour le package de demande ASD.	N

Remarque : En fonction du chemin d'accès temporaire configuré ci-dessus, le dossier sera créé sur des noeuds finaux cible s'il n'existe pas. Par exemple, sur Windows 2003, le chemin d'accès temporaire par défaut « C:\Windows\Temp\ » sera utilisé et ce dossier sera créé pendant la reconnaissance.

Annexe C. Exemple pour vérifier l'exécution des scripts

1. Exécution du script encryptprops.sh

```
/opt/IBM/taddm/dist/bin/encryptprops.sh $COLLATION_HOME
```

2. Exécution du script runBigFixDisocvery.sh

```
TADDM Server  – 9.167.42.227 (Linux)
BigFix server     – 10.160.161.195 (windows)
BigFix endpoints        – 10.160.161.196 (windows)
                           10.160.161.212 (windows)
Scope       – ASD (having both BigFix endpoints)
Profile           - ASD (having sensors mentioned in section 2.2)
Configuration     - done as per section 3.
```

a. Démarrage de la reconnaissance :

```
[taddmusr@nc042227 bin]$ ./runBigFixDiscovery.sh -d -o /tmp -p ASD -s ASD
BigFix Action will be applied total [1] times with [P1D] interval

Task created on BES server with Name [20170828083852] and Action created with ID [633]

DISCOVER: LAUNCH OK
The Bigfix Discovery script exited successfully.
```

b. Nom de la tâche : 20170828083852, Identificateur d'action : 633

c. Démarrage du sondage :

```
[taddmusr@nc042227 bin]$ ./runBigFixDiscovery.sh -p -i 633
Repeatedly poll the BigFix Action [1] number of times for every [1] seconds
Total [2] Computers returned for Action with ID [633] has status: Open

Total [1] computers with status : The action executed successfully.
[Hostname] [Apply Count] [Line Number] [Start Time] [End Time]
[PNC161196] [1] [98] [Mon, 28 Aug 2017 14:43:56 +0000] [Mon, 28 Aug 2017 14:44:11 +0000]

Total [1] computers with status : The action failed.
[Hostname] [Apply Count] [Line Number] [Start Time] [End Time]
[PRODUCTIONWASB] [1] [37] [Mon, 28 Aug 2017 07:40:26 +0000] [Mon, 28 Aug 2017 07:40:26 +0000]

POLL FINISHED
The Bigfix Discovery script exited successfully
```

Démarrage du nettoyage :

```
[taddmusr@nc042227 bin]$ ./runBigFixDiscovery.sh -c
CLEANUP TASK FOUND: TADDMCLEANUP with ID: 2067

Cleanup Action created with ID: [2068]

CLEANUP: LAUNCH OK
The Bigfix Discovery script exited successfully
```

Démarrage de la nouvelle reconnaissance :

```
[taddmusr@nc042227 bin]$ ./runBigFixDiscovery.sh –r –i 20171117085907

TASK FOUND : 20171117085907 with ID : 2075

Action created with ID: [2086]

REDISCOVERY: LAUNCH OK
The Bigfix Discovery script exited successfully.
```

Annexe D. Codes d'erreur et description

Tableau 72.

ID message	M : Message, C : Cause, E : Effet
CTJTD1260E	M : Bigfix Discovery n'est pas activé, Configurez com.collation.bigfix.enabled dans collation.properties E : Le script de Bigfix Discovery ne s'exécutera pas et l'unité d'exécution pour l'extraction des résultats ne sera pas appelée
CTJTD1261E	M : Arguments manquants ou incorrects C : Tentative d'exécution du script dans un mode autre que Reconnaître, Sonder, Nettoyer ou Reconnaître à nouveau E : Le script ne s'exécutera pas
CTJTD1262E	M : Format numérique fourni incorrect C : Les propriétés ou arguments sont indiqués au format chaîne alors qu'ils doivent être au format numérique E : Le script de BigFix Discovery ne s'exécutera pas et l'unité d'exécution pour l'extraction des résultats ne fonctionnera pas correctement
CTJTD1263E	M : Echec de l'analyse des propriétés de la ligne de commande : <nom de la propriété> C : Les arguments transmis lors de l'exécution des scripts ne sont pas pris en charge E : Le mode script ne sera pas appelé
CTJTD1264E	M : <Nom de la propriété> est manquant dans collation.properties C : Lors de l'exécution du script, la ou les propriétés obligatoires sont manquantes ou non valides (voir l'Annexe A) E : Le script de BigFix Discovery ne s'exécutera pas et l'unité d'exécution pour l'extraction des résultats ne fonctionnera pas correctement
CTJTD1265I	M : Seule la pertinence personnalisée sera utilisée, au lieu de la portée indiquée
CTJTD1266I	M : La pertinence personnalisée sera utilisée en plus de la portée indiquée
CTJTD1267E	M : Portée vide indiquée, aucun élément trouvé C : La portée ou le groupe de portées indiqué ne contient aucun élément pour définir le noeud final E : La reconnaissance ne sera pas appelée
CTJTD1268E	M : Aucun détecteur disponible ou activé dans le profil spécifié C : Le profil indiqué ne contient aucun détecteur E : La reconnaissance ne sera pas appelée
CTJTD1269E	M : Le package de demande AASD n'existe pas C : Problème lors de la création du package de demande, droits insuffisants ou package inexistant pour le téléchargement E : La reconnaissance ne sera pas appelée

Tableau 72. (suite)

ID message	M : Message, C : Cause, E : Effet
CTJTD1270E	M : La taille du package AASD est supérieure au seuil com.collation.bigfix.aasdpkgmaxsize configuré C : La taille du package de demande créé est supérieure au seuil configuré E : La reconnaissance ne sera pas appelée
CTJTD1271E	M : Impossible de se connecter à BigFix en raison de : <cause> C : Problème de connexion au service Web de Bigfix dû à des paramètres ou un certificat non valides. E : Le package ne sera pas téléchargé et la reconnaissance ne sera pas appelée
CTJTD1272E	M : Erreur décelée lors de la configuration : <cause> C : Scénario inattendu pour du code qui n'est pas traité E : L'exécution du script ne fonctionnera pas correctement
CTJTD1273I	M : Script principal pour (ré)exécuter BigFix Discovery, sonder une action de reconnaissance spécifiée ou exécuter un nettoyage manuel

Remarques

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. Toute référence à un produit, logiciel ou service IBM n'établit ou n'implique 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 toutefois de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, programmes 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
Armonk, NY 10504-1785 U.S.A.

Les informations sur les licences concernant les produits qui utilisent un jeu de caractères double octet peuvent être obtenues auprès du service de la propriété intellectuelle d'IBM de votre pays l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales :

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, améliorer et/ou 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 Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 Etats-Unis

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'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

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.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Le présent document contient des exemples de données et de rapports utilisés dans les opérations quotidiennes d'une entreprise. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Tous ces noms sont fictifs et toute ressemblance avec des noms et des adresses utilisés par une véritable entreprise serait purement fortuite.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur ne s'affichent pas.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et services 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 http://www.ibm.com/legal/copytrade.shtml.

Java et toutes les marques et logos incluant Java sont des marques d'Oracle et/ou de ses affiliés.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Microsoft et 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.

Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.

Imprimé en France