Tivoli® Federated Identity Manager
Version 6.2.1

Guide de configuration

IBM

GC11-6781-00

Tivoli® Federated Identity Manager
Version 6.2.1

Guide de configuration

IBM

GC11-6781-00

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 553.

Première édition - juin 2010

Réf. US : GC27-2719-00

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.can.ibm.com (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

Table des matières

Figures

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 ce document

IBM® Tivoli Federated Identity Manager Version 6.2.1 implémente des solutions de connexion unique fédérée, de gestion de sécurité de service Web et d'application des accès basées sur des normes ouvertes. IBM Tivoli Federated Identity Manager étend les solutions d'authentification et d'autorisation fournies par IBM Tivoli Access Manager afin de simplifier l'intégration de plusieurs solutions Web existantes.

Ce guide décrit comment configurer IBM Tivoli Federated Identity Manager.

Public ciblé

Ce guide s'adresse aux architectes de la sécurité des réseaux, aux administrateurs système, aux administrateurs de réseau et aux intégrateurs système. Les lecteurs doivent savoir gérer les aspects de la sécurité des réseaux, la technologie de chiffrement, les clés et les certificats. Ils doivent également avoir une bonne connaissance de la mise en oeuvre des règles d'authentification et d'autorisation dans un environnement réparti.

Le présent guide décrit une mise en oeuvre d'une solution de services Web qui prend en charge plusieurs normes des services Web. Les lecteurs doivent connaître les normes des services Web spécifiques, telles qu'elle sont extraites de la documentation diffusée par l'organisme de normalisation pour chacune des normes concernées.

Les lecteurs doivent avoir une bonne connaissance du développement et du déploiement des applications à utiliser dans un environnement de services Web. Cela inclut une expérience en déploiement d'applications dans un environnement IBM WebSphere Application Server.

Publications

Consultez les descriptions de la bibliothèque IBM Tivoli Federated Identity Manager, les publications prérequises et connexes afin de déterminer lesquelles vous seront utiles. La section décrit également comment accéder aux publications Tivoli en ligne et comment les commander.

Bibliothèque IBM Tivoli Federated Identity Manager

Les documents de la bibliothèque IBM Tivoli Federated Identity Manager sont les suivants :

- *IBM Tivoli Federated Identity Manager - Guide de démarrage rapide*

  Fournit des instructions pour la mise en route d'IBM Tivoli Federated Identity Manager.
- *IBM Tivoli Federated Identity Manager - Guide d'installation*

  Fournit des instructions pour l'installation d'IBM Tivoli Federated Identity Manager.

- *IBM Tivoli Federated Identity Manager - Guide de configuration*

  Fournit des instructions pour la configuration d'IBM Tivoli Federated Identity Manager.
- *IBM Tivoli Federated Identity Manager for z/OS Program Directory*

  Fournit des instructions pour l'installation d'IBM Tivoli Federated Identity Manager sur z/OS.
- *IBM Tivoli Federated Identity ManagerGuide d'administration*

  Fournit des instructions pour réaliser les tâches d'administration nécessaires à tous les déploiements.
- *IBM Tivoli Federated Identity Manager - Guide de gestion de la sécurité des services Web*

  Fournit des instructions pour réaliser les tâches de configuration nécessaires à la gestion de la sécurité des services Web.
- *IBM Tivoli Federated Identity Manager - Guide d'audit*

  Fournit des instructions pour effectuer un audit des événements IBM Tivoli Federated Identity Manager.
- *IBM Tivoli Federated Identity Manager Error Message Reference*

  Fournit des explications sur les messages d'erreur d'IBM Tivoli Federated Identity Manager.
- *IBM Tivoli Federated Identity Manager - Guide d'identification des problèmes*

  Fournit des informations pour l'identification des incidents et des instructions pour les résoudre.

Vous pouvez vous procurer les publications à partir du centre de documentation d'IBM Tivoli Federated Identity Manager :

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.tivoli.fim.doc_6.2.1/toc.xml

Publications prérequises

Pour utiliser efficacement le présent guide, vous devez vous familiariser avec les logiciels associés en consultant les sources suivantes :

- Centre de documentation d'IBM Tivoli Access Manager for e-business :

  http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.itame.doc/toc.xml
- Centre de documentation d'IBM WebSphere Application Server Version 6.1 :

  http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp

  Vous pouvez obtenir les versions PDF de la documentation IBM WebSphere Application Server à l'adresse :

  http://www.ibm.com/software/webservers/appserv/was/library/

Documentation associée

Vous pouvez obtenir les publications connexes sur les sites Web d'IBM :

- Le Centre de documentation d'IBM Tivoli Federated Identity Manager Business Gateway Information Center à l'adresse
- *Enterprise Security Architecture avec IBM Tivoli Security Solutions*. Ce guide est disponible au format PDF (Portable Document Format) à l'adresse http://www.redbooks.ibm.com/redbooks/pdfs/sg246014.pdf ou au format HTML (Hypertext Markup Language) à l'adresse http://www.redbooks.ibm.com/redbooks/SG246014/
- *Federated Identity Management et Web Services Security avec IBM Tivoli Security Solutions* (SG24-6394-01). Ce manuel est disponible au format PDF à l'adresse http://www.redbooks.ibm.com/redbooks/pdfs/sg246394.pdf ou au format HTML à l'adresse http://www.redbooks.ibm.com/redbooks/SG246394/
- La bibliothèque de logiciels Tivoli offre une grande diversité de documents Tivoli tels que des livres blancs, des fiches techniques, des démonstrations, des livres rouges et des lettres d'annonces. La bibliothèque de logiciels Tivoli est disponible sur le Web à l'adresse suivante : http://publib.boulder.ibm.com/tividd/td/tdprodlist.html
- Le document *Tivoli Software Glossary* inclut des définitions pour de nombreux termes techniques liés au logiciel Tivoli. Le document *Tivoli Software Glossary* est disponible à l'adresse suivante :http://publib.boulder.ibm.com/tividd/glossary/tivoliglossarymst.htm

Accès à la terminologie en ligne

Le site terminologique Web rassemble la terminologie relative aux bibliothèques des produits IBM à un seul emplacement pratique. Vous pouvez accéder au site Web de terminologie à l'adresse http://www.ibm.com/software/globalization/terminology

Accès aux publications en ligne

Post publications IBM pour ce produit et les autres produits Tivoli, dès qu'ils sont disponibles et mis à jour, dans le centre de documentation Tivoli à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp.

Remarque : Si vous imprimez les documents PDF au format autre que lettre, définissez l'option dans la fenêtre **Fichier → Imprimer** permettant à Adobe® Reader d'imprimer des pages de taille de lettre sur votre papier local.

Commande de publications

Vous pouvez commander de nombreuses publications Tivoli en ligne sur le site Web suivant : http://www.elink.ibmlink.ibm.com/public/applications/cgibin/pbi.cgi

Vous pouvez également passer votre commande par téléphone en composant l'un des numéros suivants :

- Aux Etats-Unis : 800-879-2755
- Au Canada : 800-426-4968

Pour obtenir la liste des numéros de téléphone pour les autres pays, voir le site Web suivant : http://www.ibm.com/software/tivoli/order-lit/

Accessibilité

Les fonctions d'accessibilité permettent à un utilisateur souffrant d'un handicap physique, comme une mobilité réduite ou une vision limitée, d'utiliser plus facilement les logiciels. Ce logiciel permet d'utiliser des technologies d'assistance pour entendre les commandes et naviguer dans l'interface. Il permet également d'utiliser le clavier à la place de la souris pour activer toutes les fonctions de l'interface graphique.

Pour plus d'informations, voir la rubrique "Accessibilité" dans le centre de documentation à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.tivoli.fim.doc_6.2.1/toc.xml.

Formation technique Tivoli

Pour obtenir des informations sur la formation technique Tivoli, consulte le site Web IBM Tivoli à l'adresse http://www.ibm.com/software/tivoli/education.

Informations de support

Si vous rencontrez un problème avec votre logiciel IBM, vous souhaitez le résoudre rapidement. IBM vous propose différentes manières d'obtenir l'aide dont vous avez besoin :

En ligne
Accédez au site du support logiciel IBM à l'adresse http://www.ibm.com/software/support/probsub.html et suivez les instructions.

IBM Support Assistant
L'assistant IBM Support Assistant (ISA) est un outil de support logiciel local et gratuit, qui vous permet de trouver des réponses aux questions et aux incidents liés à l'utilisation d'un logiciel IBM. L'assistant ISA fournit un accès rapide aux informations d'aide et aux outils de mise en service pour la détermination d'un problème. Pour installer le logiciel ISA, voir le document *IBM Tivoli Federated Identity Manager - Guide d'installation*. Voir également : http://www.ibm.com/software/support/isa.

Guide d'identification des problèmes
Pour plus d'informations sur la résolution des problèmes, voir *IBM Tivoli Federated Identity Manager - Guide d'identification des problèmes*.

Conventions utilisées dans ce document

Ce document utilise plusieurs conventions typographiques pour signaler des actions et des termes particuliers, ainsi que des commandes et des chemins d'accès spécifiques du système d'exploitation.

Conventions typographiques

Cette publication utilise les conventions typographiques suivantes :

Gras

- Commandes en minuscules ou majuscules-minuscules combinées difficiles à distinguer du texte environnant
- Composants d'interface (cases à cocher, boutons de fonction, boutons radio, sélecteurs rotatifs, zones, dossiers, icônes, listes déroulantes, options des listes déroulantes, listes à colonnes multiples, conteneurs, options de menu, noms de menus, onglets et pages de propriétés) et intitulés de rubrique (tels que **Astuce :** ou **Spécificité liée au système d'exploitation** :)
- Mots clés et paramètres du texte

Italique

- Citations (exemple : titres des publications, disquettes et CD)
- Mots définis dans le texte (exemple : une ligne spécialisée est appelée une *ligne point-à-point*)
- Emphase mise sur les mots et les lettres (mots en mots, exemple : "Utilisez le mot *que* pour commencer une clause restrictive."; lettres en lettres, exemple : "L'adresse LUN doit commencer par la lettre *L*.")
- Nouveaux termes du texte (sauf dans une liste de définitions) : une *vue* est un cadre dans un espace de travail contenant des données.
- Variables et valeurs à saisir : ... où *valeur1* repésente....

Espacement simple

- Exemples et exemples de code
- Noms de fichier, mots clés de programmation et autres éléments difficiles à distinguer du texte environnant
- Texte des messages et invites destinés à l'utilisateur
- Texte que l'utilisateur doit taper
- Valeurs des arguments ou des options de commande

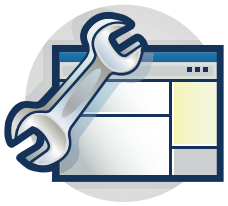
Variables et chemins de système d'exploitation

Le présent document utilise la convention UNIX® pour la spécification des variables d'environnement pour la notation des répertoires.

Lorsque vous utilisez la ligne de commande Windows®, remplacez la **$***variable* par la **%** *variable***%** pour les variables d'environnement et remplacez chaque barre oblique (*/*) par une barre oblique inverse (\) dans les noms de chemin des répertoires. Les noms des variables d'environnement ne sont pas toujours les mêmes dans les environnements Windows et UNIX. Par exemple, %TEMP% dans les environnements Windows est équivalent à $TMPDIR dans les environnements UNIX.

Remarque : Si vous utilisez le shell bash sur un système Windows, vous pouvez vous servir des conventions UNIX.

Partie 1. Configuration d'un domaine



Les rubriques de la section Configuration vous guident pas à pas lors de la configuration d'un domaine. La console de gestion est dotée d'assistants qui vous guident dans de nombreuses tâches de configuration.

Tous les déploiements Tivoli Federated Identity Manager nécessitent le déploiement d'un domaine. Vous devez déployer un domaine avant de configurer d'autres fonctions telles que la fédération de connexion unique, la gestion de sécurité des services Web, les services de jeton ou User Self Care.

Démarrez par la rubrique :

- Chapitre 1, «Configuration de domaine», à la page 3

Chapitre 1. Configuration de domaine

Un domaine Tivoli Federated Identity Manager est un déploiement du composant d'exécution Tivoli Federated Identity Manager sur un serveur WebSphere unique ou sur un cluster WebSphere.

Il existe un domaine par cluster WebSphere. Un environnement comportant un serveur unique ne peut contenir qu'un seul domaine.

Chaque domaine est géré indépendamment. Vous pouvez utiliser le processus d'installation de la console de gestion Tivoli Federated Identity Manager pour gérer plusieurs domaines. Vous ne pouvez gérer qu'un seul domaine à un moment donné. Le domaine à gérer est désigné par *domaine actif*.

Une fois que Tivoli Federated Identity Manager est installé, aucun domaine n'existe. Pour créer un domaine, utilisez la console de gestion. Une fois Tivoli Federated Identity Manager installé, le service de gestion est déployé sur un serveur WebSphere (mode serveur unique) ou sur un gestionnaire de déploiement WebSphere (mode cluster WebSphere). Vous allez vous connecter à ce service de gestion et choisir un serveur ou un cluster WebSphere sur lequel déployer le composant d'exécution Tivoli Federated Identity Manager. Une fois que le module d'exécution est déployé et configuré, vous êtes prêt à configurer les fonctionnalités complémentaires telles que la connexion unique fédérée ou la gestion de la sécurité des services Web.

Dans un environnement WebSphere Network Deployment, le déploiement et la configuration du module d'exécution Tivoli Federated Identity Manager sur les membres du cluster constituent un processus automatisé. Il n'est pas nécessaire d'installer également les logiciels Tivoli Federated Identity Manager ou Tivoli Access Manager sur les ordinateurs WebSphere en cluster. Le déploiement et la configuration du module d'exécution sur les membres de cluster distribués sont exécutés par le service de gestion Tivoli Federated Identity Manager à l'aide des services de déploiement d'application de WebSphere Deployment Manager.

La console de gestion offre un assistant qui vous guidera tout au long de la création du domaine. Les sections ci-après répertorient les propriétés que l'assistant vous invite à spécifier.

Propriétés des noeuds finals de service de gestion de domaine

Hôte Nom de domaine complet de l'**hôte** sur lequel WebSphere Application Server est en cours d'exécution. Par exemple :

```
idp.exemple.com
```

Port de connexion SOAP
Le port SOAP (autonome) par défaut WebSphere Application Server est 8880. Lors de la création d'un domaine pour un serveur WebSphere Application Server qui fait partie d'un cluster WebSphere, le numéro de port SOAP peut s'avérer différent. Par exemple, 8879. Si vous avez un doute sur le numéro de port SOAP correct, utilisez la console d'administration de WebSphere Application Server pour déterminer le port.

Propriétés de sécurité globale WebSphere

WebSphere Application Server est doté d'une option d'activation de sécurité globale. Lorsque la sécurité globale est activée, les propriétés de sécurité doivent être configurées pour le service de gestion Tivoli Federated Identity Manager. La sécurité globale est activée dans la plupart des déploiements.

Remarque relative à z/OS : Lors du déploiement sous z/OS, WebSphere est généralement configuré en vue d'utiliser un fichier de clés RACF (ou un autre logiciel de sécurité) avec les certificats. Pour obtenir des instructions sur la configuration de certificats utilisés avec Tivoli Federated Identity Manager sur z/OS, consultez le document README sur le média de distribution z/OS. Ces instructions décrivent la méthode permettant d'extraire un certificat dans un fichier de clés RACF et de l'ajouter à un fichier de clés Java™ destiné à être utilisé par Tivoli Federated Identity Manager. Le fichier de clés sécurisé, ainsi que les fichiers et mots de passe client optionnels créés à l'aide de ces instructions, doivent être utilisés en remplacement des valeurs par défaut (par exemple, le fichier trust.p12) indiquées ci-dessous.

Nom de l'utilisateur d'administration
Nom de l'administrateur WebSphere Application Server. Par exemple : `wsadmin`

Mot de passe d'administration
Mot de passe de l'administrateur WebSphere Application Server tel qu'il a été spécifié lors de l'installation de WebSphere.

Fichier de clés certifiées SSL
Fichier de clés utilisé par WebSphere Application Server.

Si vous avez installé Tivoli Federated Identity Manager sur un ordinateur hébergeant une installation WebSphere existante, le chemin d'accès par défaut sous Linux® ou UNIX est le suivant :

```
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/etc/trust.p12
```

Sous Windows :

```
C:\Program Files\IBM\WebSphere\AppServer\
  profiles\AppSrv01\etc\trust.p12
```

Si vous avez installé l'instance WebSphere intégrée dans le cadre de l'installation de Tivoli Federated Identity Manager, le chemin d'accès par défaut sous Linux ou UNIX est le suivant :

```
/opt/IBM/FIM/ewas/profiles/
 itfimProfile/etc/trust.p12
```

Sous Windows :

```
C:\Program Files\IBM\FIM\ewas\
   profiles\AppSrv01\etc\trust.p12
```

Mot de passe du fichier de clés certifiées SSL
Mot de passe requis pour l'accès au fichier de clés certifiées SSL.

Le mot de passe par défaut pour la clé WebSphere est le suivant :

```
WebAS
```

Fichier de clés client SSL
Fichier de clés utilisé par WebSphere Application Server.

Ce fichier de clés est un élément de configuration optionnel. Certains déploiements WebSphere ne nécessitent aucun fichier de clés client SSL.

Mot de passe du fichier de clés client SSL
Mot de passe requis pour l'accès au fichier de clés client SSL. Cette zone doit être renseignée lorsque vous avez entré un fichier de clés client SSL.

Nom de serveur ou cluster WebSphere

Lors de la création d'un domaine, l'assistant de domaine vous demande le nom de serveur ou de cluster WebSphere.

Nom du serveur
Nom de l'instance WebSphere Application Server sur laquelle le service de gestion Tivoli Federated Identity Manager doit être configuré.

Le serveur correspond à un serveur unique et ne fait pas partie d'un cluster.

Le nom par défaut est créé automatiquement par l'assistant. A titre d'exemple, pour un hôte appelé `host1` :

```
WebSphere:cell=host1Node01Cell,node=host1Node01,server=server1
```

Nom de cluster
Nom du cluster WebSphere Application Server sur lequel le service de gestion Tivoli Federated Identity Manager doit être configuré.

Propriétés d'environnement Tivoli Access Manager

L'assistant vous invite à préciser su vous devez ou non effectuer la configuration dans un environnement Tivoli Access Manager. N'effectuez *pas* la configuration dans un environnement Tivoli Access Manager si vous utilisez un serveur point de contact autre que WebSEAL. A titre d'exemple, n'effectuez *pas* la configuration dans un environnement Tivoli Access Manager si vous utilisez WebSphere en tant que serveur point de contact.

L'invite affichée par l'assistant est la suivante :

Cet environnement utilise Tivoli Access Manager
Si vous ne cochez pas cette case, vous n'aurez besoin de configurer aucune propriété pour Tivoli Access Manager.

Si vous cochez cette case, vous devez spécifier les propriétés indiquées dans le tableau suivant

Nom d'utilisateur de l'administrateur
Administrateur Tivoli Access Manager. L'ID par défaut est sec_master. Si vous avez choisi un autre ID administrateur lors de l'installation de Tivoli Access Manager, entrez-le dans cette zone.

Mot de passe de l'administrateur
Mot de passe de l'administrateur Tivoli Access Manager.

Nom d'hôte du serveur de règles
Nom d'hôte complet de l'ordinateur qui exécute le serveur de règles de Tivoli Access Manager. Par exemple :

```
idp.exemple.com
```

Port Numéro de port permettant de communiquer avec le serveur de règles. Il correspond au numéro que vous avez indiqué lors de la configuration de Tivoli Access Manager. La valeur par défaut de Tivoli Access Manager est `7135`.

Nom d'hôte du serveur d'autorisations
Nom d'hôte complet de l'ordinateur qui exécute le serveur d'autorisations de Tivoli Access Manager. Par exemple :

```
idp.exemple.com
```

Port Numéro de port permettant de communiquer avec le serveur d'autorisations. Il correspond au numéro que vous avez indiqué lors de la configuration de Tivoli Access Manager. La valeur par défaut de Tivoli Access Manager est `7136`.

Domaine Tivoli Access Manager
Nom du domaine d'administration Tivoli Access Manager que vous avez indiqué lors de la configuration de ce dernier. La valeur par défaut est `Default`.

Formulaire de configuration de domaine

Complétez ce formulaire avant d'exécuter l'assistant de création et de déploiement du domaine et de l'environnement d'exécution.

Les propriétés spécifiées dans ce formulaire sont décrites au Chapitre 1, «Configuration de domaine», à la page 3

Tableau 1. Propriétés de configuration du domaine

Propriété	**Votre valeur**
Hôte	
Port de connexion SOAP	
Nom de l'utilisateur d'administration	
Mot de passe d'administration	
Fichier de clés certifiées SSL	
Mot de passe du fichier de clés certifiées SSL	
Fichier de clés client SSL	
Mot de passe du fichier de clés client SSL	
Nom du cluster WebSphere ou Nom du serveur WebSphere	
Cet environnement utilise Tivoli Access Manager	Sélectionnez ou désélectionnez

Lorsque votre environnement inclut Tivoli Access Manager (par exemple, lors de l'utilisation de WebSEAL en tant que serveur point de contact), vous devez également fournir un certain nombre de propriété de configuration de Tivoli Access Manager

Tableau 2. Propriétés d'environnement Tivoli Access Manager

Propriété	Description
Nom d'utilisateur de l'administrateur	
Mot de passe de l'administrateur	
Nom d'hôte du serveur de règles	
Port	
Nom d'hôte du serveur d'autorisations	
Port	
Domaine Tivoli Access Manager	La valeur par défaut est `Default`.

Création et déploiement d'un nouveau domaine

Vous devez créer un domaine et déployer un module d'exécution pour chaque instance de Tivoli Federated Identity Manager. Cette tâche est une condition requis pour la configuration de fonctionnalités complémentaires de Tivoli Federated Identity Manager telles que la gestion de la connexion unique fédérée ou de la sécurité des services Web. Elle constitue également une condition prérequise pour les déploiements qui utilisent l'échange de jetons via le service STS de Tivoli Federated Identity Manager. Un exemple de scénario d'échange de jeton est celui du déploiement d'une délégation contrainte Kerberos Tivoli Federated Identity Manager avec des jonctions WebSEAL.

Avant de commencer

Un assistant vous invite à fournir les propriétés de configuration nécessaires. Vous pouvez utiliser les propriétés indiquées sur le formulaire que vous avez préparé. Pour plus d'informations sur le formulaire, voir Chapitre 1, «Configuration de domaine», à la page 3

Procédure

1. Vérifiez que l'application WebSphere Application Server est en cours d'exécution.
2. Lorsque vous déployez un domaine dans un cluster WebSphere Application Server et que la sécurité globale WebSphere est activée, vous devez vous assurer que les fichiers de clés WebSphere du gestionnaire de déploiement sont copiés sur tous les noeuds du cluster. Sur chaque noeud, placez les clés dans un répertoire identique à celui du gestionnaire de déploiement. WebSphere 6.1 doit en principe accomplir cette tâche automatiquement. Néanmoins, assurez-vous que lorsque la console d'administration est utilisée à distance du service de gestion DMGR, le certificat serveur présenté par DMgr est accrédité par la console. L'une des méthodes pour cela consiste à copier le fichier de clés sécurisées de DMgr vers le profil de la console.
3. Connectez-vous à la console WebSphere et cliquez sur **Tivoli Federated Identity Manager → Mise en route**.

   Le portlet Mise en route s'affiche.
4. Cliquez sur **Gestion des domaines**. Le portlet Gestion des domaines s'affiche.
5. uliquez sur **Créer**. Le panneau Bienvenue de l'assistant de domaine s'affiche.
6. Cliquez sur **Suivant**. Le panneau Noeud final du service de gestion s'affiche.
7. Saisissez les valeurs des propriétés indiquées et cliquez sur **Suivant**.

8. Le panneau Sécurité WebSphere apparaît. Indiquez si la sécurité globale WebSphere est activée.

   Remarque : Lors de l'installation sur z/OS, consultez le fichier README sur le support de diffusion de z/OS afin de prendre connaissance des informations importantes sur la configuration des propriétés de sécurité de WebSphere.

   - Si c'est le cas, entrez des valeurs pour les propriétés indiquées, puis cliquez sur **Suivant**.
   - Si ce n'est pas le cas, ne renseignez pas les zones des propriétés restantes. Cliquez sur **Suivant**.

9. Cliquez sur **Test de la connexion**. En cas de succès de l'opération, le message d'information suivant s'affiche :

   ```
   FBTCON317I Tivoli Federated Identity Manager s'est connecté correctement.
   ```

10. Cliquez sur **Suivant**. Le panneau Mappage de cible WebSphere s'affiche. Sélectionnez ou entrez le nom de votre serveur ou cluster. Une fois que vous avez terminé, cliquez sur **Suivant**.

    - Lorsque l'environnement WebSphere comprend un serveur unique, l'écran affiche un menu Nom du serveur comportant un nom par défaut.
    - Lorsque l'environnement WebSphere comprend un cluster, le panneau affiche le menu Nom de cluster. Ce menu répertorie les noms des clusters définis dans la cellule. Sélectionnez le nom du cluster à utiliser.

11. Le panneau Sélection du domaine s'affiche. Un nom par défaut est fourni. Acceptez-le ou entrez le nom du nouveau domaine.
12. Le panneau Paramètres d'environnement Tivoli Access Manager s'affiche. Sélectionnez ou désélectionnez l'option **Cet environnement utilise Tivoli Access Manager**, selon les cas. et cliquez sur **Suivant**. Lorsque vous sélectionnez cette option, indiquez des valeurs pour le reste des propriétés.
13. Le panneau Récapitulatif s'affiche. Vérifiez que les informations de domaine sont correctes, puis cliquez sur **Terminer**.

    La création du domaine est terminée et l'assistant de domaine se ferme. Le panneau Création du domaine terminée s'affiche.

14. Cochez les deux cases du panneau Création du domaine terminée, puis cliquez sur **OK**.

    La création et le déploiement initiaux du service de gestion et de l'environnement d'exécution Tivoli Federated Identity Manager requièrent l'exécution des deux tâches suivantes :

    - **Faire de ce domaine le domaine de gestion actif**
    - **Ouvrir la fonction Gestion des noeuds d'exécution à la fin de l'opération**

15. Si vous déployez Tivoli Federated Identity Manager dans un cluster WebSphere, assurez-vous que l'agent de noeud WebSphere est en cours d'exécution sur tous les noeuds du cluster.

    Utilisez la console d'administration WebSphere pour vérifier le statut des agents de noeud.

16. Les portlets Domaine en cours et Gestion des noeuds d'exécution s'affichent. Dans le portlet Gestion des noeuds d'exécution, cliquez sur **Déployer l'environnement d'exécution**. Un message s'affiche :

    ```
    FBTCON355I - Une requête de déploiement de l'environnement d'exécution Tivoli
    Federated Identity Manager est en cours.
    ```

    Le lien suivant s'affiche :

    ```
    Cliquez pour régénérer l'état de déploiement et vérifier l'exécution de l'opération.
    ```

L'opération de déploiement peut prendre plusieurs minutes. Durant cette période, vous pouvez cliquez sur le lien pour vérifier l'avancement de l'opération. Une fois le déploiement terminé, le message suivant est renvoyé lorsque vous cliquez sur le lien :

```
FBTCON132I Le module d'exécution a été déployé dans le domaine.
```

Le panneau Gestion des noeuds d'exécution s'affiche de nouveau. Une entrée correspondant au composant d'exécution est ajoutée dans le tableau **Noeuds d'exécution** pour chaque noeud du domaine. En outre, le bouton **Configurer** est activé.

17. Dans le tableau Noeuds d'exécution, cochez la case correspondant à votre noeud, puis cliquez sur **Configurer**.

    L'application d'exécution est configurée dans l'environnement.

18. Dans un environnement WebSphere en cluster, configurez chaque noeud du cluster en répétant l'étape précédente.
19. Une fois que tous les noeuds sont configurés, cliquez sur le bouton **Charger les modifications de configuration dans l'environnement d'exécution de Tivoli Federated Identity Runtime**.

    Le bouton est situé sur le portlet du domaine Current.

20. Poursuivez avec les instructions pour appliquer la configuration à votre déploiement :
    - Dans un environnement WebSphere en *clusters*, poursuivez avec la rubrique «Mappage du composant d'exécution vers un serveur Web».
    - Dans un environnement WebSphere *non configuré en clusters* (serveur autonome), la création et le déploiement du domaine s'arrêtent là. Poursuivez avec les instructions appropriées suivant votre scénario.

Mappage du composant d'exécution vers un serveur Web

Pourquoi et quand exécuter cette tâche

Lors du déploiement du composant d'exécution Tivoli Federated Identity Manager, celui-ci est automatiquement mappé vers le serveur WebSphere Application Server par défaut. Dans les environnements groupés WebSphere, WebSphere Application Server est généralement déployé dans une configuration dotée d'un serveur Web, tel qu'IBM HTTP Web Server. Dans ce cas, un plug-in WebSphere a été installé et configuré pour IBM HTTP Web Server.

IBM HTTP Web Server exécute l'équilibrage de charge de travail entre les membres du cluster. Cela signifie que le composant d'exécution Tivoli Federated Identity Manager doit être mappé vers le serveur Web.

Procédure

1. Connectez-vous à la console d'administration WebSphere :

   `http://votre_nom_hôte:9060/admin`

2. Accédez à la page **Applications d'entreprise -> ITFIM Runtime**.
3. L'onglet Configuration s'affiche. Dans la section Propriétés du module Web, sélectionnez le lien **Hôtes virtuels**. Une section intitulée Appliquer plusieurs mappages affiche un tableau contenant une ligne pour chaque module Web.
4. Cochez la case de chaque module Web. Assurez-vous que toutes les cases sont cochées.
5. Acceptez l'entrée par défaut de `default_host` dans la zone Hôte virtuel de chaque module Web.

6. Une boîte de message vous invite à sauvegarder vos modifications. Cliquez sur le lien **Sauvegarder**.
7. Le panneau Sauvegarde s'affiche. Cliquez sur le bouton **Sauvegarder**.
8. Revenez à la page **Applications d'entreprise -> ITFIM Runtime**.
9. L'onglet Configuration s'affiche. Dans la section Modules, sélectionnez le lien **Gérer les modules**. La page **Applications d'entreprise -> Environnement d'exécution ITFIM -> Gérer les modules** s'affiche. Dans la partie supérieure, le titre Gestion des modules doit être affiché.
10. Cochez la case correspondant à *chacun* des modules Web. Pour Tivoli Federated Identity Manager, la liste des modules peut inclure les éléments suivants, de façon non limitative :
    - ITFIM-Runtime
    - ITFIM Security Token Service
    - ITFIM Information Service
    - TokenService
    - TrustServerWST13
11. Une fenêtre déroulante affiche Clusters et serveurs. Sélectionnez les deux entrées suivantes :
    - L'entrée correspondant à votre cluster. Par exemple, `cluster=fimCluster`.
    - L'entrée correspondant au serveur Web. Par exemple, `server=webserver1`
12. Lorsque les deux éléments sont mis en évidence, cliquez sur **Valider**. Dans le tableau des modules, la définition de chaque serveur et cluster s'ajoute à l'entrée (dans la colonne Serveur) pour chacun des modules Web que vous avez sélectionnés.
13. Cliquez sur **OK** au bas de la page. Un message vous invite à sauvegarder vos modifications.
14. Cliquez sur le lien **Sauvegarder**. L'écran **Applications d'entreprise → Sauvegarder** s'affiche.
15. Cliquez sur **Sauvegarder**.
16. Pour terminer la configuration du composant d'exécution de Tivoli Federated Identity Manager dans un cluster WebSphere, passez à la section «Activation de la réplication dans un cluster WebSphere».

Activation de la réplication dans un cluster WebSphere

Pourquoi et quand exécuter cette tâche

Remarque : Cette tâche de configuration s'applique aux environnements groupés WebSphere. Si vous avez déjà configuré le composant d'exécution Tivoli Federated Identity Manager dans un environnement WebSphere comportant un serveur unique, ignorez la présente rubrique.

WebSphere prend en charge l'utilisation d'un *service de mémoire cache dynamique* pour le stockage des données d'application. Les objets données gérés par ce service peuvent être répartis dans des *instances de cache* pouvant être configurées individuellement. L'administrateur WebSphere peut configurer des paramètres, tels que la taille du cache, la persistance sur disque, etc. Chaque instance de cache peut faire partie d'un *domaine de réplication*, de sorte que les données de la mémoire cache sont dupliquées et accessibles à tous les serveurs participant au domaine de réplication.

L'application d'exécution Tivoli Federated Identity Manager utilise cette fonction pour améliorer les performances. Lorsque le composant d'exécution Tivoli Federated Identity Manager est déployé, certaines étapes de configuration WebSphere sont automatiquement exécutées :

- Un domaine de réplication est créé. Le nom du domaine de réplication est `FIM-nom_votre_cluster` ou `FIM-nom_votre_serveur`.
- Plusieurs instances de cache utilisant le domaine de réplication sont créées.

Une configuration supplémentaire est requise.

Le service de mémoire cache dynamique des serveurs d'applications du cluster doit désormais être configuré sous la forme d'un *client* du domaine de réplication.

Remarque : Les étapes de cette section doivent être exécutées pour chaque serveur du cluster.

Exécutez les étapes suivantes pour *chaque* serveur d'applications qui fait partie du cluster :

Procédure

1. Dans la console d'administration WebSphere, accédez à **Serveurs -> Serveurs d'applications -> *nom_de_votre_serveur***. Les propriétés du serveur sélectionné s'affichent.
2. Dans la section Paramètres du conteneur, développez **Services du conteneur**. Cliquez sur **Service de mémoire cache dynamique**.
3. Dans la section Propriétés générales de l'écran, accédez à la section des paramètres de cohérence. Cochez la case **Activer la réplication de cache**. Vérifiez que la zone des paramètres de cohérence comporte les valeurs suivantes :
   - Domaine de réplication de groupe complet

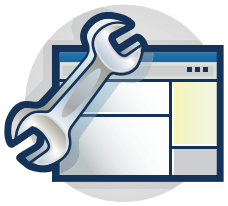
     Sélectionnez le nom du cluster où vous avez déployé le module d'exécution.
   - Type de réplication : **Insertion et extraction**
   - Fréquence d'insertion : **0**
4. Cliquez sur **OK**. Lorsque vous êtes invité à sauvegarder vos modifications, cliquez sur le lien **Sauvegarder**. Une fois que la page suivante s'affiche, cliquez sur le bouton **Sauvegarder**.
5. Dans la console d'administration WebSphere, accédez à **Serveurs -> Serveurs d'applications -> *nom_de_votre_serveur***.

   Remarque : Il se peut que les propriétés indiquées dans la présente section soient déjà définies.
6. Dans la section **Paramètres du conteneur** section, sélectionnez **Gestion de session**.
7. Un onglet Configuration s'affiche. Dans la section Propriétés supplémentaires, sélectionnez **Paramètres de l'environnement distribué**.
8. L'écran Propriétés générales est régénéré. Consultez la section **Paramètres de l'environnement distribué**.
   a. Cliquez sur le bouton d'option **Réplication mémoire à mémoire**.
   b. Cliquez sur le lien hypertexte **Réplication mémoire à mémoire**.

9. Le panneau Propriétés générales s'affiche.
   a. Pour le domaine de réplication, sélectionnez le nom du cluster où vous avez déployé le module d'exécution Tivoli Federated Identity Manager.
   b. Paramétrez le mode de réplication sur **Client et serveur**.
10. Lorsque vous êtes invité à sauvegarder vos modifications, cliquez sur le lien **Sauvegarder**. Une fois que la page suivante s'affiche, cliquez sur le bouton **Sauvegarder**.
11. Dans l'écran Cluster de serveurs, cochez la case correspondant à votre cluster et cliquez sur **Démarrage en cascade**.

    Vous devez redémarrer le cluster pour que les modifications effectuées soient prises en compte.

Partie 2. Configuration d'une fédération de connexion unique



Les rubriques de la section Configuration vous guident pas à pas lors de la configuration d'une fédération à connexion unique. La console de gestion est dotée d'assistants qui vous guident dans de nombreuses tâches de configuration.

De nombreuses tâches de configuration sont communes à tous les types de fédération. Certaines tâches de configuration concernent uniquement des types de fédération spécifiques.

Complétez les tâches de configuration dans l'ordre suivant :

1. Passez en revue les tâches de configuration communes à tous les types de fédérations. Effectuez les tâches de configuration applicables à votre déploiement.

   Remarque : La plupart des types de fédération prennent en charge une grande variété de scénarios de déploiement. Les étapes effectives requises pour chaque tâche de configuration varient selon le scénario.

   a. Chapitre 3, «Rôles du fournisseur d'identité et du fournisseur de services», à la page 17
   b. Chapitre 4, «Utilisation des clés et certificats pour sécuriser les communications», à la page 19
   c. Chapitre 5, «Configuration de LTPA et de ses clés», à la page 27
   d. Chapitre 6, «Configuration de la sécurité des messages», à la page 29
   e. Chapitre 7, «Configuration de la sécurité du transport», à la page 51
   f. Chapitre 8, «Sélection d'un serveur point de contact», à la page 65
   g. Chapitre 9, «Configuration de WebSphere en tant que serveur point de contact», à la page 69
   h. Chapitre 10, «Configuration d'un plug-in de serveur Web», à la page 101
   i. Chapitre 11, «Configuration de la base de données de service d'alias», à la page 115
   j. Chapitre 12, «Planification du mappage des identités d'utilisateur», à la page 127

2. Suivez les instructions relatives à votre type de fédération :
   - Chapitre 13, «Fédérations SAML : présentation», à la page 147
   - Chapitre 18, «Planification d'une fédération Information Card», à la page 239
   - Chapitre 21, «Présentation de la planification sous OpenID», à la page 283
   - Chapitre 24, «Planification d'une fédération Liberty», à la page 343
   - Chapitre 26, «Configuration d'une fédération de connexion unique WS-Federation», à la page 373

Chapitre 2. Présentation des tâches de configuration pour la connexion unique fédérée

Tivoli Federated Identity Manager vous permet d'établir une fédération de connexions uniques à laquelle les utilisateurs peuvent se connecter une seule fois pour accéder à plusieurs applications Web via différents fournisseurs.

Une fédération est un groupe composé d'au moins deux partenaires d'échange accrédités qui souhaitent initier ou recevoir le transfert d'identités d'utilisateurs au sein de la fédération. L'intégrité de l'identité repose sur des relations d'accréditation entre les membres de la fédération, souvent codifiées par accord légal. La participation à une fédération par le biais d'une connexion unique fédérée permet à un utilisateur appartenait à une société d'accéder sans contraintes aux ressources des partenaires commerciaux fédérés à cette société, de manière sécurisé et fiable, généralement via un simple navigateur Web.

Lorsque vous établissez la fédération au moyen de Tivoli Federated Identity Manager, vous bénéficiez des caractéristiques suivantes du produit :

- Normes ouvertes pour la connexion unique
- Intégration aux capacités de connexion unique d'IBM WebSphere Application Server 6.1, qui élimine la nécessité de recourir à une authentification via des applications individuelles
- Prise en charge d'un nombre illimité de fédérations et possibilité de définir des configurations personnalisées unique pour chaque fédération. Vous pouvez par exemple jouer le rôle de fournisseur d'identité ou de fournisseur de services dans toutes les fédérations, moyennant une seule installation de Tivoli Federated Identity Manager.
- Support d'intégration pour les applications Web exécutées sur l'un des types de serveurs suivants :
  - WebSphere Application Server 5.1 ou 6.x
  - Microsoft® Internet Information Server (IIS)
  - IBM HTTP Server (IHS)
  - Serveur HTTP Apache 2.0 ou 2.2
- Administration Web simplifiée

Le déploiement d'une fédération à connexion unique nécessite l'accomplissement d'une série de tâches. Certaines de ces tâches sont communes à tous les types de fédérations. D'autres tâches concernent plus particulièrement le protocole standard de la fédération (par exemple SAML 2.0).

Pour déployer une fédération à connexion unique, vous pouvez d'abord passer en revue les tâches communes, puis procéder à la configuration spécifique du protocole standard.

Remarque : Vous devez créer un domaine avant de déployer une fédération de connexion unique. Si vous n'avez pas encore déployé un domaine, suivez les instructions au Chapitre 1, «Configuration de domaine», à la page 3.

Les tâches décrites dans les rubriques suivantes sont communes à tous les types de fédérations. Parcourez chaque rubrique dans l'ordre indiqué avant de configurer le protocole sélectionné pour votre fédération.

1. Chapitre 3, «Rôles du fournisseur d'identité et du fournisseur de services», à la page 17
2. Chapitre 4, «Utilisation des clés et certificats pour sécuriser les communications», à la page 19
3. Chapitre 5, «Configuration de LTPA et de ses clés», à la page 27
4. Chapitre 6, «Configuration de la sécurité des messages», à la page 29
5. Chapitre 7, «Configuration de la sécurité du transport», à la page 51
6. Chapitre 8, «Sélection d'un serveur point de contact», à la page 65
7. Chapitre 9, «Configuration de WebSphere en tant que serveur point de contact», à la page 69
8. Chapitre 10, «Configuration d'un plug-in de serveur Web», à la page 101
9. Chapitre 11, «Configuration de la base de données de service d'alias», à la page 115
10. Chapitre 12, «Planification du mappage des identités d'utilisateur», à la page 127

Pour plus d'informations sur les concepts de la fédération et sur l'assistance à la mise en oeuvre d'une solution de gestion d'identité fédérée, reportez-vous au chapitre "Federation concepts" du document *Enterprise Security Architecture Using IBM Tivoli Security Solutions* disponible à l'adresse http://www.redbooks.ibm.com/redbooks/pdfs/sg246014.pdf.

Chapitre 3. Rôles du fournisseur d'identité et du fournisseur de services

Au sein d'une fédération, chaque partenaire a un rôle. Il s'agit du rôle **Fournisseur d'identité** ou **Fournisseur de services**.

- **Fournisseur d'identité**

  Le fournisseur d'identité est un partenaire de fédération qui garantit l'identité des utilisateurs. Le fournisseur d'identité authentifie un utilisateur et transmet un *jeton d'authentification* (c'est-à-dire les informations permettant de vérifier l'authenticité de l'utilisateur) au fournisseur de services.

  Le fournisseur d'identité authentifie directement l'utilisateur, par exemple en validant un nom d'utilisateur et un mot de passe, ou authentifie indirectement l'utilisateur, par exemple, en validant une assertion concernant l'identité de l'utilisateur, telle qu'elle est présentée par un fournisseur d'identité distinct.

  Le fournisseur d'identité traite la gestion des identités utilisateur afin de libérer le fournisseur de services de cette responsabilité.

- **Fournisseur de services**

  Un fournisseur de services est un partenaire de fédération qui fournit des services à l'utilisateur final. En général, les fournisseurs de services n'authentifient pas les utilisateurs, mais demandent à un fournisseur d'identité de prendre les décisions d'authentification. Les fournisseurs de services comptent sur les fournisseurs d'identité pour vérifier l'identité d'un utilisateur, ainsi que, généralement, certains attributs relatifs à l'utilisateur qui sont gérés par le fournisseur d'identité. Les fournisseurs de services peuvent également gérer un compte local au profit de l'utilisateur, en fournissant des attributs uniques du point de vue de leur service.

  Les fournisseurs de services peuvent gérer pour l'utilisateur un compte local qui peut être référencé par un identificateur de l'utilisateur.

  Certains protocoles de fédération utilisent une terminologie distincte pour faire référence au rôle du fournisseur de services :

  – **Partie de confiance**

    La spécification du protocole Information Card emploie le terme de partie de confiance pour désigner le rôle du fournisseur de services. Lorsque vous configurez la fédération Information Card à l'aide de l'assistant Tivoli Federated Identity Manager, vous êtes amené à sélectionner le rôle de Fournisseur de services pour la partie de confiance.

  – **Consommateur**

    La spécification du protocole OpenID emploie le terme de consommateur pour désigner le rôle du fournisseur de services. Lorsque vous configurez la fédération OpenID à l'aide de l'assistant Tivoli Federated Identity Manager, vous êtes amené à sélectionner le rôle de Fournisseur de services pour le consommateur.

Avant d'installer Tivoli Federated Identity Manager, vous devez savoir si vous serez amené à être le fournisseur d'identité ou le fournisseur de services dans chacune des fédérations configurées. Il vous faudra également définir les options du serveur point de contact correspondant à votre rôle.

Chapitre 4. Utilisation des clés et certificats pour sécuriser les communications

Dans un environnement de production standard, tous les messages et toutes les communications de ces messages entre les partenaires et les utilisateurs membres de la fédération sont sécurisés. En outre, il est peut-être nécessaire de sécuriser les communications entre les serveurs de votre environnement, par exemple, les communications entre votre serveur et votre registre d'utilisateurs.

Les normes SAML stipulent par exemple que les partenaires doivent établir une relation d'accréditation au moyen d'une infrastructure PKI (Public Key Infrastructure) et mettent en oeuvre le protocole SSL (Secure Sockets Layer) sur HTTP (HTTPS) afin de garantir l'intégrité et la confidentialité des messages lors de leur transport.

La mise en oeuvre de la sécurité est un sujet complexe et est fonction de la configuration de votre environnement et des règles de sécurité de votre organisation. Cette présentation explique les concepts généraux de la sécurisation des éléments dans un environnement Tivoli Federated Identity Manager. Si vous avez besoin d'une assistance concernant cette rubrique, consultez les recommandations et exigences de sécurité contenues dans le document relatif aux spécifications du protocole, ou prenez contact avec spécialiste de la sécurité informatique.

Sécurité de niveau message

Pour sécuriser le contenu des messages et des assertions, les normes SAML préconisent l'utilisation d'une cryptographie à clé publique. Les partenaires d'une fédération peuvent, grâce à cette méthode, échanger des paires de clés publies/privées et les utiliser pour signer, chiffrer, valider et déchiffrer des messages, ainsi que les assertions que ceux-ci contiennent, conformément à la norme SAML ou aux exigences de leur environnement.

Lorsque vous configurez une fédération dans Tivoli Federated Identity Manager, l'assistant de configuration de fédération vous présente, selon les cas, des *exigences* relatives à la signature, à la validation ou au chiffrage, ou des *options* de signature, validation ou chiffrage selon le protocole SAML, le profil ou les liaisons que vous avez sélectionnés. Si vous avez par exemple choisi, lors de la configuration de votre fédération, d'indiquer qu'une signature était requise, l'assistant vous invite à spécifier une clé de signature. Si vos sélections entraînent la définition visant à signer ou à ne pas signer, l'assistant vous permet d'effectuer une sélection.

Avant de pouvoir utiliser l'assistant de configuration de fédération, vous devez avoir créé les clés appropriées. Les informations du Chapitre 6, «Configuration de la sécurité des messages», à la page 29 peuvent vous aider à planifier les clés requises dans votre environnement et contiennent des instructions relatives à leur création et à leur obtention.

Les sections qui suivent fournissent une description générale des clés en usage dans les fédérations SAML.

Signature

La signature des messages XML et des assertions SAML est effectuée par un partenaire unique, afin de protéger l'intégrité du message. La signature permet à la partie récipiendaire de savoir si le message a été modifié durant la transmission. La signature s'effectue au moyen d'une clé privée. Le partie qui a reçu le message XML ou l'assertion SAML signé(e) a besoin du certificat X.509 (clé publique) qui correspond à la clé privée du signataire du message. Par défaut, le certificat X.509 (clé publique) est inclus dans la signature sous forme de certification X.509 codée en base 64. Toutefois, vous avez la possibilité de spécifier les données de certificat à inclure avec vos signatures.

Validation

Les signatures contenues dans les messages et assertions peuvent être validées par le partenaire récipiendaire. La validation permet de confirmer que l'identité du signataire a été certifiée. La validation s'effectue au moyen de la clé publique ou du partenaire ayant signé les messages ou les assertions.

Chiffrement et déchiffrement

Dans SAML 2.0, le chiffrement des messages peut avoir lieu en plus de leur signature. L'usage des paires de clés publique/privée lors du chiffrement et du déchiffrement diffère de la procédure appliquée lors de la signature et de la validation. Le chiffrement s'effectue au moyen la *clé publique du destinataire prévu*. En d'autres termes, pour qu'un partenaire puisse chiffrer un message, il doit être en possession de la clé publique du partenaire auquel le message est adressé. Le partenaire récipiendaire du message chiffré doit utiliser sa clé *privée* pour déchiffrer le message. Dans Tivoli Federation Identity Manager, et lorsque SAML 2.0 est utilisé, les deux partenaires doivent obtenir leurs propres paires de clés publiques/privées afin de les utiliser pour le chiffrement. Ils doivent échanger leurs clés publiques de manière à ce que chaque partenaire puisse chiffrer les messages adressés à l'autre.

Sécurité de niveau transport

La sécurité de niveau message, telle que décrite à la section précédente, ne protège que le contenu du message. Pour permettre la protection du message lors de sa communication (ou de son transport) entre les partenaires, SAML recommande d'utiliser une connexion SSL (Secure Sockets Layer) avec authentification sur le serveur et, dans certains cas, une authentification réciproque.

Le protocole SSL permet d'établir l'authenticité, l'intégrité et la confidentialité entre les parties impliquées dans la transmission de données par le biais d'autres protocoles (tels que HTTP) sur un réseau.

Remarque : Le protocole SSL est une notion complexe. La présente rubrique et une description brève et simplifiée visant à vous familiariser avec les concepts de base et la terminologie employés dans ce manuel.

Authentification sur le serveur

Dans un environnement In a Tivoli Federated Identity Manager, le protocole SSL a pour rôle de protéger les noeuds finals en provenance et en direction desquels les messages SAML sont envoyés et reçus. Dans le cadre de communications protégées par SSL entre des partenaires de fédération, l'un des partenaires agit en tant que *client* (partie qui émet la requête de données), tandis que l'autre partenaire agit en tant que *serveur* (récipiendaire de la requête et émetteur de la réponse à cette requête).

Dans une fédération SAML 1.x, une connexion unique est reçue au niveau du partenaire fournisseur d'identité. Ainsi, lorsqu'une connexion SSL est établie entre les partenaires de la fédération, le partenaire fournisseur d'identité joue le rôle de *serveur*, tandis que le fournisseur de services agit en tant que *client*.

Dans une fédération SAML 2.0, une requête de connexion unique peut être reçue par l'un ou l'autre des partenaires. Chaque partenaire peut donc aussi bien jouer le rôle de serveur que de client.

Le protocole SSL peut être configuré sur le serveur uniquement (*authentification de serveur*, ou bien à la fois sur le serveur et le client (*authentification réciproque*). Les normes SAML recommandent d'appliquer au moins l'authentification de serveur entre les partenaires. L'ajout d'une authentification réciproque permet de bénéficier d'une sécurité renforcée.

Pour permettre l'authentification de serveur, vous devez créer une biclé composée d'un clé publique et d'une clé privée, puis obtenir un certificat, dont le rôle est de permettre à votre serveur de s'authentifier auprès du client. Ce certificat est appelé *certificat serveur* ou encore, *certificat personnel*.

Bien que vous puissiez créer votre propre certificat serveur (via le logiciel prenant en charge la création de certificats), il est généralement souhaitable, dans un environnement de production, d'obtenir un certificat serveur de la part d'une tierce partie, qui est représentée par l'*autorité de certification* ou *CA* chargée d'émettre les certificats. Avant de tenter d'établir une connexion SSL, le client auquel le serveur présente son certificat doit obtenir le certificat de la part de l'autorité de certification (CA) qui a émis le certificat serveur. Le client assure la gestion d'une liste d'émetteurs dignes de confiance à laquelle il ajoute le certificat de CA.

Le certificat serveur contient des informations telles que la clé publique du certificat serveur, le numéro de série du certificat, la période de validité du certificat, le nom distinctif du serveur (qui comprend le nom d'hôte associé au serveur), le nom distinctif de l'émetteur et la signature numérique de l'émetteur.

Pour établir la connexion SSL, le serveur présente son certificat, qui doit être vérifié par le client. A titre d'exemple, le client vérifie sa liste d'émetteurs (autorités de certification) dignes de confiance afin de voir si l'émetteur du certificat du serveur est sécurisé, puis compare la signature numérique de l'émetteur contenue dans le certificat du serveur avec celle qui est contenue dans le certificat de CA.

Le serveur doit exporter son certificat de CA et le fournir à son client partenaire.

En résumé, l'authentification du serveur nécessite les clés et certificats suivants :

Tableau 3. Exigences liées au certificat d'authentification de serveur SSL

Certificat requis	Qui doit obtenir le certificat	Remarque
Certificat serveur et clé privée associée à ce certificat	Partenaire agissant en tant que serveur	Dans une fédération SAML 1.x, le fournisseur d'identité agit toujours en tant que serveur.
Certificat de CA lié à l'émetteur du certificat serveur	Partenaire agissant en tant que client	Dans une fédération SAML 1.x, le fournisseur de services agit toujours en tant que client.

Les instructions d'activation de SSL sont décrites à la rubrique «Activation de SSL sur WebSphere Application Server», à la page 52.

Authentification client

Un serveur peut être configuré en vue d'exiger une authentification de la part de ses clients pour confirmer leurs identités. Tivoli Federated Identity Manager accepte l'une des méthodes d'authentification client suivantes :

Authentification de base (par mot de passe)
Si l'authentification de base est configuré, le serveur demande au client de s'authentifier au moyen d'un nom d'utilisateur et d'un mot de passe. Aucun certificat n'est utilisé avec cette méthode.

Authentification par certificat client
Un *certificat client* est similaire à un certificat serveur. Pour obtenir un certificat client, le client en effectue généralement la demande auprès d'une autorité de certification. Avant d'établir une fédération, les partenaires s'accordent généralement sur le choix d'une autorité de certification pour la signature du certificat client. Le serveur doit s'assurer que cette autorité de certification se trouve dans la liste des émetteurs dignes de confiance. Lorsque l'authentification par certificat client est configurée, le serveur demande l'authentification au client, puis celui-ci répond en envoyant au serveur son certificat client et sa signature numérique via un élément de données à génération aléatoire. Le certificat client contient généralement la clé publique du client, le numéro de série du certificat, la période de validité du certificat, le nom distinctif du client, le nom distinctif de l'émetteur et la signature numérique de l'émetteur. Le serveur vérifie les informations client. Le client exporte par exemple son certificat et le fournit au serveur partenaire. Ensuite, le serveur utilise la clé publique du client contenue dans le certificat client pour valider la signature numérique du client, vérifie sa liste d'émetteurs (autorités de certification) dignes de confiance afin de voir si l'émetteur du certificat client est sécurisé, puis compare la signature numérique de l'émetteur contenue dans le certificat client avec celle qui est contenue dans le certificat de CA.

Si l'authentification par certificat client est employée, les certificats suivants sont requis :

Tableau 4. Exigences liées au certificat d'authentification client SSL

Certificat requis	Qui doit obtenir le certificat	Remarque
Certificat client et clé privée associée	Partenaire agissant en tant que client	Dans une fédération SAML 1.x, le fournisseur de services agit toujours en tant que client.
Certificat de CA lié à l'émetteur du certificat client	Partenaire agissant en tant que serveur	Dans une fédération SAML 1.x, le fournisseur d'identité agit toujours en tant que serveur.

Les partenaires agissant en tant que *serveurs* doivent suivre les instructions relatives à la configuration d'une authentification client sur leurs serveurs ; voir «Configuration des exigences relatives à l'authentification client», à la page 56.

Les partenaires agissant en tant que *clients dont les partenaires exigent une authentification par certificat client* doivent suivre les instructions relatives à la configuration de leurs certificats client ; voir «Configuration des certificats client», à la page 61.

Stockage et gestion des clés et certificats

Les clés et certificats sont stockés dans des fichiers de clés et des fichiers de clés certifiées.

Fichiers de clés
Les clés privées et les certificats sont stockés dans des fichiers de clés.

Fichier de clés certifiées
Les clés privées et les certificats CA sont stockés dans des fichiers de clés certifiées. Un fichier de clés certifiées est un fichier de clés qui, par convention, contient uniquement des clés certifiées et des certificats.

Dans votre environnement Tivoli Federated Identity Manager, un certain nombre de clés et de certificats sont stockés dans les fichiers de clés et fichiers de clés certifiées de WebSphere Application Server, tandis que d'autres sont stockés dans ceux de Tivoli Federated Identity Manager et sont gérés par une fonction de Tivoli Federated Identity Manager appelée le *service de clés*. L'emplacement dépend de l'objectif d'utilisation des clés et des certificats.

Les clés et certificats sont stockés un fichier de clés et un fichier de clés certifiées de WebSphere Application Server :

- Certificats serveur SSL et leurs clés privées (dans le fichier de clés WebSphere du serveur partenaire)
- Certificat de CA pour les clients présentant un certificat client (dans le fichier de clés certifiées WebSphere du serveur partenaire)

Les clés et certificats sont stockés un fichier de clés et un fichier de clés certifiées de Tivoli Federated Identity Manager :

- Certificats client SSL (utilisés pour l'authentification par certificat client) et leurs clés privées (dans le fichier de clés du client)
- Certificats de CA pour les serveurs sur lesquels l'authentification sur serveur SSL est configurée (dans le Serveurs du client)
- Les clés de signature, de validation et de chiffrement sont également gérées dans les fichiers de clés et fichiers de clés sécurisée de Tivoli Federated Identity Manager. Par exemple :

  Clés de signature
  Il s'agit des clés privées stockées dans les fichiers de clés.

  Clés de validation
  Il s'agit des clés publiques qui correspondent aux clés privées utilisées pour la signature. Elles sont stockées dans les fichiers de clés sécurisées.

  Clés de chiffrement
  - La clé employée pour le chiffrement de données est une clé publique obtenue auprès de votre partenaire. Son stockage s'effectue dans votre fichier de clés certifiées.
  - La clé servant à déchiffrer les données est une clé privée. Son stockage s'effectue dans votre fichier de clés.

Par défaut, WebSphere Application Server et Tivoli Federated Identity Manager comportent des fichiers de clés, fichiers de clés certifiées, clés et certificats destinés aux environnements de test.

WebSphere Application Server
Durant la création de profils, WebSphere Application Server crée les éléments suivants :

- Fichier de clés key.p12
- Fichier de clés certifiées trust.p12
- Un certificat d'auto-signature par défaut dans le fichier de clés key.p12

Le mot de passe utilisé à la fois pour le fichier de clés et le fichier de clés certifiées est `WebAS`.

Tivoli Federated Identity Manager

Tivoli Federated Identity Manager fournit deux fichiers de clés Java par défaut, un certificat d'auto-signature et quelques certificats de CA :

- DefaultKeyStore.jks pour les clés de signature t de chiffrement (clés privées)
- DefaultTrustedKeyStore.jks pour les certificats de CA
- Un certificat d'auto-signature comportant l'alias `testkey`, qui peut être utilisé en tant que clé de signature en environnement de test, et est contenu dans le fichier de clé s
- Plusieurs certificats de CA contenus dans le fichier de clés certifiées

Le mot de passe par défaut des fichiers de clés certifiées est `testonly`.

Du fait que les clés et certificats par défaut sont utilisés uniquement aux fins de test, vous devez créer une nouvelle série de clés et de certificats ainsi que, le cas échéant, de nouveaux fichiers de clés lors de la configuration deTivoli Federated Identity Manager.

Pour plus d'informations, voir «Création des magasins de clés, clés et certificats».

Création des magasins de clés, clés et certificats

Comme décrit dans les sections précédentes, la configuration de la sécurité au niveau des message et du transport nécessite l'utilisation de paires de clés publiques et privées, ainsi que de certificats. Pour pouvoir utiliser les clés et certificats, vous devez appliquer un processus général lors de leur création, ainsi que pour créer les magasins de clés dans lesquels vous allez les stocker, si vous choisi de le pas utiliser les magasins par défaut.

La procédure générale de création des clés, certificats et de leurs magasins de clés est la suivante :

1. Créez le magasin de clés (sous forme de fichier de clés normales ou de fichier de clés certifiées), ou reprenez un magasin existant.
2. Créez la demande de certificat, qui permet de générer une paire de clés publique/privée et peut être adresse à une autorité de certification (CA). La demande de certificat contient la clé publique et les données relative à vous-même (en tant que demandeur) spécifiées dans le certificat.
3. Envoyez la demande de certificat à l'autorité de certification. L'autorité de certification émet le certificat.
4. Recevez le certificat en provenance de l'autorité de certification et importez-le dans les magasins de clés appropriés.
5. Partagez les clés publiques des certificats avec votre partenaire selon les besoins.

En outre, vous devrez peut-être importer certaines clés et certains certificats dans vos magasins de clés en provenance de votre partenaire.

WebSphere Application Server et Tivoli Federated Identity Manager comprennent tous deux des utilitaires permettant de créer des demandes de certificat et de recevoir celles-ci de la part de l'autorité de certification.

Les informations relatives à l'exécution de toutes les tâches de sécurité au niveau des messages et du transport, y compris la création de magasins de clés, clés et certificats à l'aide des utilitaires concernés, sont décrites dans les sections suivantes du présente manuel :

Instructions de sécurité de niveau message :
Chapitre 6, «Configuration de la sécurité des messages», à la page 29.

Instructions de sécurité de niveau transport :
Chapitre 7, «Configuration de la sécurité du transport», à la page 51

Critère de sélection de clé

Configurez l'ordre des certificats ou clés en utilisant les critères de sélection de clé d'exécution.

Par défaut, Tivoli Federated Identity Manager, version 6.1, crée une liste de certificats ou de clés partageant la même valeur SubjectDN et optimisée de la durée de vie la plus longue à la plus courte. Cette fonction de produit, appelée Auto Key Rollover (Substitution de clé automatique), possède les caractéristiques suivantes :

- Lors de la signature de documents, la fonction utilise une clé valide avec la durée de vie restante la plus courte (par exemple, le certificat X.509 le plus ancien ou la clé privée la plus ancienne).
- Lors de la validation, la fonction parcoure la liste des clés pour la valeur SubjectDN donnée jusqu'à réussite de la validation. Une validation échoue signifie que toutes les clés disponibles étaient incorrectes.

En utilisant les critères de sélection de clé d'exécution, toutefois, vous pouvez configurer l'ordre des certificats ou des clés des manières suivantes :

- Alias uniquement : la clé sélectionnée uniquement, sans substitution automatique. Si la clé est incorrecte, le logiciel indique un échec.
- Durée de vie la plus courte : pour la signature, une clé valide avec la durée de vie disponible la plus courte. Pour la validation, la disponibilité de la durée de vie de clé fonctionne de la plus courte à la plus longue.
- Durée de vie la plus longue : pour la signature, une clé valide avec la durée de vie disponible la plus longue. Pour la validation, la disponibilité de la durée de vie de clé fonctionne de la plus longue à la plus courte.

Chapitre 5. Configuration de LTPA et de ses clés

Vous devez consulter les paramètres LTPA de votre serveur WebSphere Application Server après avoir installé Tivoli Federated Identity Manager. Vous pouvez utiliser la configuration LTPA par défaut ou l'adapter à votre environnement.

Pourquoi et quand exécuter cette tâche

La configuration LTPA par défaut est la suivante :

Groupe de jeux de clés
Les clés LTPA servent à chiffrer et à déchiffrer les données à envoyer d'un serveur à un autre. Elles sont stockées par jeux, qui sont à leur tour stockés par groupes. Le groupe de jeux de clés par défaut est NodeLTPAKeySetGroup.

Jeux de clés
Les jeux de clés par défaut sont NodeLTPAKeyPair et NodeLTPASecret.

Génération de clés
Par défaut, les clés LTPA sont générées automatiquement au premier démarrage du serveur. Elles sont régénérées automatiquement toutes les 12 semaines le dimanche à 22h:00 (horloge au format 24 heures).

Avertissement : Si votre configuration comporte un serveur d'applications cible distinct (par exemple, un serveur WebSphere Application Server, un un serveur pris en charge par le plug-in du serveur Web Tivoli Federated Identity Manager Web, les clés LTPA doivent résider sur le serveur point de contact WebSphere Application Server et sur le serveur d'applications cible. Si vous générez des clés en mode automatique, vous devez les conserver sur le serveur d'applications en les synchronisant avec les clés générées sur votre serveur point de contact WebSphere Application Server. Pour plus d'informations sur l'exportation de clés à partir de WebSphere Application Server et leur importation sur votre serveur d'applications, consultez les rubriques «Exportation de la clé LTPA à partir du serveur point de contact», à la page 98 et «Importation de la clé LTPA dans WebSphere Application Server», à la page 106 ou «Configuration de la clé LTPA sur le serveur Web», à la page 109.

Délai d'attente du cache d'authentification
Cette valeur indique le délai de validité (en minutes) d'un jeton LTPA. Par défaut, ce délai est de 10 minutes.

Délai de validité du transfert de droits d'accès entre serveurs
Cette valeur indique le délai de validité des droits d'accès émanant d'un autre serveur. La valeur par défaut est 120 minutes.

Pour consulter ou modifier ces paramètres, procédez comme suit :

Procédure

1. Connectez-vous à la console.
2. Cliquez sur **Sécurité → Administration, applications et infrastructure sécurisées**.

   Le panneau Administration, application et infrastructure sécurisées s'affiche.
3. Sur la gauche, cliquez sur **Mécanismes d'authentification et expiration**. L'onglet Configuration s'affiche. Utilisez-le pour vérifier ou modifier le groupe de jeux de clés défini, le délai d'attente du cache d'authentification et le délai de validité du transfert de droits d'accès entre serveurs.
4. Pour modifier les paramètres du groupe de jeux de clés et de génération de clés, cliquez sur **Groupe de jeux de clés**. Sélectionnez les paramètres adaptés à votre environnement, puis cliquez sur **Appliquer**. Revenez à l'onglet Configuration.
5. Dans la section Expiration de l'authentification de l'onglet Configuration, vérifiez ou modifiez les valeurs des zones **Délai d'attente du cache d'authentification** et **Délai de validité du transfert de droits d'accès entre serveurs**. Lorsque vous avez terminé, cliquez sur **Appliquer**.
6. Enregistrez les modifications dans le fichier de configuration principale lorsqu'un message vous y invite.

Que faire ensuite

Poursuivez avec la configuration de votre environnement. Par exemple, poursuivre avec le Chapitre 6, «Configuration de la sécurité des messages», à la page 29.

Chapitre 6. Configuration de la sécurité des messages

Tivoli Federated Identity Manager utilise des certificats (paires de clés publiques et privées) pour sécuriser les messages.

Avant l'établissement d'une fédération, vous devez déterminer, en accord avec votre partenaire, les configurations de sécurité que vous allez utiliser au sein de votre fédération. Vous devez ensuite créer ou demander des certificats, ou encore les obtenir auprès de votre partenaire, selon les cas, puis les importer dans le service de clés Tivoli Federated Identity Manager.

Remarque : Les instructions relatives à la configuration des certificats compatibles avec SSL, tels que les certificats serveur, certificats client ou exigences d'authentification client, sont décrites au Chapitre 7, «Configuration de la sécurité du transport», à la page 51. Hormis les rubriques relatives à la préparation des fichiers de clés, les rubriques du présent chapitre traitent uniquement de la sécurité au niveau message.

Pour configurer la sécurité des messages dans votre environnement, procédez comme suit :

1. Préparez les fichiers de clés. Voir «Préparation des fichiers de clés».
2. Discutez avec votre partenaire des consignes de sécurité de message, puis établissez une liste des fichiers de clés et des certificats dont chacun de vous aura besoin. Evaluez la possibilité d'utiliser les listes de contrôle mentionnées à la rubrique «Planification de la sécurité au niveau message», à la page 32.
3. Obtenez les certificats requis pour votre environnement. Voir «Obtention de vos clés et certificats», à la page 35.
4. Ajoutez les certificats aux fichiers de clés. Voir «Ajout de vos certificats à votre fichier de clés», à la page 38.
5. Demandez à votre partenaire les certificats dont vous avez besoin. Voir «Obtention d'un certificat de votre partenaire», à la page 41.
6. Fournissez à votre partenaire les certificats dont celui-ci est susceptible d'avoir besoin. Voir «Transmission de certificats au partenaire», à la page 43.
7. Si un des certificats utilisés correspond à un fichier PKCS#12, vous devez mettre à jour votre stratégie de cryptographie Java. Voir «La mise à jour de la stratégie de cryptographie», à la page 45.
8. Si vous configurez un environnement de production et que vous n'allez pas utiliser les fichiers de clés et les certificats par défaut, vous pouvez être amené à les supprimer de sorte qu'ils ne soient pas utilisés par inadvertance. Voir «Suppression de fichiers de clés par défaut», à la page 46.

Préparation des fichiers de clés

Quel que soit votre rôle dans la fédération, ou la norme SAML que vous appliquez, vous devez préparer des fichiers de clés dans le service de clés de Tivoli Federated Identity Manager. Les fichiers de clés ont pour fonction de mémoriser les clés et certificats utilisés pour sécuriser le contenu et le transport des messages.

Pourquoi et quand exécuter cette tâche

Le service de clés contient au minimum les deux fichiers de clés suivants :

Fichier des clés de signature et de chiffrement
Le fichier de clés est l'endroit où vous stockez vos clés privées (c'est-à-dire celles que vous utilisez pour les opérations de signature et de déchiffrement, ainsi que pour les certificats client si vous tenez le rôle de client dans une connexion SSL et que votre partenaire exige votre authentification par certificat).

Fichier de clés des certificats de CA (appelé magasin de clés, ou fichier de clés certifiées)
Ce fichier de clés est celui dans lequel vous stockez les clés publiques de votre partenaire (utilisées pour la validation de signatures ou le chiffrement de données auprès de votre partenaire), ainsi que les certificats de CA liés aux autorités de certification que vous accréditez.

Pour préparer le fichier de clés et le fichier de clés certifiées pour votre environnement, plusieurs méthodes sont possibles :

- Utilisez le fichier de clés et le fichier de clés certifiées par défaut, et modifiez leurs mots de passe, afin que leurs mots de passe par défaut ne soient plus en usage. Pour ce faire, consultez la rubrique «Modification du mot de passe d'un fichier de clés».
- Créez un nouveau fichier de clés et un nouveau fichier de clés certifiées, comme décrit à la rubrique «Création d'un fichier de clés», à la page 31, puis importez-les dans le service de clés.

Vous pouvez créer autant de fichiers de clés et de fichiers de clés certifiées que nécessaire, afin de simplifier la répartition des clés en plusieurs catégories uniques pour vos fédérations.

Modification du mot de passe d'un fichier de clés

Vous pouvez modifier le mot de passe d'un fichier de clés ou d'un fichier de clés certifiées à l'aide de la console.

Pourquoi et quand exécuter cette tâche

Vous pouvez être amené à modifier le mot de passe d'un fichier de clés dans les cas suivants :

- Vous voulez utiliser le fichier de clés ou le fichier de clés certifiées par défaut dans un environnement de production.
- La sécurité du mot de passe du fichier de clés est compromise.
- Votre stratégie de sécurité vous impose de modifier périodiquement les mots de passe de fichier de clés.

Procédure

1. Connectez-vous à la console.
2. Cliquez sur **Tivoli Federated Identity Manager → Service de clés**.
   Le panneau Fichiers de clés s'affiche.
3. Sélectionnez un fichier de clés dans le tableau Fichier de clés. Le bouton **Modifier le mot de passe** s'active.
4. Cliquez sur le bouton **Modifier le mot de passe**. Le panneau Modification du mot de passe du fichier de clés s'affiche.

5. Entrez l'ancien mot de passe et le nouveau. L'ancien mot de passe par défaut du fichier de clés et du fichier de clés certifiées est `testonly`.
6. Cliquez sur **OK**. Le mot de passe est modifié.
7. Cliquez sur **Charger les modifications de configuration dans l'environnement d'exécution de Tivoli Federated Identity Manager**.

Que faire ensuite

Répétez ce processus pour chaque fichier de clés dont le mot de passe doit être modifié. Poursuivez ensuite par la création de nouveaux fichiers de clés ou la planification de la sécurité au niveau message.

Création d'un fichier de clés

Vous serez peut-être amené à créer un fichier de clés si vous avez besoin de fichiers de clés supplémentaires ou que vous ne souhaitez pas faire usage des fichiers par défaut. **Remarque :** Le service de clés de Tivoli Federated Identity Manager prend uniquement en charge les fichiers de clés Java (.jks)

Pourquoi et quand exécuter cette tâche

Tivoli Federated Identity Manager n'est doté d'aucune utilitaire pour la création de fichiers de clés. Toutefois, vous pouvez créer un fichier de clés à l'aide de n'importe quel utilitaire de génération de clés. Par exemple, faites appel à l'utilitaire keytool qui est inclus dans WebSphere Application Server pour créer un fichier de clés comme suit :

```
keytool -import -noprompt -trustcacerts -alias myca
-file myca.pem -keystore mykeys.jks -storepass passw0rd
```

Pour plus de détails sur l'utilitaire keytool, consultez le centre de documentation de WebSphere Application Server 6.1, à l'adresse suivante : http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp

Que faire ensuite

Vous devez importer le fichier de clés dans le service de clés Tivoli Federated Identity Manager. Pour plus détails, voir «Importation d'un fichier de clés».

Importation d'un fichier de clés

Si vous avez créé un fichier de clés, vous devez l'importer dans le service de clés de Tivoli Federated Identity Manager avant de pouvoir l'utiliser.

Pourquoi et quand exécuter cette tâche

Procédure

1. Cliquez sur **Tivoli Federated Identity Manager → Service de clés**.

   Le panneau Fichiers de clés s'affiche.
2. Cliquez sur **Importer**. L'assistant d'importation démarre et affiche le panneau Importer le fichier de clés.
3. Entrez un chemin d'accès complet dans la zone **Emplacement du fichier de clés**. Par exemple :

   `/tmp/mykeys.jks`

   Vous pouvez également cliquer sur **Parcourir** pour localiser le fichier de clés sur le système de fichiers.

Remarque : Le fichier de clés à importer doit se trouver sur la même machine que le navigateur utilisé pour accéder à la console d'administration.

4. Entrez le **Mot de passe du fichier de clés**.

   Avertissement : Les clés privées (personnelles) contenues dans un fichier de clés peuvent être chiffrées au moyen d'un mot de passe. Le fichier de clés est lui-même protégé par un mot de passe. Toutefois, le service de clés ne conserve qu'un mot de passe par fichier de clés. Vous devez donc faire en sorte que la clé privée chiffrée et son fichier de clés possèdent le même mot de passe.

5. Entrez le **Nom du fichier de clés**.
6. Indiquez le type.
   - **Clés de signature/chiffrement**
   - **Certificats de CA**

   Le type indique le type de clé ou de certificat que vous souhaitez stocker dans le fichier de clés. Par exemple, si vous souhaitez utiliser ce fichier de clés pour stocker des certificats de votre partenaire, choisissez Certificats de CA. Pour utiliser le fichier de clés afin de stocker vos propres clés de signature, choisissez Clés de signature/chiffrement.

   Le type est indiqué à titre d'information uniquement et ne vous empêche pas d'ajouter d'autres types de clés dans le fichier de clés. Toutefois, l'usage de types cohérents (c'est-à-dire un type privé et un type public) permet de simplifier l'organisation et la localisation des clés.
7. Répétez ces étapes pour chaque fichier de clés à créer pour vos certificats et pour les certificats de votre partenaire.
8. Cliquez sur **Terminer**.

Que faire ensuite

Votre fichier de clés est prêt pour la réception des clés et des certificats. Répétez l'opération pour importer d'autres fichiers de clés, ou passez à l'étape «Planification de la sécurité au niveau message».

Planification de la sécurité au niveau message

Pour démarrer le processus de configuration de la sécurité des messages pour votre environnement, vous devez déterminer vos consignes.

Discutez avec votre partenaire de vos environnements. Utilisez les tables de la liste de contrôle ci-dessous pendant la discussion. Pensez à noter vos consignes dans les tables des listes de contrôle.

Les options dont vous disposez pour sécuriser le contenu des messages dépendent de la norme SAML et du profil que vous utilisez dans votre fédération et, dans certains cas, du rôle (fournisseur d'identité ou de services) qui vous incombe dans la fédération.

Vous avez généralement la possibilité de signer des messages ou des assertions et de valider les signatures de votre partenaire. Dans une fédération SAML 2.0, chaque partenaire doit également chiffrer les données échangées de part et d'autre, puis les déchiffrer afin qu'elles puissent être utilisées dans la fédération.

- Pour effectuer la signature, vous devez utiliser la clé privée provenant de votre biclé (qui comprend une clé publique et une clé privée).
- Pour effectuer la validation, vous devez utiliser la clé publique de votre partenaire, qui correspond à la clé privée utilisée par ce partenaire lors de la signature des données.
- Pour effectuer le chiffrement, vous devez utiliser la clé publique de votre partenaire, qui correspond à la clé privée utilisée par ce partenaire lors du déchiffrement des données. De même, vous devez fournir votre clé publique à votre partenaire, lequel l'utilisera pour chiffrer les données à votre intention, puis vous pourrez déchiffrer ces données à l'aide de votre clé privée correspondante.

Référez-vous à la liste de contrôle suivante pour identifier les paires de clés publiques et privées requises, ainsi que les clés nécessaires aux échanges avec votre partenaire.

Vos clés

Vous devez utiliser la *clé privée* issue d'une biclé publique/privée pour accomplir les actions indiquées dans le tableau suivant. Vous pouvez utiliser la même clé pour toutes ces actions, ou une différente par action. Toutes les clés sont facultatives et accessibles à l'ensemble des normes et règles de fournisseurs SAML, *sauf mention contraire* dans la colonne Remarques.

Tableau 5. Vos clés

But de la clé	Alias de la paire clé publique/clé privée	Fichier de stockage de la clé	Remarque
Clé de signature des messages			Requise si vous êtes un fournisseur d'identité dans une fédération SAML 1.x. **Remarque :** Dans SAML 2.0, la même clé est utilisée pour la signature des messages et assertions.
Clé de signature des assertions			Requise pour les fournisseurs d'identité. **Remarque :** Dans SAML 2.0, la même clé est utilisée pour la signature des messages et assertions.
Clé de déchiffrement			Requise dans SAML 2.0. Non disponible dans les fédérations SAML 1.x.

Clés requises fournies par votre partenaire

Vous devez utiliser la *clé publique* issue d'une biclé publique/privée fournie par votre partenaire pour accomplir les actions indiquées. La colonne Remarques indique si une clé est requise, ou si elle ne peut être utilisée en raison d'un rôle de fournisseur spécifique, ou de la spécification SAML en vigueur dans la fédération. Dans la plupart des cas, vous obtenez les clés de la part de votre partenaire au moyen d'un fichier de métadonnées. Toutefois, si vous utilisez une fédération SAML 1.x, il se peut que vous deviez obtenir ces clés manuellement. Envisagez de partager ce tableau avec votre partenaire, afin de vous assurer que celui-ci a pris connaissance des clés qu'il doit vous fournir.

Tableau 6. Clés requises fournies par votre partenaire

But de la clé	Alias de clé publique	Fichier de clés certifiées pour le stockage	Remarque
Clé de validation pour les signatures de messages			Correspond à la clé de signature de votre partenaire. Requise si votre partenaire doit signer des messages.
Clé de validation pour les signatures d'assertion			Correspond à la clé de signature de votre partenaire. Requise si votre partenaire doit signer des assertions. Non disponible pour les fournisseurs d'identité SAML 1.x.
Clé de chiffrement			Correspond à la clé de déchiffrement de votre partenaire. Requise dans SAML 2.0. Non disponible dans les fédérations SAML 1.x.

Clés que vous devez fournir à votre partenaire

Vous devez *fournir la clé publique* issue de votre biclé publique/privée à votre partenaire afin que celui-ci puisse pour accomplir les actions indiquées. La colonne Remarques indique si une clé est requise, ou si elle ne peut être utilisée en raison d'un rôle de fournisseur spécifique, ou de la spécification SAML en vigueur dans la fédération. Dans la plupart des cas, vous fournissez les clés en exportant les propriétés de votre fédération dans un fichier de métadonnées, que votre partenaire importe ensuite dans sa configuration. Toutefois, si vous utilisez une fédération SAML 1.x, il se peut que vous deviez exporter ces clés manuellement depuis votre fédération afin de les fournir à votre partenaire.

Tableau 7. Clés que vous devez fournir à votre partenaire

But de la clé	Alias de la paire clé publique/clé privée	Fichier de stockage de la clé	Remarque
Clé de validation pour les signatures de messages			Correspond à votre clé de signature. Requise si vous devez signer des messages.
Clé de validation pour les signatures d'assertion			Correspond à votre clé de signature. Requise si vous devez signer des assertions. Non disponible pour les fournisseurs d'identité SAML 1.x.
Clé de chiffrement			Correspond à votre clé de déchiffrement. Requise dans SAML 2.0. Non disponible dans les fédérations SAML 1.x.

Obtention de vos clés et certificats

Après avoir déterminé quelles clés et quels certificats vous devez utiliser pour la signature et le déchiffrement, vous devez obtenir ces éléments.

Pourquoi et quand exécuter cette tâche

En règle générale, les clés privées que vous devez obtenir sont les suivantes :

Clé de signature
Si vous devez signer des messages ou des assertions, vous devez posséder une biclé publique/privée et utiliser la clé privée pour la signature.

Clé de déchiffrement
Si vous utilisez SAML 2.0, votre partenaire doit chiffrer les données à votre intention. Vous devez posséder une biclé publique/privée pour pouvoir exécuter cette opération. Votre partenaire utilisera votre clé publique pour chiffrer les données qu'il vous envoie et vous utiliserez votre clé privée pour les déchiffrer.

La méthode utilisée pour obtenir ces clés varie selon que vous utilisez un environnement de test ou un environnement de production :

- Dans un environnement de test, vous pouvez utiliser la clé de test par défaut, ou créer un certificat d'auto-signature. Voir «Utilisation de la clé par défaut en tant que clé de signature et de déchiffrement», à la page 36 ou «Création de certificats d'auto-signature», à la page 36.

- Dans un environnement de production, vous devez demander vos clés à une autorité de certification. Voir «Demande de certificats signés par l'autorité de certification», à la page 37.

Les types de certificats ci-dessous peuvent être utilisés dans le service de clés Tivoli Federated Identity Manager. Lors de l'obtention de certificats, veillez à utiliser les types pris en charge suivants :

- PEM

  Format PEM (Privacy-Enhanced Message). Il s'agit des certificats publics au format PEM.

- PKCS#12

  Public Key Cryptography Standard 12 : norme d'échange d'informations personnelles.

  Avant d'utiliser des certificats PKCS#12, vous devez mettre à jour la règle de cryptographie. Voir «La mise à jour de la stratégie de cryptographie», à la page 45.

Utilisation de la clé par défaut en tant que clé de signature et de déchiffrement

Vous pouvez, dans un environnement de test, utiliser la clé d'essai contenue dans le fichier DefaultKeyStore en tant que clé de signature et clé de déchiffrement.

Pourquoi et quand exécuter cette tâche

Assurez-vous que la clé `testkey` se trouve dans le fichier de clés. Aucune autre préparation n'est nécessaire pour cette clé.

Création de certificats d'auto-signature

Dans un environnement de test, vous pouvez utiliser un certificat d'auto-signature pour votre signature et comme clé de déchiffrement ou comme un certificat d'authentification de l'application client que vous présentez au serveur lors d'une communication SSL.

Pourquoi et quand exécuter cette tâche

Un certificat d'auto-signature est une paire de clés publique/privée générée de manière aléatoire et signée par sa propre clé privée. La création d'un certificat d'auto-signature s'effectue via l'utilitaire de Tivoli Federated Identity Manager ou d'un autre utilitaire de création de clés. La procédure suivante décrit le maniement de l'utilitaire Tivoli Federated Identity Manager.

Remarque : Cette procédure n'est prise en charge que par WebSphere Application Server Version 6.1.

Procédure

1. Connectez-vous à la console.
2. Cliquez sur **Tivoli Federated Identity Manager → Service de clés**.

   Le panneau Fichiers de clés s'affiche.
3. Sélectionnez un fichier de clés dans le tableau Fichier de clés. Le bouton **Afficher les clés** s'active.
4. Cliquez sur **Afficher les clés**. Le panneau Mot de passe s'affiche.
5. Entrez le mot de passe du fichier de clés, puis cliquez sur **OK**.

6. Cliquez sur **Créer un certificat d'auto-signature**. Le panneau Créer un certificat d'auto-signature s'affiche.
7. Remplissez les zones du panneau. Ensuite, cliquez sur **OK**. Une paire de clés publique/privée est ajoutée au fichier de clés.
8. Cliquez sur le bouton **Charger les modifications de configuration dans l'environnement d'exécution de Tivoli Federated Identity Manager**.

Que faire ensuite

Pour vérifier que le certificat a été créé, répétez les étapes 1 à 5, à la page 36.

Demande de certificats signés par l'autorité de certification

Dans un environnement de production, vous avez besoin de recevoir des certificats de signature, de déchiffrement et d'authentification de l'application client émis et signés par une autorité de certification. Vous pouvez générer une demande de certificat de signature à l'aide de la console.

Avant de commencer

Vérifiez que vous disposez d'un fichier de clés dans lequel vous pouvez stocker la demande de certificat et, par la suite, le certificat.

Pourquoi et quand exécuter cette tâche

Une demande de certificat de signature (RSC) est un fichier électronique que vous envoyez (par e-mail, via FTP ou par tout autre moyen de communication exigé par l'autorité de certification) à une CA (VeriSign, Thawte, etc.) pour requérir un certificat signé par elle.

Sur la base des données contenues dans la RSC, la CA génère le certificat, puis le signe à l'aide de sa propre clé privée.

Cette signature valide la fiabilité du certificat.

Une RSC contient les données suivantes :

- L'identité du demandeur (vous) sous forme d'un nom distinctif du sujet.
- Les extensions du certificat (le cas échéant).
- La clé publique du certificat.
- Les algorithmes à utiliser pour la signature et la clé.

Une fois la demande générée, un certificat d'auto-signature temporaire est créé dans le fichier de clés. Il sera remplacé par le certificat signé par la CA lorsque vous recevrez celui-ci.

Remarque : Cette procédure n'est prise en charge que par WebSphere Application Server Version 6.1.

Procédure

1. Connectez-vous à la console.
2. Cliquez sur **Tivoli Federated Identity Manager → Service de clés**.
   Le panneau Fichiers de clés s'affiche.
3. Sélectionnez un fichier de clés dans le tableau Fichier de clés. Le bouton **Afficher les clés** s'active.

4. Cliquez sur **Afficher les clés**. Le panneau Mot de passe s'affiche.
5. Entrez le mot de passe du fichier de clés, puis cliquez sur **OK**.
6. Cliquez sur **Créer une demande de certificat**. Le panneau Créer une demande de certificat s'affiche.
7. Remplissez les zones du panneau. Ensuite, cliquez sur **OK**. La fenêtre Requête de signature de certificat générée s'affiche.
8. Copiez et collez le texte de la demande dans un fichier texte ou cliquez sur le bouton **Exporter la requête de signature de certificat** pour le télécharger. Le fichier enregistré ou téléchargé peut désormais être envoyé à une CA.
9. Cliquez **Terminé** après avoir enregistré le fichier. Une paire de clés publique/privée est ajoutée au fichier de clés et un fichier contenant les données BASE64 codées est créé. Le certificat d'auto-signature temporaire sera remplacé par le certificat signé par la CA.
10. Cliquez sur le bouton **Charger les modifications de configuration dans l'environnement d'exécution de Tivoli Federated Identity Manager**.

Que faire ensuite

Répétez cette procédure pour chaque certificat que vous souhaitez demander. Par exemple, vous pouvez demander un certificat distinct pour chaque activité (signature, déchiffrement et authentification de l'application client) ou utiliser un seul certificat pour toutes les activités. Une fois toutes vos demandes de certificats de signature créées, suivez les instructions de la CA pour lui transmettre le fichier de la demande. Ensuite, poursuivez la réception du certificat émis par la CA en suivant la procédure décrite dans «Réception d'un certificat signé de la part d'une autorité de certification», à la page 40.

Ajout de vos certificats à votre fichier de clés

Avant d'établir votre fédération, vous devez ajouter les clés que vous utiliserez pour la signature et le déchiffrement de votre fichier de clés.

Pourquoi et quand exécuter cette tâche

La méthode permettant d'ajouter vos clés à votre fichier de clés dépend de la manière dont vous les avez obtenues :

Création d'un certificat d'auto-signature
Si vous avez créé un certificat d'auto-signature via l'utilitaire de Tivoli Federated Identity Manager, ce certificat a été importé automatiquement dans votre fichier de clés. Si vous avez créé un certificat d'auto-signature à l'aide d'un utilitaire différent de celui qui est fourni avec Tivoli Federated Identity Manager, vous devez importer votre certificat dans le fichier de clés comme décrit à la rubrique «Importation d'un certificat», à la page 39.

Demande d'un certificat signé
Si vous avez généré une demande de signature de certificat et envoyé celle-ci à une autorité de certification, vous recevrez le certificat dans votre fichier de clés, comme décrit à la rubrique «Réception d'un certificat signé de la part d'une autorité de certification», à la page 40.

Importation d'un certificat

Pourquoi et quand exécuter cette tâche

Vous pouvez avoir besoin d'importer un certificat que vous avez reçu dans les circonstances suivantes :

- Vous avez créé un certificat d'auto-signature à l'aide d'un utilitaire différent de celui qui est fourni avec Tivoli Federated Identity Manager
- Vous avez obtenu manuellement un certificat auprès d'une CA

Il peut également être nécessaire d'importer un certificat que vous avez reçu de la part de votre partenaire. Pour plus d'informations sur l'importation de certificats de partenaire, voir «Importation d'un certificat depuis votre partenaire», à la page 42.

Avertissement : Vous pouvez chiffrer les clés privées (personnelles) contenues dans un fichier de clés à l'aide d'un mot de passe. Le fichier de clés lui-même est protégé par mot de passe. Toutefois, le service de clés ne retient qu'un mot de passe pour un fichier de clés. En conséquence,la clé privée chiffrée et son fichier de clés doivent partager le même mot de passe.

Cette tâche permet d'importer les éléments suivants :

- Un certificat à partir d'un fichier PEM
- Une clé à partir d'un fichier PKCS#12.

  Remarque : Si vous allez utiliser un fichier PKCS#12, veillez à suivre également les instructions de la section «La mise à jour de la stratégie de cryptographie», à la page 45.

Vérifiez que votre clé ou votre certificat est prêt et disponible avant de poursuivre cette procédure.

Les clés importées sont activées par défaut.

Procédure

1. Cliquez sur **Tivoli Federated Identity Manager → Service de clés**.
   Le panneau Fichiers de clés s'affiche.
2. Sélectionnez un fichier de clés dans le tableau Fichier de clés pour y stocker votre paire de clés publique/privée. Le bouton **Afficher les clés** est activé.

Avertissement : N'importez pas des clés privées (par exemple, des clés de signature ou de chiffrement) dans un fichier de clés **Certificat de CA**. Ce type de fichier de clés ne permet pas de stocker un mot de passe de clé (obligatoire pour les clés privées).

3. Cliquez sur **Afficher les clés**. Ensuite, entrez le mot de passe du fichier de clés lorsque vous y êtes invité, puis cliquez sur **OK**. Le panneau Clés s'affiche. Il répertorie les éléments du fichier de clés sélectionné.
4. Cliquez sur le bouton **Importer**. L'assistant de clé démarre et affiche le panneau Bienvenue.
5. Cliquez sur **Suivant** Le panneau Format de fichier de clés s'affiche.
6. Sélectionnez le **format de fichier de clés** adapté au fichier à importer. Cliquez ensuite sur **Suivant**. Les formats ci-dessous sont disponibles :

   PEM)
   (Privacy-Enhanced Message) Certificat public

PKCS#12
Public Key Cryptography Standard 12 : norme d'échange d'informations personnelles

JKS
Fichier de clés Java

Le panneau **Télécharger le fichier de clés (Upload Key File)** s'affiche.

7. Indiquez le chemin d'accès à l'emplacement de la clé puis, si vous y êtes invité, entrez le mot de passe du ficher de clés. Cliquez ensuite sur **Suivant**.
8. Entrez un intitulé pour la clé et, à l'invite, sélectionnez la clé à importer. Cliquez ensuite sur **Suivant**.
9. Un panneau récapitulatif s'affiche. Cliquez sur **Terminer** pour quitter l'assistant.
10. Répétez cette procédure pour importer l'ensemble des clés et certificats que vous utiliserez dans la fédération.

Que faire ensuite

Vous pouvez ensuite ajouter les clés de votre partenaire à votre fichier de clés certifiées. Voir «Obtention d'un certificat de votre partenaire», à la page 41.

Réception d'un certificat signé de la part d'une autorité de certification

Si vous envoyez à une CA une demande de certificat signé créée à l'aide de la console, vous pouvez recevoir le certificat de la CA dans votre fichier de clés.

Avant de commencer

Vérifiez que vous avez suivi la procédure décrite dans «Demande de certificats signés par l'autorité de certification», à la page 37 et enregistré le certificat émis par la CA dans un emplacement accessible au service de clés.

Procédure

1. Connectez-vous à la console.
2. Cliquez sur **Tivoli Federated Identity Manager → Service de clés**.
   Le panneau Fichiers de clés s'affiche.
3. Sélectionnez le fichier dans lequel la RSC a été générée dans le tableau Fichiers de clés. Le bouton **Afficher les clés** est activé.
4. Cliquez sur **Afficher les clés**. Le panneau Mot de passe s'affiche.
5. Entrez le mot de passe du fichier de clés, puis cliquez sur **OK**.
6. Cliquez sur **Réception de certificat de CA**.
7. Sélectionnez l'emplacement du certificat que vous avez reçu de la CA. Ensuite, cliquez sur **OK**. Le certificat d'auto-signature temporaire présent dans le fichier de clés est remplacé par le certificat signé que vous avez reçu.
8. Cliquez sur le bouton **Charger les modifications de configuration dans l'environnement d'exécution de Tivoli Federated Identity Manager**.

Que faire ensuite

Vous pouvez ensuite ajouter les clés de votre partenaire à votre fichier de clés certifiées. Voir «Obtention d'un certificat de votre partenaire», à la page 41.

Obtention d'un certificat de votre partenaire

En fonction des besoins de votre environnement, vous devez peut-être vous procurer des certificats auprès de votre partenaire.

Avant de commencer

Utilisez le formulaire «Planification de la sécurité au niveau message», à la page 32 pour déterminer les certificats que vous devez peut-être demander à votre partenaire. En règle générale, les clés publiques que vous devez obtenir auprès de votre partenaire sont les suivantes :

Clé de validation
Si votre partenaire signe les messages ou assertions et que vous devez valider ces signatures, vous devez être en possession de la clé publique correspondant à celle qui a été utilisée pour la signature.

Clé de chiffrement
Si vous devez procéder au chiffrement des données que vous envoyez à votre partenaire, vous devez obtenir une clé publique auprès de celui-ci. L'utilisation de cette clé publique est destinée au chiffrement des données, lesquelles seront déchiffrées par votre partenaire au moyen de sa clé privée correspondante.

Pourquoi et quand exécuter cette tâche

Dans une fédération SAML 2.0, vous recevez généralement les clés de validation et de chiffrement de votre partenaire sous la forme d'un fichier de métadonnées fourni par votre partenaire. Ce processus est expliqué plus en détails à la section «Importation de certificats à partir du fichier de métadonnées de votre partenaire». En plus de ces clés, d'autres informations de votre partenaire, telles que le nom de l'entreprise, sont inclues dans le fichier de métadonnées. Lorsque vous créez votre partenaire dans la fédération, vous êtes invité à sauvegarder les clés du partenaire dans le fichier de clés approprié. Il convient de sauvegarder les clés du partenaire dans votre fichier de clés certifiées.

Si vous avez déjà reçu les métadonnées de la part de votre partenaire et que vous avez uniquement besoin de recevoir un nouveau certificat de sa part, que que vous utilisez une fédération SAML 1.x, vous pouvez recevoir les clés manuellement (par exemple, via FTP, par e-mail ou une autre méthode de transfert), puis les importer dans votre fichier de clés certifiées en suivant les instructions de la rubrique «Importation d'un certificat depuis votre partenaire», à la page 42.

Importation de certificats à partir du fichier de métadonnées de votre partenaire

Si un fichier de métadonnées relatif à la configuration de votre fédération vous est fourni par votre partenaire, il convient que les clés publiques de ce dernier soient incluses dans ce fichier.

Pourquoi et quand exécuter cette tâche

Selon la sécurité définie pour les messages et la spécification SAML que vous appliquez avec votre partenaire sur la fédération, il convient que le fichier de métadonnées contienne l'une ou plusieurs des clés publiques suivantes :

- Clé de validation des assertions signées, si vous êtes censé valider les assertions signées par votre partenaire

- Clé de validation des messages signés, si vous êtes censé valider les messages signées par votre partenaire
- Clé de chiffrement (dans une fédération SAML 2.0)

Voir «Planification de la sécurité au niveau message», à la page 32.

Si votre partenaire utilise Tivoli Federated Identity Manager, les clés publiques qui correspondent aux clés privées que le partenaire a définies dans sa configuration sont automatiquement ajoutées au fichier de métadonnées au moment où le partenaire exporte sa configuration.

Si vous obtenez les clés de votre partenaire à partir d'un fichier de métadonnées, vous devez importer les métadonnées dans le cadre de l'établissement de votre fédération. Pour poursuivre, exécutez les tâches indiquées dans ce chapitre.

Importation d'un certificat depuis votre partenaire

Vous pouvez obtenir les clés publiques de votre partenaire via une connexion SSL, ou en important un fichier de métadonnées contenant les paramètres de la configuration du partenaire. Toutefois, si aucune de ces méthodes n'est disponible, vous pouvez obtenir les clés manuellement et les importer.

Avant de commencer

Avant de commencer cette tâche, assurez-vous d'avoir reçu une ou plusieurs clés publiques de la part de votre partenaire (par exemple, via FTP, par e-mail ou une autre méthode de transfert).

Pourquoi et quand exécuter cette tâche

Vous pouvez avoir besoin d'importer un certificat dans les circonstances suivantes :

- Un certificat d'auto-signature créé à l'aide d'un utilitaire autre que celui fourni avec Tivoli Federated Identity Manager
- Certificat obtenu manuellement auprès d'une autorité de certification

Il peut également être nécessaire d'importer un certificat que vous avez reçu de la part de votre partenaire. Pour plus d'informations sur l'importation de certificats de partenaire, voir «Importation d'un certificat depuis votre partenaire».

Avertissement : Vous pouvez chiffrer les clés privées (personnelles) contenues dans un fichier de clés à l'aide d'un mot de passe. Le fichier de clés lui-même est protégé par mot de passe. Toutefois, le service de clés ne retient qu'un mot de passe pour un fichier de clés. En conséquence,la clé privée chiffrée et son fichier de clés doivent partager le même mot de passe.

Cette tâche permet d'importer les éléments suivants :

- Un certificat à partir d'un fichier PEM
- Une clé à partir d'un fichier PKCS#12.

  Remarque : Si vous allez utiliser un fichier PKCS#12, veillez à suivre également les instructions de la section «La mise à jour de la stratégie de cryptographie», à la page 45.

Vérifiez que votre clé ou votre certificat est prêt et disponible avant de poursuivre cette procédure.

Les clés importées sont activées par défaut.

Procédure

1. Cliquez sur **Tivoli Federated Identity Manager → Service de clés**.
   Le panneau Fichiers de clés s'affiche.
2. Sélectionnez un fichier de clés dans le tableau Fichier de clés pour y stocker votre paire de clés publique/privée. Le bouton **Afficher les clés** est activé.

Avertissement : N'importez pas des clés privées (par exemple, des clés de signature ou de chiffrement) dans un fichier de clés **Certificat de CA**. Ce type de fichier de clés ne permet pas de stocker un mot de passe de clé (obligatoire pour les clés privées).

3. Cliquez sur **Afficher les clés**. Ensuite, entrez le mot de passe du fichier de clés lorsque vous y êtes invité, puis cliquez sur **OK**. Le panneau Clés s'affiche. Il répertorie les éléments du fichier de clés sélectionné.
4. Cliquez sur le bouton **Importer**. L'assistant de clé démarre et affiche le panneau Bienvenue.
5. Cliquez sur **Suivant** Le panneau Format de fichier de clés s'affiche.
6. Sélectionnez le **format de fichier de clés** adapté au fichier à importer. Cliquez ensuite sur **Suivant**. Les formats ci-dessous sont disponibles :

   PEM)
   (Privacy-Enhanced Message) Certificat public

   PKCS#12
   Public Key Cryptography Standard 12 : norme d'échange d'informations personnelles

   JKS
   Fichier de clés Java

   Le panneau **Télécharger le fichier de clés (Upload Key File)** s'affiche.
7. Indiquez le chemin d'accès à l'emplacement de la clé puis, si vous y êtes invité, entrez le mot de passe du ficher de clés. Cliquez ensuite sur **Suivant**.
8. Entrez un intitulé pour la clé et, à l'invite, sélectionnez la clé à importer. Cliquez ensuite sur **Suivant**.
9. Un panneau récapitulatif s'affiche. Cliquez sur **Terminer** pour quitter l'assistant.
10. Répétez cette procédure pour importer l'ensemble des clés et certificats que vous utiliserez dans la fédération.

Que faire ensuite

Vous devez ensuite fournir les clés à votre partenaire. Voir «Transmission de certificats au partenaire».

Transmission de certificats au partenaire

En fonction des besoins de votre environnement, vous devez peut-être fournir une clé à votre partenaire.

Avant de commencer

Utilisez votre «Planification de la sécurité au niveau message», à la page 32, pour déterminer les certificats que vous devez peut-être fournir à votre partenaire. En règle générale, les clés publiques que vous devez obtenir sont les suivantes :

Clé de validation
Si vous devez signer des messages ou des assertions et que votre partenaire doit valider ces signatures, vous devez fournir la clé publique correspondant à celle qui a été utilisée pour la signature.

Clé de chiffrement
Pour que votre partenaire puisse chiffrer les données à votre intention, vous devez lui fournir une clé publique. Votre partenaire utilisera cette clé publique pour le chiffrement des données, que vous pourrez déchiffrer au moyen de votre clé privée correspondante.

Pourquoi et quand exécuter cette tâche

La délivrance de votre clé de validation et de chiffrement s'effectue généralement au moyen d'un fichier de métadonnées, que vous créez et fournissez à votre partenaire. En plus de ces clés, d'autres informations vous concernant, telles que le nom de votre entreprise, sont inclues dans le fichier de métadonnées. La création de ce fichier a lieu ultérieurement au cours du processus de configuration. Pour plus d'informations, voir «Exportation de certificats dans un fichier de métadonnées».

Dans une fédération SAML 1.0, vous avez également la possibilité de fournir manuellement ces informations à votre partenaire. Pour plus d'informations, voir «Exportation d'un certificat», à la page 45. Vous pouvez également faire appel à la méthode manuelle si vous avez déjà fourni vos métadonnées à votre partenaire et que vous avez besoin de délivrer un certificat mis à jour par vos soins.

Exportation de certificats dans un fichier de métadonnées

Si vous fournissez à votre partenaire un fichier de métadonnées sur la configuration de votre fédération, vos clés publiques sont incluses dans ce fichier.

Pourquoi et quand exécuter cette tâche

Selon la sécurité définie pour les messages et la spécification SAML que vous appliquez avec votre partenaire sur la fédération, il convient que le fichier de métadonnées contienne l'une ou plusieurs des clés publiques suivantes :

- Clé que le partenaire utilise pour la validation des assertions signées, si vous signez les assertions
- Clé que le partenaire utilise pour la validation des messages signées, si vous signez les messages
- Clé que le partenaire utilise pour le chiffrement des messages à votre intention (dans une fédération SAML 2.0)

Voir «Planification de la sécurité au niveau message», à la page 32.

Si votre partenaire utilise Tivoli Federated Identity Manager, vous pouvez exporter votre configuration vers un un fichier de métadonnées, y compris vos clés, afin que votre partenaire puisse importer le fichier.

Si vous choisissez cette méthode pour fournir les clés à votre partenaire, il convient que exportiez les métadonnées dans le cadre de l'établissement de votre fédération. Pour poursuivre, exécutez les tâches indiquées dans ce chapitre.

Exportation d'un certificat

Pourquoi et quand exécuter cette tâche

Cette tâche permet d'exporter vos certificats si vous n'êtes pas en mesure de fournir à votre partenaire un fichier de métadonnées contenant vos clés.

Procédure

1. Cliquez sur **Tivoli Federated Identity Manager → Service de clés**.

   Le panneau Fichiers de clés s'affiche.
2. Sélectionnez le fichier de clés approprié dans le tableau Fichier de clés. Vous êtes invité à entrer le mot de passe du fichier de clés.
3. Entrez le mot de passe du fichier de clés et cliquez sur **OK**. Le bouton **Afficher les clés** s'active.
4. Cliquez sur **Afficher les clés**. Le panneau Clés s'affiche. Il répertorie les éléments du fichier de clés sélectionné.
5. Sélectionnez les clés à exporter, puis cliquez sur le bouton **Exporter**. Le panneau Exporter la clé s'affiche.
6. Sélectionnez le format de la clé à exporter.

   (PEM)
   (Privacy-Enhanced Message) Certificat public

   PKCS#12
   Public Key Cryptography Standard 12 : norme d'échange d'informations personnelles
7. Vérifiez que la case **Inclure une clé privée** *n'est pas* cochée. Vous devez être la seule personne à détenir votre clé privée.
8. Cliquez sur **Télécharger la clé**.
9. Lorsque vous y êtes invité, entrez le nom de fichier de la clé exportée.

   Par exemple : `maclépublique.pem`

   Vous pouvez également cliquer sur **Parcourir** pour localiser le fichier sur le système de fichiers.
10. Cliquez sur **Annuler** pour quitter.

La mise à jour de la stratégie de cryptographie

L'utilisation de la technologie de chiffrement est contrôlée par la législation des Etats-Unis. Les SDK IBM Java comprennent des fichiers de règles de juridiction strictes, mais limitées. Avant d'utiliser les fichiers PKCS#12 avec Tivoli Federated Identity Manager, vous devez vous procurer les fichiers de règles JCE (Java Cryptography Extension) de juridiction illimitée.

Pourquoi et quand exécuter cette tâche

Pour consulter les informations de sécurité relatives aux kits de développement de logiciels IBM Java, accédez à l'adresse URL suivante :

`http://www.ibm.com/developerworks/java/jdk/security/index.html`

Pour vous procurer les fichiers de règles de juridiction illimitée, procédez comme suit :

Procédure

1. Mettez à jour WebSphere à l'aide de fichiers de règles JCE (Java Cryptography Extension) non limitées. Accès : http://www.ibm.com/developerworks/java/jdk/security/index.html
2. Sélectionnez le lien vers le SDK qui correspond à votre environnement, par exemple, pour Java 1.5, le SDK est J2SE 5.0. Une page affichant l'en-tête Security Information (informations de sécurité) apparaît.
3. Sélectionnez le lien suivant : **IBM SDK Policy Files**.

   Remarque : Lorsque vous cliquez sur ce lien, vous êtes redirigé vers le fichier de règles contenu dans le kit SDK compatible avec votre version de Java. Il est à noter, toutefois, que le numéro de version du kit SDK n'est pas nécessairement le même que celui de la version de Java utilisée. Par exemple, pour Java 1.5, vous pouvez être redirigé vers le kit SDK 1.4.
4. Le programme vous demande de vous connecter à l'aide de votre ID utilisateur et de votre mot de passe IBM. Si vous n'avez ni ID utilisateur, ni mot de passe IBM, vous devrez vous inscrire. Suivez le lien de la page de connexion relatif à l'inscription.
5. Connectez-vous au service de support IBM.
6. A l'invite, sélectionnez le fichier .zip correspondant à la version de Java que vous utilisez. Cliquez ensuite sur **Continuer** pour démarrer le téléchargement.
7. Décomprimez le fichier .zip. Les fichiers JAR sont les suivants :
   - local_policy.jar
   - US_export_policy.jar
8. Placez les fichiers dans le répertoire suivant :

   rep_installation_composant_exec_Java/jre/lib/security

   Par exemple, il se peut que le composant d'exécution Java ait été installé dans le cadre de la version imbriquée de WebSphere Application Server. Dans ce cas, le répertoire peut être le suivant :

   /opt/IBM/FIM/*ewas*/java/jre/lib/security

Suppression de fichiers de clés par défaut

Des fichiers de clé et des certificats par défaut sont inclus dans Tivoli Federated Identity Manager. Si vous avez créé os propres fichiers de clés, vous pouvez être amené à supprimer les fichiers de clés par défaut. Toutefois, cette tâche est facultative.

Procédure

1. Cliquez sur **Tivoli Federated Identity Manager → Service de clés**.

   Le panneau Fichiers de clés s'affiche.
2. Sélectionnez **DefaultKeyStore**, puis cliquez sur **Supprimer**. Un message vous invite à confirmer que vous voulez supprimer le fichier de clés indiqué.
3. Cliquez sur **OK** pour supprimer le magasin de clés.
4. Sélectionnez **DefaultTrustedKeyStore**, puis cliquez sur **Supprimer**. Un message vous invite à confirmer que vous voulez supprimer le fichier de clés indiqué.
5. Cliquez sur **OK** pour supprimer le magasin de clés.

Activation de la vérification du retrait de certificat

Vous pouvez recourir au gestionnaire d'accréditation IbmPKIX pour déterminer la validité des certificats serveur. Si vous activez cette fonction, le gestionnaire d'accréditation vérifie le certificat présenté par le serveur SSL lorsque le client SOAP établit une connexion SSL. S'il découvre que le certificat a été retiré, l'opération de fédération échoue.

Pourquoi et quand exécuter cette tâche

L'activation de la vérification du retrait de certificat nécessite les procédures suivantes :

- «Activation du contrôle de la révocation de certificat sous WebSphere».
- «Activation du gestionnaire d'accréditation IbmPKIX», à la page 49.

Activation du contrôle de la révocation de certificat sous WebSphere

Avant de pouvoir activer le contrôle de retrait de certificat sur Tivoli Federated Identity Manager, vous devez activer certains paramètres dans WebSphere Application Server.

Pourquoi et quand exécuter cette tâche

La procédure à suivre pour activer les paramètres varie selon que vous utilisez la version intégrée de WebSphere Application Server ou une version existante de WebSphere Application Server. Choisissez la procédure appropriée suivant votre installation :

Version intégrée de WebSphere Application Server
«Activation de CRC sur une instance intégrée de WebSphere Application Server»,

Version existante de WebSphere Application Server
«Activation de CRC sur une instance existante de WebSphere Application Server», à la page 48.

Activation de CRC sur une instance intégrée de WebSphere Application Server

Si vous utilisez la version intégrée de WebSphere Application Server, vous devez activer les paramètres requis pour le contrôle du retrait de certificats (CRC) avant de configurer le contrôle de retrait de certificat dans votre environnement Tivoli Federated Identity Manager.

Avant de commencer

Avertissement : N'appliquez cette procédure que si vous avez installé Tivoli Federated Identity Manager à l'aide de la version intégrée de WebSphere Application Server.

Pourquoi et quand exécuter cette tâche

Pour activer les paramètres appropriés, procédez comme suit :

Procédure

1. Ouvrez une invite de commande.
2. Démarrez l'outil 'wsadmin' de WebSphere Application Server. A partir de votre profil WebSphere, entrez la commande appropriée afin que votre système d'exploitation démarre l'outil :

   Windows

   ```
   wsadmin.bat
   ```

   AIX, Linux, HP-UX ou Solaris

   ```
   wsadmin.sh
   ```

   Remarque : Pour de plus amples informations sur les options pouvant être définies à l'aide de l'outil wsadmin, reportez-vous au centre d'information en ligne à l'adresse http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp.
3. A l'invite de commande, exécutez les commandes suivantes en remplaçant *server1* par le nom de votre serveur :

   ```
   set jvm [$AdminConfig getid
     /Server:server1/JavaProcessDef:/JavaVirtualMachine:/]
    $AdminConfig modify $jvm {{genericJvmArguments
     "-Dcom.ibm.jsse2.checkRevocation=true
      -Dcom.ibm.security.enableCRLDP=true"}}
    $AdminConfig save
   ```
4. Redémarrez WebSphere Application Server.

Que faire ensuite

Allez aux étapes de la section «Activation du gestionnaire d'accréditation IbmPKIX», à la page 49.

Activation de CRC sur une instance existante de WebSphere Application Server

Si vous avez installé Tivoli Federated Identity Manager sur une version existante de WebSphere Application Server, vous devez activer le gestionnaire d'accréditation IbmPKIX avant de configurer le contrôle de retrait de certificat dans votre environnement Tivoli Federated Identity Manager.

Procédure

1. Connectez-vous à la console de votre instance WebSphere Application Server.
2. Cliquez sur **Serveurs** → **Serveurs d'application**.
3. Sélectionnez votre serveur.
4. Cliquez sur **Gestion des processus et Java** → **Définition des processus** → **Machine virtuelle Java**.
5. Sous Arguments JVM génériques, ajoutez le texte suivant :

   ```
   dcom.ibm.jsse2.checkRevocation=true
   Dcom.ibm.security.enableCRLDP=true
   ```
6. Redémarrez WebSphere Application Server.

Que faire ensuite

Allez aux étapes de la section «Activation du gestionnaire d'accréditation IbmPKIX».

Activation du gestionnaire d'accréditation IbmPKIX

Pour activer la vérification du retrait de certificat, vous devez d'abord permettre à Tivoli Federated Identity Manager d'utiliser le gestionnaire d'accréditation IbmPKIX.

Procédure

1. Connectez-vous à la console, puis cliquez sur **Tivoli Federated Identity Manager → Gestion de la configuration → Gestion des noeuds d'exécution**.
2. Le panneau Gestion des noeuds d'exécution s'affiche. Cliquez sur **Propriétés personnalisées de l'environnement d'exécution**. Le panneau Propriétés personnalisées de l'environnement d'exécution s'affiche.
3. uliquez sur **Créer**. Un élément est ajouté à la liste des propriétés, avec le nom **nouvelle clé** et la valeur **nouvelle valeur**.
4. Cliquez de nouveau sur **Créer**. Un autre élément est ajouté à la liste des propriétés, avec le nom **nouvelle clé** et la valeur **nouvelle valeur**.
5. Sélectionnez une des propriétés de la marque de réservation.
6. Tapez `com.tivoli.am.fim.soap.client.jsse.provider` dans la zone **Nom**. N'insérez pas d'espace dans cette zone.
7. Tapez `JSSE2` dans la zone **Valeur**.
8. Sélectionnez la propriété suivante de la marque de réservation.
9. Tapez `com.tivoli.am.fim.soap.client.trust.provider` dans la zone **Nom**.
10. Tapez `IbmPKIX` dans la zone **Valeur**.
11. Cliquez sur **OK** pour appliquer les modifications effectuées et quitter le panneau.

Chapitre 7. Configuration de la sécurité du transport

Pour permettre la protection du message lors de sa communication (ou de son transport) entre les partenaires, SAML recommande d'utiliser une connexion SSL (Secure Sockets Layer) avec authentification sur le serveur et, dans certains cas, une authentification réciproque.

Pourquoi et quand exécuter cette tâche

Vous pouvez assurer la sécurité d'un environnement Tivoli Federated Identity Manager en activant le protocole SSL sur l'instance de WebSphere Application Server sur laquelle le composant d'exécution et du service de gestion est installé. En outre, si vous avez le rôle de client dans une communication SSL où l'authentification réciproque repose sur un certificat client, vous devez également configurer ce certificat.

La procédure générale permettant d'activer l'authentification côté client et côté serveur comprend les tâches suivantes :

Procédure

1. «Activation de SSL sur WebSphere Application Server», à la page 52.

Remarque : Si vous tenez le rôle de fournisseur de services dans une fédération SAML 1.x, vous serez toujours le *client* dans une configuration SSL. Il n'est donc pas nécessaire de configurer le protocole *SSL serveur*. Reportez-vous à la procédure de configuration des certificats client dans «Configuration des certificats client», à la page 61.

   L'activation SSL sur un serveur comprend les tâches annexes suivantes :
   a. «Création d'une demande de certificat», à la page 52.
   b. «Réception d'un certificat signé émis par une autorité de certification», à la page 53.
   c. «Association d'un certificat à la configuration SSL», à la page 54.
   d. Vous pouvez, en option, effectuer les étapes de la section «Suppression du certificat par défaut», à la page 55.
   e. «Extraction d'un certificat à partager avec votre partenaire», à la page 56.
2. «Configuration des exigences relatives à l'authentification client», à la page 56. Les options liées aux exigences d'authentification sont les suivantes :
   - Aucune authentification
   - Authentification de base, au cours de laquelle un nom d'utilisateur et un mot de passe sont demandés
   - Authentification par certificat client
3. Si vous tenez le rôle de client dans la fédération et que votre partenaire exige votre authentification à l'aide d'un certificat client, vous devez également accomplir les étapes de la rubrique «Configuration des certificats client», à la page 61.

Activation de SSL sur WebSphere Application Server

Pour vous assurer que les messages sont sécurisés lorsqu'ils sont communiqués entre les partenaires de la fédération, vous pouvez être amené à activer SSL sur l'instance de WebSphere Application Server sur laquelle le composant d'exécution et du service de gestion est installé.

Avant de commencer

Remarque : Si vous tenez le rôle de fournisseur de services dans une fédération SAML 1.x, vous serez toujours le client dans une configuration SSL. Il ne vous est donc pas nécessaire de configurer le protocole SSL sur votre serveur. Reportez-vous à la procédure de configuration des certificats client dans «Configuration des certificats client», à la page 61.

Création d'une demande de certificat

Pour assurer une communication SSL, les serveurs exigent un certificat personnel (également appelé certificat serveur) signé par une autorité de certification (CA). Vous devez au préalable créer une demande de certificat personnel pour obtenir un certificat signé par une CA.

Avant de commencer

Il doit exister un fichier de clés, qui contient la demande de certificat et qui contiendra, par la suite, le certificat. Vous pouvez utiliser le fichier de clés par défaut de WebSphere Application Server, NodeDefaultKeyStore, ou en créer un. Pour des instructions de création d'un fichier de clés, voir le centre de documentation de WebSphere Application Server 6.1 à l'adresse http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp

Pourquoi et quand exécuter cette tâche

Exécutez les tâches ci-dessous sur la console. Pour plus d'informations, voir la rubrique du centre de documentation de WebSphere relative à la création d'une demande de certificat.

Procédure

1. Connectez-vous à la console.
2. Cliquez sur **Sécurité → Certificat SSL et gestion des clés**.
3. Sous **Articles liés** à droite, cliquez sur **Magasins de clés et certificats**, puis sur le nom du fichier de clés dans lequel le certificat sera enregistré, par exemple **NodeDefaultKeyStore**.
4. Cliquez sur **Demandes de certificats personnels (Personal certificate requests)** sous Propriétés supplémentaires (Additional Properties).
5. Cliquez sur **Nouveau**.
6. Dans la zone **Fichier de demande de certificat (File for certificate request)**, entrez le chemin d'accès complet de l'emplacement d'enregistrement de la demande de certificat ainsi que le nom du fichier. Une extension .arm sera associée au fichier. Exemple : `c:\servercertreq.arm` (sur un serveur Windows).
7. Entrez un alias pour le certificat dans la zone **Intitulé de clé**. L'alias est le nom que vous donnez à votre demande de certificat afin de l'identifier dans le magasin de clés.

8. Entrez une valeur de nom usuel. Celui-ci est le nom de l'entité que le certificat représente. Le nom usuel correspond souvent au nom d'hôte DNS dans lequel réside le serveur.
9. Dans la zone **Unité organisationnelle**, entrez la partie du nom distinctif relative à l'unité organisationnelle.
10. Dans la zone **Localité**, entrez la partie du nom distinctif relative à la localité.
11. Dans la zone **Etat ou province**, entrez la partie du nom distinctif relative à l'Etat.
12. Dans la zone **Code postal**, entrez la partie du nom distinctif relative au code postal.
13. Dans la liste **Pays ou région**, sélectionnez la partie du nom distinctif correspondant aux deux lettres du code pays.
14. Cliquez sur **Appliquer**, puis sur **Enregistrer**. La demande de certificat est créée à l'adresse de fichier spécifiée dans le fichier de clés. Elle fonctionne comme une marque de réservation temporaire du certificat signé jusqu'à ce que vous receviez manuellement le certificat dans le fichier de clés.

    Avertissement : Les outils du fichier de clés (notamment iKeyman et keyTool) ne peuvent pas recevoir les certificats signés générés par les demandes de certificat issues de WebSphere Application Server. De même, WebSphere Application Server n'accepte pas les certificats générés par les demandes de certificat issues d'autres utilitaires de fichiers de clés.
15. Envoyez le fichier .arm de la demande de certificat à une autorité de certification pour qu'elle la signe. Chaque autorité de certification a adopté une méthode privilégiée pour la réception des demandes. Utilisez celle qui est recommandée par l'autorité de certification à laquelle vous envoyez votre demande.
16. Gardez une copie de sauvegarde de votre fichier de clés jusqu'à réception du certificat demandé. Vous pouvez rechercher votre fichier de clés à l'aide du chemin d'accès figurant sur la console. Copiez-le dans un autre emplacement en guise de sauvegarde.

Que faire ensuite

Pour terminer la procédure d'obtention d'un certificat signé pour votre serveur, recevez le certificat de la CA, comme indiqué dans «Réception d'un certificat signé émis par une autorité de certification».

Réception d'un certificat signé émis par une autorité de certification

Lorsqu'une autorité de certification (CA) reçoit une demande, elle émet un nouveau certificat sous forme de marque de réservation temporaire d'un certificat émis par la CA. Le nouveau certificat est reçu dans un fichier de clés qui génère le certificat personnel signé par la CA, que WebSphere Application Server peut utiliser pour la sécurité SSL.

Avant de commencer

La demande de certificat doit être déjà créée et figurer dans un fichier de clés de WebSphere comme indiqué dans «Création d'une demande de certificat», à la page 52. De même, le certificat doit provenir de la CA et être placé sur votre ordinateur pour vous permettre de le recevoir dans le fichier de clés.

WebSphere Application Server ne peut recevoir que les certificats générés par une demande de certificat de WebSphere Application Server. Il ne peut pas recevoir les certificats demandés à l'aide d'autres outils du fichiers de clés, comme iKeyman ou keyTool.

Pourquoi et quand exécuter cette tâche

Exécutez les tâches ci-dessous sur la console. Pour plus d'informations, voir la rubrique du centre de documentation de WebSphere, http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp, relative à la réception d'un certificat émis par une autorité de certification.

Procédure

1. Connectez-vous à la console.
2. Cliquez sur **Sécurité → Certificat SSL et gestion des clés → Gérer les configurations de sécurité du noeud final**.
3. Cliquez sur le nom de votre noeud dans l'arborescence **Entrant**.
4. Cliquez sur le bouton **Gérer les certificats**.
5. Cliquez sur **Recevoir un certificat émis pas une autorité de certification**.
6. Entrez le chemin d'accès complet et le nom du fichier du certificat que vous avez reçu de l'autorité de certification.
7. Sélectionnez le type de données par défaut dans la liste.
8. Cliquez sur **Valider**, puis sur **Enregistrer**. Le fichier de clés contient un nouveau certificat personnel émis par une CA. La configuration SSL peut désormais utiliser le nouveau certificat personnel signé par la CA.

Que faire ensuite

Pour terminer, vous devez associer le certificat à votre configuration SSL. Voir «Association d'un certificat à la configuration SSL».

Association d'un certificat à la configuration SSL

Après avoir ajouté un certificat signé à votre fichier de clés, vous devez lui associer les paramètres de configuration SSL de votre serveur.

Pourquoi et quand exécuter cette tâche

Lorsque vous installez WebSphere Application Server 6.1 et Tivoli Federation Identity Manager, deux configurations SSL sont créées sur WebSphere Application Server :

- NodeDefaultSSLSettings
- FIMSOAPEndpointSSLSettings

NodeDefaultSSLSettings est le paramètre de configuration SSL par défaut défini par WebSphere Application Server. Il est destiné à la stratégie SSL de votre serveur WebSphere. La configuration FIMSOAPEndpointSSLSettings est ajoutée par Tivoli Federated Identity Manager pour vous permettre d'avoir une stratégie SSL distincte, spécialement dédiée à la communication des messages SOAP avec votre partenaire de fédération.

Après l'installation, les deux configurations utilisent le certificat à signature automatique `par défaut` présent dans NodeDefaultKeystore.

Lorsque vous demandez et recevez un certificat personnel signé, les paramètres des deux configurations SSL sont définis sur aucun.

Vous devez spécifier manuellement le certificat personnel à utiliser dans chaque configuration SSL. Vous pouvez utiliser le même certificat pour les deux configurations. Si vous souhaitez utiliser un certificat différent, suivez les instructions relatives à la «Création d'une demande de certificat», à la page 52 et à la «Réception d'un certificat signé émis par une autorité de certification», à la page 53 pour créer et recevoir un certificat signé supplémentaire, puis répétez ces instructions.

Procédure

1. Connectez-vous à la console.
2. Cliquez sur **Sécurité → Certificat SSL et gestion des clés**.
3. Sous **Articles liés**, sur la droite, cliquez sur **Configurations SSL**.
4. Cliquez sur le nom de la configuration SSL à utiliser. Par exemple, cliquez sur **NodeDefaultSSLSettings**.
5. Vérifiez que le fichier de clés dans lequel votre certificat est enregistré apparaît dans la zone **Nom de fichier de clés**.
6. Cliquez sur le bouton **Extraire les alias de certificat (Get certificate aliases)** pour vérifier que tous les alias de certificat de votre fichier de clés sont affichés.
7. Dans la zone **Alias de certificat serveur par défaut (Default server certificate alias)**, sélectionnez votre certificat signé.
8. Cliquez sur **Appliquer**, puis sur **Enregistrer** lorsque vous êtes invité à enregistrer la configuration SSL dans la configuration principale. La configuration SSL utilise désormais le nouveau certificat.

Que faire ensuite

Répétez la procédure pour associer l'autre configuration SSL au certificat approprié. Poursuivez ensuite avec les instructions de suppression du certificat par défaut, indiquées à la rubrique «Suppression du certificat par défaut», afin d'empêcher tout risque d'utilisation par inadvertance.

Suppression du certificat par défaut

Une fois que vous avez reçu votre certificat personnel signé, supprimez la clé par défaut, afin d'empêcher toute utilisation de celle-ci par inadvertance.

Pourquoi et quand exécuter cette tâche

Avertissement : Avant d'accomplir cette procédure, assurez-vous qu'aucune configuration SSL n'utilise la clé par défaut. Reportez-vous aux instructions de la section «Association d'un certificat à la configuration SSL», à la page 54.

Procédure

1. Cliquez sur **Sécurité → Certificat SSL et gestion des clés**.
2. Sous l'option **Articles liés**, cliquez sur**Magasins de clés et certificats**.
3. Cliquez sur **NodeDefaultKeyStore**.
4. Sous Propriétés supplémentaires, cliquez sur **Certificats personnels**.
5. Cochez la case en regard du certificat **default**.
6. Cliquez sur le bouton **Supprimer**.
7. Cliquez sur **Appliquer**, puis sur **Enregistrer**.

Que faire ensuite

Poursuivez avec les instructions de la rubrique «Extraction d'un certificat à partager avec votre partenaire» pour pouvoir transmettre les données à votre partenaire.

Extraction d'un certificat à partager avec votre partenaire

Après avoir ajouté un certificat de CA signé à votre serveur, vous devez exporter une copie de ce certificat de CA accompagnée de sa clé publique et la fournir à votre partenaire.

Avant de commencer

Il doit exister un fichier de clés et un certificat personnel.

Procédure

1. Cliquez sur **Sécurité → Certificat SSL et gestion des clés → Gérer les configurations de sécurité du noeud final**.
2. Sélectionnez votre noeud dans l'arborescence **Sortant**.
3. Cliquez sur **Gérer les certificats**.
4. Sélectionnez le certificat de CA signé, puis cliquez sur **Extraire** dans l'angle supérieur droit.
5. Entrez le chemin d'accès complet de l'emplacement d'extraction du certificat. Incluez le nom de fichier du certificat dans le chemin d'accès. Le certificat de signataire est enregistré dans ce fichier. Sous Windows, par exemple, vous pouvez spécifier : `c:\certificates\local_cert.arm`
6. Sélectionnez le type de données par défaut dans la liste.
7. Cliquez sur **Appliquer**, puis sur **Enregistrer**. La partie du certificat personnel relative au signataire est stockée dans le fichier .arm spécifié.

Que faire ensuite

Désormais, vous pouvez fournir le fichier à votre partenaire afin qu'il ajoute votre certificat à son fichier de clés certifiées.

Remarque : Si votre partenaire utilise Tivoli Federated Identity Manager, il doit importer le certificat dans son fichier de clés certifiées Tivoli Federated Identity Manager.

Pour achever la configuration SSL, exécutez les étapes de la rubrique «Configuration des exigences relatives à l'authentification client».

Configuration des exigences relatives à l'authentification client

Parmi les options de sécurisation des messages, vous pouvez exiger de votre partenaire qu'il s'authentifie sur votre serveur point de contact.

Pourquoi et quand exécuter cette tâche

Remarque : Dans une fédération SAML 1.x, seul le fournisseur d'identité agit en tant que serveur. Toutefois, seul le partenaire du fournisseur d'identité est tenu de configurer un paramètre d'authentification client.

Vous devez d'abord décider si vous allez demander l'authentification client.

- Si vous ne demandez pas l'authentification client, reportez-vous à la section «Configuration de l'accès sans aucune authentification».
- Si vous demandez l'authentification client, vous disposez des deux options suivantes :
  - Authentification de base. Voir «Configuration de l'accès à l'authentification de base».
  - Authentification par certificat client. Voir «Configuration de l'accès via l'authentification par certificat client», à la page 59.

Configuration de l'accès sans aucune authentification

Si vous ne demandez pas l'authentification client à votre partenaire, configurez les paramètres d'authentification SOAP de façon appropriée.

Pourquoi et quand exécuter cette tâche

Par défaut, après l'installation, les paramètres de sécurité de noeud final ont pour valeur **Autoriser les utilisateurs non authentifiés à accéder aux noeuds finals SOAP**.

Remarque : Ces instructions s'appliquent aux serveurs WebSphere autonomes. Pour les serveurs WebSphere Network Deployment inclus dans un cluster, voir «Configuration du serveur IHS pour l'authentification client», à la page 73.

Pour vous assurer que ce paramètre est sélectionné :

Procédure

1. Connectez-vous à la console. Cliquez sur **Tivoli Federated Identity Manager → Gestion des domaines → Point de contact**.
2. Sélectionnez le serveur point de contact utilisé dans votre environnement.
3. Cliquez sur le bouton **Avancé**. Le panneau Paramètres de sécurité de noeud final SOAP s'affiche.
4. Assurez-vous que le port SOAP est correct dans votre configuration et que l'option **Autoriser les utilisateurs non authentifiés à accéder aux noeuds finaux SOAP** est sélectionnée.
5. Cliquez sur **OK**.
6. Cliquez sur le bouton **Charger les modifications de configuration dans l'environnement d'exécution de Tivoli Federated Identity Manager**.

Que faire ensuite

Si vous configurez une fédération SAML 2.0, poursuivez avec les étapes permettant de configurer votre certificat client à la rubrique «Configuration des certificats client», à la page 61. Si vous configurez une fédération SAML 1.x, la procédure est terminée.

Configuration de l'accès à l'authentification de base

Si vous demandez l'authentification de base à votre partenaire, vous devez créer, dans votre registre d'utilisateurs, un utilisateur représentant votre fournisseur de services partenaire.

Avant de commencer

Avant de démarrer cette tâche, procédez comme suit :

- Choisissez si vous allez autoriser des utilisateurs authentifiés individuels ou par des utilisateurs authentifiés faisant partie de groupes spécifiques à accéder au noeud final.
- Veillez à connaître le nom d'utilisateur et le mot de passe à utiliser par votre fournisseur de services.

Pourquoi et quand exécuter cette tâche

Pour configurer l'authentification de base, effectuez les étapes ci-dessous.

Procédure

1. Dans votre registre d'utilisateurs, créez un utilisateur dont le nom évoque votre partenaire de fournisseur de service. Par exemple, créez un utilisateur dont le nom est `soapclient`.

   Remarque : Voir les instructions de création d'utilisateurs du registre d'utilisateurs que vous avez configuré pour votre environnement.
2. L'étape suivante varie selon si vous allez autoriser des utilisateurs authentifiés individuels ou des utilisateurs authentifiés faisant partie de groupes spécifiques.
   - Si vous demandez l'authentification de base à des utilisateurs individuels, répétez l'étape 1 pour chaque utilisateur de fournisseur de services à configurer. Allez ensuite à l'étape 3.
   - Si vous demandez l'authentification de base à des utilisateurs faisant partie de groupes spécifiques, créez un groupe pour les utilisateurs, puis ajoutez, dans ce groupe, l'utilisateur que vous avez créé à l'étape 1. Par exemple, créez un groupe intitulé `soapgroup`, puis ajoutez l'utilisateur `soapclient` dans ce groupe.

     Remarque : Voir les instructions de création de groupes pour le registre d'utilisateurs que vous avez configuré pour votre environnement.
3. Configurez les paramètres d'authentification SOAP de la console de Tivoli Federated Identity Manager :

   Remarque : Ces instructions s'appliquent aux serveurs WebSphere autonomes. Pour les serveurs WebSphere Network Deployment inclus dans un cluster, voir «Configuration du serveur IHS pour l'authentification client», à la page 73.
   a. Connectez-vous à la console. Cliquez sur **Tivoli Federated Identity Manager → Gestion de la configuration → Point de contact**.
   b. Sélectionnez le serveur point de contact utilisé dans votre environnement.
   c. Cliquez sur le bouton **Avancé**. Le panneau Paramètres de sécurité de noeud final SOAP s'affiche.
   d. Vérifiez que vous avez correctement configuré le port SOAP, puis sélectionnez l'option correspondant à votre configuration :
      - Pour exiger l'authentification des utilisateurs individuels, sélectionnez **Autoriser les utilisateurs authentifiés à accéder aux noeuds finaux SOAP**.

- Pour exiger l'authentification des utilisateurs faisant partie de groupes spécifiques, sélectionnez, **Autoriser les utilisateurs du groupe spécifié à accéder aux noeuds finaux SOAP**, puis indiquez le nom du groupe dans la zone **Nom de groupe**.

e. Sélectionnez **Authentification de base**.

f. Cliquez sur **OK**.

g. Cliquez sur le bouton **Charger les modifications de configuration dans l'environnement d'exécution de Tivoli Federated Identity Manager**.

Que faire ensuite

Si vous configurez une fédération SAML 2.0, poursuivez avec les étapes permettant de configurer votre certificat client à la rubrique «Configuration des certificats client», à la page 61.

Si vous configurez une fédération SAML 1.x, la procédure est terminée.

Configuration de l'accès via l'authentification par certificat client

Si vous demandez l'authentification par certificat client à votre partenaire, vous devez procéder comme suit :

Avant de commencer

1. Configurez la reconnaissance du certificat client par WebSphere Application Server.
2. Créez un utilisateur et éventuellement un groupe représentant le fournisseur de services partenaire.
3. Configurez la demande d'authentification sur Tivoli Federated Identity Manager.

Avant de démarrer cette tâche, procédez comme suit :

- Vérifiez que vous possédez le certificat de clé publique du certificat client que votre partenaire utilisera pour accéder à votre noeud final de résolution d'artefacts.
- Vérifiez que vous disposez de l'attribut de nom usuel du certificat client qui permet à votre partenaire d'accéder à votre noeud final. Par exemple, si le nom distinctif (DN) du certificat est "/C=US/ST=TX/L=AUSTIN/O=SERVICEPROVIDER/CN=soapclient", alors le nom usuel (CN) est "soapclient".
- Indiquez si vous souhaitez autoriser les utilisateurs authentifiés individuels ou les utilisateurs authentifiés faisant partie de groupes spécifiques à accéder au noeud final.

Pourquoi et quand exécuter cette tâche

Pour configurer l'authentification par certificat client, effectuez les étapes ci-dessous.

Procédure

1. Copiez le certificat de clé publique que votre partenaire doit présenter pour s'authentifier à votre serveur WebSphere Application Server.

Remarque : Dans ces instructions, le certificat du partenaire est nommé `partnerca.pem`, et le répertoire dans lequel il a été copié `/tmp`.

2. Connectez-vous à la console.
3. Sélectionnez **Sécurité** → **Certificat SSL et gestion des clés**.
4. Sélectionnez **Magasins de clés et certificats**.
5. Sélectionnez **NodeDefaultTrustStore**.
6. Sélectionnez **Certificats de signataires**.
7. Sélectionnez **Ajouter**.
8. Entrez dans les zones les informations pertinentes relatives au certificat. Par exemple :
   - Alias : `CACert`
   - Nom de fichier : `/tmp/partnerca.pem`
   - Type de données : `codées Base64`
9. Cliquez sur **OK**.
10. WebSphere doit pouvoir mapper le certificat client présenté par votre partenaire à une identité utilisateur de votre registre d'utilisateurs à l'aide de l'attribut de nom usuel du certificat. Pour afficher cet attribut, cliquez sur le certificat dans la console, puis recherchez la zone **Emis pour**.
    a. Dans votre registre d'utilisateurs, créez un utilisateur dont le nom évoque votre partenaire de fournisseur de service. Par exemple, créez un utilisateur dont le nom est `soapclient`.

       Remarque : Voir les instructions de création d'utilisateurs du registre d'utilisateurs que vous avez configuré pour votre environnement.

    b. La suite de la procédure dépend des utilisateurs autorisés à accéder au noeud final (utilisateurs authentifiés individuels ou utilisateurs authentifiés faisant partie de groupes spécifiques).
       - Si vous demandez l'authentification par certificat client à des utilisateurs individuels, répétez l'étape 10a pour chaque utilisateur de fournisseur de services à configurer. Allez ensuite à l'étape 11.
       - Si vous demandez l'authentification par certificat client à des utilisateurs faisant partie de groupes spécifiques, créez un groupe pour les utilisateurs, puis ajoutez, dans ce groupe, l'utilisateur que vous avez créé à l'étape 10a. Par exemple, créez un groupe dont le nom est `soapgroup`, puis ajoutez-y l'utilisateur `soapclient`.

         Remarque : Voir les instructions de création de groupes pour le registre d'utilisateurs que vous avez configuré pour votre environnement. Allez ensuite à l'étape 11.
11. Configurez les paramètres d'authentification SOAP de la console de Tivoli Federated Identity Manager :

    Remarque : Ces instructions s'appliquent aux serveurs WebSphere autonomes. Pour les serveurs WebSphere Network Deployment inclus dans un cluster, voir «Configuration du serveur IHS pour l'authentification client», à la page 73.

    a. Connectez-vous à la console. Cliquez sur **Tivoli Federated Identity Manager** → **Gestion de la configuration** → **Point de contact**.
    b. Sélectionnez le serveur point de contact utilisé dans votre environnement.
    c. Cliquez sur le bouton **Avancé**. Le panneau Paramètres de sécurité de noeud final SOAP s'affiche.

d. Vérifiez que vous avez correctement configuré le port SOAP, puis sélectionnez l'option correspondant à votre configuration :
   - Pour exiger l'authentification des utilisateurs individuels, sélectionnez **Autoriser les utilisateurs authentifiés à accéder aux noeuds finaux SOAP**.
   - Pour exiger l'authentification des utilisateurs faisant partie de groupes spécifiques, sélectionnez, **Autoriser les utilisateurs du groupe spécifié à accéder aux noeuds finaux SOAP**, puis indiquez le nom du groupe dans la zone **Nom de groupe**.

e. Sélectionnez **Authentification par certificat client**.

f. Cliquez sur **OK**.

g. Cliquez sur le bouton **Charger les modifications de configuration dans l'environnement d'exécution de Tivoli Federated Identity Manager**.

Que faire ensuite

Si vous configurez une fédération SAML 2.0, poursuivez avec les étapes permettant de configurer votre certificat client à la rubrique «Configuration des certificats client». Si vous configurez une fédération SAML 1.x, la procédure est terminée.

Configuration des certificats client

Si l'authentification par certification client est également requise par votre partenaire, vous devez créer et importer le certificat que vous présenterez lors de l'authentification, et exporter également le certificat pour votre partenaire.

Réception certificat serveur de votre partenaire

Si l'authentification serveur est configurée chez votre partenaire, vous devez disposer de la clé publique de ce certificat serveur, que vous stockerez dans un fichier de clés certifiées utilisé par votre service de clés Tivoli Federated Identity Manager.

Avant de commencer

Avant de poursuivre cette procédure, vérifiez qu'un fichier de clés certifiées est disponible pour stocker le certificat. Voir «Préparation des fichiers de clés», à la page 29.

Procédure

1. Connectez-vous à la console.
2. Cliquez sur **Tivoli Federated Identity Manager → Service de clés**.
   Le panneau Fichiers de clés s'affiche.
3. Sélectionnez le fichier de clés certifiées dans lequel vous voulez stocker le certificat dans le tableau des fichiers de clés. Le bouton **Afficher les clés** s'active.
4. Cliquez sur **Extraire le certificat de SSL**. Le panneau Mot de passe s'affiche.
5. Entrez le mot de passe du fichier de clés certifiées, puis cliquez sur **OK**.
6. Remplissez les zones prévues pour le nom d'hôte et le nom de port à partir desquels vous devez récupérer le certificat. Vous pouvez également cliquer sur **Afficher les informations sur le signataire** pour visualiser le certificat avant de le récupérer.

7. Entrez dans la zone **Alias** le nom à attribuer au certificat. Cliquez ensuite sur **OK**. Le certificat est ajouté au fichier de clés certifiées.

Que faire ensuite

Si vous avez le rôle de client dans une connexion SSL et que votre partenaire exige votre authentification à l'aide d'un certificat client, passez à l'étape «Obtention de votre certificat client».

Obtention de votre certificat client

Si vous avez le rôle de client dans une connexion SSL et que votre partenaire exige votre authentification à l'aide d'un certificat client, vous devez obtenir et configurer le certificat et le partager avec lui.

Avant de commencer

Avant de poursuivre cette procédure, vérifiez qu'un fichier de clés est disponible pour stocker le certificat. Voir «Préparation des fichiers de clés», à la page 29.

Procédure

1. Demandez un certificat de paire de clés publique/privée auprès d'une autorité de certification (CA). Pour ce faire :
   a. Connectez-vous à la console.
   b. Cliquez sur **Tivoli Federated Identity Manager → Service de clés**.
      Le panneau Fichiers de clés s'affiche.
   c. Sélectionnez un fichier de clés dans le tableau Fichier de clés. Le bouton **Afficher les clés** s'active.
   d. Cliquez sur **Afficher les clés**. Le panneau Mot de passe s'affiche.
   e. Entrez le mot de passe du fichier de clés, puis cliquez sur **OK**.
   f. Cliquez sur **Demande de certificat**. Le panneau Créer une demande de certificat s'affiche.
   g. Remplissez les zones du panneau. Ensuite, cliquez sur **OK**. Une paire de clés publique/privée est ajoutée au fichier de clés et un fichier contenant les données BASE64 codées est créé. Le certificat d'auto-signature temporaire doit être remplacé par le certificat signé par la CA.

   Revenez à ces instructions lorsque la CA vous aura notifié que votre certificat signé est prêt.
2. Recevez le certificat signé émis par la CA. Pour ce faire :
   a. Connectez-vous à la console.
   b. Cliquez sur **Tivoli Federated Identity Manager → Service de clés**.
      Le panneau Fichiers de clés s'affiche.
   c. Sélectionnez le fichier dans lequel la RSC a été générée dans le tableau Fichiers de clés. Le bouton **Afficher les clés** est activé.
   d. Cliquez sur **Afficher les clés**. Le panneau Mot de passe s'affiche.
   e. Entrez le mot de passe du fichier de clés, puis cliquez sur **OK**.
   f. Cliquez sur **Réception de certificat de CA**.
   g. Sélectionnez l'emplacement du certificat que vous avez reçu de la CA. Ensuite, cliquez sur **OK**. Le certificat d'auto-signature temporaire présent dans le fichier de clés est remplacé par le certificat signé que vous avez reçu.

3. Fournissez la clé publique de ce certificat à votre partenaire. Pour ce faire :
   a. Connectez-vous à la console.
   b. Cliquez sur **Tivoli Federated Identity Manager → Service de clés**.

      Le panneau Fichiers de clés s'affiche.
   c. Sélectionnez le fichier de clés approprié dans le tableau Fichier de clés. Vous êtes invité à entrer le mot de passe du fichier de clés.
   d. Entrez le mot de passe du fichier de clés et cliquez sur **OK**. Le bouton **Afficher les clés** s'active.
   e. Cliquez sur **Afficher les clés**. Le panneau Clés s'affiche. Il répertorie les éléments du fichier de clés sélectionné.
   f. Sélectionnez les clés à exporter, puis cliquez sur le bouton **Exporter**. Le panneau Exporter la clé s'affiche.
   g. Sélectionnez le format de la clé à exporter.

      (PEM)
      (Privacy-Enhanced Message) Certificat public

      PKCS#12
      Public Key Cryptography Standard 12 : norme d'échange d'informations personnelles
   h. Vérifiez que la case **Inclure une clé privée** *n'est pas* cochée. Vous devez être la seule personne à détenir votre clé privée.
   i. Cliquez sur **Télécharger la clé**.
   j. Lorsque vous y êtes invité, entrez le nom de fichier de la clé exportée.

      Par exemple : `maclépublique.pem`

      Vous pouvez également cliquer sur **Parcourir** pour localiser le fichier sur le système de fichiers.
   k. Cliquez sur **Annuler** pour quitter.

Que faire ensuite

Fournissez le certificat à votre partenaire. Ce dernier doit vérifier ce qui suit :

- Il a, dans son fichier de clés certifiées, le certificat de CA de l'autorité de certification qui a émis votre certificat.
- Son serveur peut accéder à la liste de révocation de certificat de la CA.

Chapitre 8. Sélection d'un serveur point de contact

Tivoli Federated Identity Manager n'est pas directement impliqué dans l'authentification d'utilisateurs ni dans la création d'une session d'application. Au lieu de cela, Tivoli Federated Identity Manager s'appuie sur un *serveur point de contact*.

Le serveur point de contact est un proxy ou une application qui interagit avec un utilisateur et gère à la fois l'authentification et les sessions. Dans un déploiement classique, le point de contact est situé au bord d'un réseau protégé et devant un pare-feu, comme dans une zone démilitarisée, par exemple.

Le serveur point de contact fournir des noeuds finals qui correspondent aux emplacements vers lesquels et à partir desquels les messages sont envoyés et reçus. Chaque noeud final possède une adresse URL, de sorte que les noeuds finals puissent être accessibles aux utilisateurs externes sous forme de sites Web sur Internet. Le point de contact reçoit les requêtes d'accès et fournit le service d'authentification. Il représente le premier composant capable d'évaluer les données d'identification de l'utilisateur demandant l'accès au réseau protégé. En outre, il gère le cycle de vie des sessions utilisateur, depuis leur création jusqu'à l'accès et à leur suppression (par exemple, en réponse aux services de fermeture de session).

Le choix du type de serveur point de contact à utiliser est déterminé par les besoins en termes d'architecture de sécurité et de topologie réseau. Tivoli Federated Identity Manager prend en charge les quatre options suivantes pour le serveur point de contact :

- IBM WebSphere Application Server
- Tivoli Access Manager WebSEAL
- WebSEAL, aucun ACLD
- Serveur point de contact générique
- Serveur point de contact personnalisé

WebSphere en tant que serveur point de contact

Si vous prévoyez d'utiliser IBM WebSphere Application Server, vos options de configuration varient selon que vous êtes partenaire du fournisseur d'identité ou du fournisseur de services.

Options de fournisseur d'identité

Lorsqu'IBM WebSphere Application Server est utilisé en tant que serveur point de contact et que vous êtes le fournisseur d'identité dans une fédération, vous disposez des options suivantes en ce qui concerne le type d'authentification à utiliser :

- Authentification par formulaires, utilisant n'importe quel registre d'utilisateurs pris en charge
- Mécanisme SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism) utilisant l'authentification TAI (Trust Association Interceptor) et le registre d'utilisateurs Microsoft Active Directory

Options de fournisseur de services

Lorsqu'IBM WebSphere Application Server est utilisé en tant que serveur point de contact et que vous êtes le fournisseur de services dans une fédération, la connexion unique est soumise à l'authentification STPA (Lightweight Third-Party Authentication). Vous disposez des options suivantes lors de l'hébergement d'applications destinées à être utilisées dans fédération qui est configuré dans Tivoli Federated Identity Manager :

- IBM WebSphere Application Server, soit sur le même serveur que celui sur lequel Tivoli Federated Identity Manager est installé, soit sur un un serveur séparé exécutant WebSphere Application Server version 5.1 ou 6.x.
- Microsoft Internet Information Services version 6.0 avec plug-in du serveur Web Tivoli Federated Identity Manager installé
- IBM HTTP Server 6.1 avec plug-in du serveur Web Tivoli Federated Identity Manager installé
- Serveur Apache HTTP 2.0 ou 2.2 avec plug-in du serveur Web Tivoli Federated Identity Manager installé

Chacune de ces options est soumise à des exigences spécifiques. Pour plus d'informations sur ces configurations, voir «WebSphere en tant que point de contact pour les fournisseurs d'identité», à la page 74, et «Serveur point de contact WebSphere pour un fournisseur de services», à la page 91.

WebSEAL en tant que serveur point de contact

Pour répondre aux exigences fonctionnelles d'un serveur point de contact, Tivoli Federated Identity Manager peut tire parti des fonctions d'authentification et d'autorisation étendues de Tivoli Access Manager. Dans les environnements exploitant Tivoli Access Manager, un serveur WebSEAL fait généralement office de point de contact.

WebSEAL est généralement utilisé comme proxy inverse permettant de contrôler l'accès à des ressources protégées extensives via l'établissement et la gestion de jonctions WebSEAL. WebSEAL reçoit les requêtes d'accès et représente le premier composant capable d'évaluer les données d'identification de l'utilisateur demandant l'accès au réseau protégé. Il doit en outre gérer les sessions Web pour les utilisateurs.

L'assistant de création de fédération nécessite la spécification d'une URL pour les serveurs point de contact. L'assistant affiche une zone dans laquelle vous devez entrer l'URL donnant accès aux noeuds finals sur le serveur point de contact. L'URL doit contenir les éléments suivants :

- Un protocole de communication. Le protocole HTTPS ou HTTP être utilisé pour les communications entre le serveur point de contact et l'utilisateur. L'utilisation de HTTPS est recommandée pour une sécurité optimale.

  Il est à noter que cette valeur doit correspondre à la façon dont vous avez configuré votre serveur point de contact (WebSEAL).

  Par exemple :

  ```
  https://
  ```

- L'adresse de domaine du serveur WebSEAL :

  Par exemple :

  ```
  idp.exemple.com
  ```

- Lors de l'utilisation de WebSEAL, l'élément suivant est le nom de la jonction WebSEAL par laquelle passent les requêtes de services de connexion unique. N'importe quelle valeur est admise, mais elle doit correspondre au nom d'une jonction sur le serveur WebSEAL.

  Par exemple :

  `/FIM`
- Le dernier élément est la chaîne `/sps`. L'élément /sps de l'URL est défini par Tivoli Federated Identity Manager et désigne un contexte WebSphere destiné aux services de connexion unique. La valeur de cette chaîne n'est pas modifiable.

Ces éléments sont combinés pour former une adresse URL. Par exemple :

`https://idp.exemple.com/FIM/sps`

Ultérieurement, lors de la configuration de fédération, l'URL est étendue lorsque vous sélectionnez un protocole de connexion unique (SAML, WS-Federation ou Liberty) et affectez des noeuds finals spécifiques pour des profils, par exemple pour la connexion et la déconnexion. Par conséquent, elle fait désormais partie de plusieurs chemins d'URL plus longs (noeuds finals) gérés comme objets Tivoli Access Manager protégés.

WebSEAL No ACLD en tant que serveur point de contact

Les déploiements Tivoli Access Manager incluent souvent un serveur de règles (pdmgrd) et un serveur d'autorisation (acld). Tivoli Access Manager requiert un serveur de règles déployé, mais ne requiert pas de serveur d'autorisation actif. Tivoli Federated Identity Manager requiert également un serveur de règles déployé uniquement. Le serveur point de contact WebSEAL ne dépend pas du serveur d'autorisation pour les services d'autorisation ou d'authentification.

Par défaut, l'instance de module IVCred par défaut du produit contacte le serveur d'autorisation Tivoli Access Manager (également appelé pdacld) pour émettre des données d'identification. Des données d'identification modèles sont alors créées à partir du nom d'utilisateur. Ces données incluent les groupes (et ID utilisateur universels) pour cet utilisateur tel que défini dans le registre utilisateur pour Tivoli Access Manager. Toutefois, lorsque vous sélectionnez WebSEAL No ACLD en point de contact, le produit n'utilise pas le serveur d'autorisation pour créer les données d'identification.

Pour configurer le profil de point de contact " WebSEAL No ACLD" :

1. Connectez-vous à la console.
2. Sélectionnez **Tivoli Federation Identity Manager → Configurer le service d'accréditation → Instances de module**.
3. Sélectionnez **Jeton IVCred par défaut** et cliquez sur **Propriétés**.
4. Décochez **Activer l'émission de droits d'accès Access Manager (IVCred) (nécessite la configuration de PDJRTE)**.
5. Cliquez sur **OK**.

Remarque : Si vous repassez le point de contact sur un serveur WebSEAL avec un serveur d'autorisation, vous devez sélectionner **Activer l'émission de droits d'accès Access Manager (IVCred) (nécessite la configuration de PDJRTE)**.

Serveur point de contact générique

Le serveur point de contact générique est une implémentation de point de contact supplémentaire fournie par Tivoli Federated Identity Manager. Il s'agit d'une solution reposant sur des en-têtes HTTP qui offre aux administrateurs la possibilité de modifier leurs environnements de point de contact (par exemple, Apache) de manière à pouvoir définir et lire les en-têtes. ceci permet l'intégration à Tivoli Federated Identity Manager sans nécessiter la création d'un serveur point de contact personnalisé. Le serveur point de contact générique fonctionne de manière très similaire au point de contact WebSEAL. La principale différence réside dans le fait que les noms des en-têtes sont utilisés pour définir les informations utilisateur.

Le serveur point de contact générique est inclus dans les profils de point de contact fournis avec Tivoli Federated Identity Manager. L'administrateur doit procéder à son activation en le sélectionnant sur la console et en la configurant comme étant active. L'administrateur peut, à l'aide de la console, modifier les noms des en-têtes utilisés par chaque rappel.

Serveur point de contact personnalisé

Un serveur point de contact personnalisé est constitué de plusieurs modules de rappel personnalisés d'ouverture qui définissent les paramètres d'ouverture de session, de fermeture de session, d'ID local et d'authentification. Un serveur point de contact personnalisé peut constituer le choix approprié pour votre environnement si vous souhaitez intégrer une application d'authentification ou de gestion d'accès Web existante à Tivoli Federated Identity Manager. Un serveur point de contact personnalisé peut s'avérer utile dans les situations suivantes :

- Si vous disposez d'un cookie de connexion unique existant, qui est utilisé sur l'ensemble de l'entreprise, vous pouvez mettre en oeuvre un serveur point de contact personnalisé utilisant un rappel SignIn qui définit le cookie du domaine de connexion unique conformément à votre stratégie de connexion unique.
- Si vous disposez d'un logiciel de gestion d'accès Web qui expose une interface API personnalisée en vue de certifier l'identité d'un utilisateur dans l'environnement, ou d'extraire l'utilisateur actuel pour les besoins de la requête. Vous pouvez mettre en oeuvre un serveur point de contact qui exécute un un rappel d'identité local (afin d'extraire l'utilisateur lié à la transaction), ou mettre en oeuvre un serveur point de contact personnalisé utilisant un rappel SignIn pour certifier l'identité d'un utilisateur dans l'environnement, ou bien mettre en oeuvre un serveur point de contact qui exploite ces deux types de rappel.

La mise au point d'un serveur point de contact personnalisé nécessite une certaine expérience dans la programmation de modules de rappel, ainsi qu'une bonne connaissance des concepts de programmation de Tivoli Federated Identity Manager. Consultez les liens des documents developerWorks dans le centre de documentation à l'adresse http://publib.boulder.ibm.com/infocenter/tiv2help/index.jsp.

Une fois le travail de développement terminé, vous devez procéder à l'intégration de la solution dans votre environnement Tivoli Federated Identity Manager. Pour plus d'informations, reportez-vous au document *IBM Federated Identity Manager - Guide d'administration*.

Chapitre 9. Configuration de WebSphere en tant que serveur point de contact

Tivoli Federated Identity Manager peut être installé soit sur un serveur WebSphere intégré, soit dans un environnement WebSphere existant. Lors de l'installation du serveur intégré et lorsque WebSphere est utilisé en tant que serveur point de contact, le programme d'installation automatise une grande partie de la configuration. Lorsque vous effectuez l'installation dans un environnement WebSphere existant et que vous souhaitez utiliser WebSphere en tant que serveur point de contact, vous devez configurer manuellement les serveurs WebSphere et IHS afin qu'ils répondent aux spécifications de votre déploiement.

Lorsque WebSphere est configuré en tant que serveur point de contact, des services d'authentification sont disponibles. Les services d'authentification sont propres au rôle défini au sein de la fédération (fournisseur d'identité ou fournisseur de services).

Remarque : WebSphere Application Server Version 6.0.2, WebSphere en point de contact n'est pas pris en charge par Tivoli Federated Identity Manager.

Voir aussi :

- «Utilisation d'IBM HTTP Server avec WebSphere configuré en tant que point de contact»
- «WebSphere en tant que point de contact pour les fournisseurs d'identité», à la page 74
- «Serveur point de contact WebSphere pour un fournisseur de services», à la page 91

Utilisation d'IBM HTTP Server avec WebSphere configuré en tant que point de contact

WebSphere Application Server Network Deployment (ND) peut être déployé soit en mode autonome, soit en tant que membre d'un cluster WebSphere. Dans un cas comme dans l'autre, un environnement de déploiement typique comprend une instance IBM HTTP Server (IHS) positionnée entre le serveur WebSphere et des connexions externes, telles que celles qui proviennent d'un pare-feu ou d'une zone démilitarisée (DMZ).

Le déploiement du serveur IHS repose généralement sur la configuration de connexions SSL (Secure Socket Layer) permettant de sécuriser à la fois les connexions externes et les liaisons établies en interne avec les serveurs WebSphere. Le succès du déploiement dans un environnement Tivoli Federated Identity Manager utilisant WebSphere en tant que serveur point de contact nécessite l'activation du protocole SSL sur le serveur IHS.

L'activation de SSL sur IHS nécessite la génération d'une base de données de clés SSL et d'une clé. Vous pouvez générer les clés nécessaires au moyen de l'utilitaire ikeyman. Si vous n'avez pas activé SSL sur le serveur IHS, vous devez accomplir cette tâche avant d'effectuer la configuration de Tivoli Federated Identity Manager.

Pour obtenir les instructions correspondantes, consultez le centre de documentation de votre instance IBM HTTP Server pour WebSphere Application Server : http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp. Consultez les rubriques relatives à la sécurité d'IBM HTTP Server, notamment :

- Maniement de la base de données de clés
- Sécurisation au moyen de communications SSL

Ajout d'un port SSL à un canal de retour SOAP

Les fédérations à connexion unique Tivoli Federated Identity Manager prennent en charge la configuration de l'authentification par certificat ou l'authentification de base entre les partenaires de la fédération. Lorsque l'environnement de déploiement inclut un serveur IHS, vous devez configurer un canal de retour SOAP afin de permettre la prise en charge de ces méthodes d'authentification.

Vous devez ajouter un hôte virtuel à la configuration IHS. Les paramètres de configuration sont généralement présents dans le fichier de configuration IHS standard. Par exemple, sous Linux ou UNIX :

```
/opt/IBM/HTTPServer/httpd.conf
```

Pour obtenir les instructions correspondantes, consultez le centre de documentation de votre instance IBM HTTP Server pour WebSphere Application Server :http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp. Consultez les rubriques relatives à la sécurité d'IBM HTTP Server, notamment :

- Sécurisation au moyen de communications SSL

Mise à jour de la configuration de la fédération pour les connexions SOAP

Lorsque l'instance IBM HTTP Server est configurée pour l'écoute simultanée sur le port par défaut et le port de retour SOAP, vous devez définir et configurer votre fédération en utilisant ces ports dans les adresses URL de la fédération.

Il convient de définir les URL de la fédération sur le port 443. Comme il s'agit du port HTTPS par défaut, il n'est pas nécessaire d'inclure le numéro de port réel dans la syntaxe de l'URL. Le port de retour SOAP est généralement le port 9444.

Du fait que la sécurité du canal de retour SOAP implique une connexion avec le serveur IHS, la procédure de configuration typique appliquée lors de la définition d'une fédération ne nécessite aucune authentification client sur le canal de retour SOAP.

Il est à noter que l'environnement WebSphere peut impliquer l'instauration d'une configuration SSL entre le serveur IHS et les noeuds compris dans le cluster WebSphere. Si cette configuration est appropriée pour votre déploiement, reportez-vous à la documentation de WebSphere.

Confirmation des propriétés de sécurité de WebSphere Application Server

Si vous avez installé la version imbriquée de WebSphere Application Server avec l'installation du composant de services d'exécution et de gestion, plusieurs de ses paramètres ont été configurés lors de l'installation. Si vous utilisez une version existante de WebSphere Application Server (par exemple, une version installée précédemment, ou la version installable séparément, vous devez configurer ces paramètres manuellement.

Avant de commencer

Les paramètres sont les suivants :

- La sécurité des applications et la sécurité d'administration sont activées.
- La connexion unique (cookie LTPA) est activée.

Utilisez les procédures ci-dessous pour confirmer que les paramètres de configuration sont corrects pour votre environnement Tivoli Federated Identity Manager.

Utilisez la console de gestion de WebSphere pour contrôler les paramètres de WebSphere.

Pourquoi et quand exécuter cette tâche

La sécurité des applications et la sécurité d'administration sont activées

Pour confirmer que la sécurité des applications et la sécurité d'administration sont activées, procédez comme suit :

1. Cliquez sur **Sécurité → Administration, applications et infrastructure sécurisées**.
2. Confirmez que la sécurité des applications et la sécurité d'administration sont activées.

La connexion unique est activée

Pour confirmer que la connexion unique est activée, procédez comme suit :

1. Cliquez sur **Sécurité → Administration, applications et infrastructure sécurisées**.
2. Développez **Sécurité Web** à droite pour afficher :
   - **Paramètres généraux**
   - **connexion unique**
   - **Relation de confiance**
3. Cliquez sur **connexion unique**.
4. Assurez-vous que l'option **Activé(e)** est sélectionnée.
5. cliquez sur **Sécurité → Administration, applications et infrastructure sécurisées > Sécurité Web - Paramètres généraux**
6. Sous l'onglet Configuration, dans la section Propriétés générales, cochez la case **Utiliser les données d'authentification disponibles lors de l'accès à un URI non protégé**.

Activation de codage multilingue sur WebSphere Application Server

Activez le codage multilingue en activant le codage client UTF-8 dans WebSphere Application Server.

Pourquoi et quand exécuter cette tâche

La procédure pour activer le codage multilingue est identique à celle de la version intégrée de WebSphere Application Server et de la version de WebSphere Application Server existante.

Procédure

1. Ouvrez une invite de commande.
2. Démarrez l'outil 'wsadmin' de WebSphere Application Server. A partir de votre profil WebSphere, entrez la commande appropriée afin que votre système d'exploitation démarre l'outil :

   Windows

   ```
   wsadmin.bat
   ```

   AIX, Linux, HP-UX ou Solaris

   ```
   wsadmin.sh
   ```

   Remarque : Pour de plus amples informations sur les options pouvant être définies à l'aide de l'outil wsadmin, reportez-vous au centre d'information en ligne à l'adresse http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp.
3. A l'invite de commande, exécutez les commandes suivantes pour activer le codage UTF-8 :
   a. Pour afficher les propriétés JVM en cours :

      ```
      $AdminTask showJVMProperties { -propertyName genericJvmArguments }
      ```

   b. Pour définir les propriétés JVM :

      ```
      $AdminTask setGenericJVMArguments { -genericJvmArguments
      "<current-jvm-properties>  -Dclient.encoding.override=UTF-8" }
      ```

   c. Pour sauvegarder les modifications de configuration :

      ```
      $AdminConfig save
      ```
4. Redémarrez WebSphere Application Server.

Mappage de rôles d'application avec des utilisateurs

Avant de commencer

Lorsqu'IBM Tivoli Federated Identity Manager est déployé avec la version intégrée de WebSphere, l'installation d'IBM Tivoli Federated Identity Manager mappe automatiquement les rôles d'application avec des utilisateurs. Lorsqu'IBM Tivoli Federated Identity Manager est déployé avec une instance existante du serveur WebSphere, IBM Tivoli Federated Identity Manager, vous devez procéder à la création des mappages manuellement.

Vous pouvez définir les différents rôles d'après les besoins de votre déploiement en matière de sécurité.

Pourquoi et quand exécuter cette tâche

Utilisez la console d'administration WebSphere pour spécifier les mappages.

Procédure

1. Accédez à **Applications d'entreprise > ITFIMRuntime > Rôle de sécurité pour le mappage utilisateur/groupe**
2. Sélectionnez les mappages dans la table des rôles.

   Pour chaque rôle, sélectionnez l'option tout le monde (Everyone) ou Tous les utilisateurs authentifiés (All authenticated).

   Remarque : FIMAnyAuthenticated *ne doit pas* être mappé avec Tout le monde.

   Exemples de rôles :
   - TrustClientRole
   - FIMUnauthenticated
   - FIMSoapClient
   - FIMAnyAuthenticated
   - FIMAdministrator
   - TrustClientInternalRole
   - FIMNobody
3. Cliquez sur **OK** quand vous avez terminé.
4. Synchronisez tous les noeuds du cluster.

   Pour obtenir des instructions, consultez le centre de documentation de WebSphere : http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp. Reportez-vous à la rubrique *Mappage d'utilisateur avec des rôles*.

Résultats

Le composant d'exécution de Tivoli Federated Identity Manager fonctionne maintenant avec WebSphere en tant que serveur point de contact dans un environnement WebSphere Network Deployment (ND).

Configuration du serveur IHS pour l'authentification client

Lors de la configuration de partenaires pour une fédération de connexion unique, vous pouvez spécifier les méthodes prises en charge pour l'authentification client. L'assistant à interface graphique du partenaire de fédération vous invite à spécifier soit l'authentification par certificat SSL, soit l'authentification de base. Suivant votre choix, vous devez configurer IBM HTTP Server (IHS) en conséquence. Suivez les instructions contenues dans la section suivante en fonction de votre méthode d'authentification.

Configuration de l'authentification par certificat pour IHS

Lorsque la configuration du partenaire de fédération implique la gestion d'un certificat client SSL sur une connexion SOAP, vous devez importer ce certificat en tant que certificat d'autorité de certification (CA) dans la base de données de clés utilisée par IHS sur SSL.

A titre d'exemple, voici une base de données de clés sur Linux ou UNIX :

```
/usr/IBM/HTTPServer/conf/httpkeys.kdb
```

Exécutez l'utilitaire **ikeyman** pour importer le certificat.

Pour obtenir les instructions correspondantes, consultez le centre de documentation de votre instance IBM HTTP Server pour WebSphere Application Server : http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp. Consultez les rubriques relatives à la sécurité d'IBM HTTP Server, notamment :

- Stockage d'un certificat pour l'autorité de certification

Configuration de l'authentification de base pour IHS

Lorsque la configuration du partenaire de fédération implique une authentification de base sur une connexion SOAP, vous devez activer l'authentification LDAP pour IHS.

Pour obtenir les instructions correspondantes, consultez le centre de documentation de votre instance IBM HTTP Server pour WebSphere Application Server : http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp. Consultez les rubriques relatives à la sécurité d'IBM HTTP Server, notamment :

- Authentification LDAP sur IBM HTTP Server

WebSphere en tant que point de contact pour les fournisseurs d'identité

Si vous prévoyez d'être le fournisseur d'identité dans votre fédération et que vous utilisez IBM WebSphere Application Server en tant que serveur pour de contact, vous disposez de deux options en ce qui concerne la méthode d'authentification. Le choix de la méthode d'authentification détermine la configuration requise dans votre environnement.

Choisissez une des options suivantes pour la méthode d'authentification sur votre WebSphere Application Server :

- Authentification par formulaires, à l'aide de tout registre d'utilisateurs pris en charge par WebSphere Application Server
- Authentification du bureau Windows via la prise en charge de SPNEGO TAI sur WebSphere Application Server 6.1 et l'utilisation de Microsoft Active Directory en tant que registre d'utilisateurs

Avertissement : Avant d'accomplir les tâches décrites dans le présent chapitre, assurez-vous que les paramètres sont corrects en appliquant la procédure «Confirmation des propriétés de sécurité de WebSphere Application Server», à la page 71.

authentification par formulaires

Dans cette configuration, le fournisseur d'identité utilise n'importe quel registre d'utilisateurs pris en charge par WebSphere Application Server doté de la fonction d'authentification par formulaires, afin d'authentifier les utilisateurs qui demandent la connexion unique. Tous les utilisateurs du fournisseur d'identité doivent exister dans le registre d'utilisateurs pris en charge. Lorsque des utilisateurs tentent de faire appel à la connexion unique pour accéder à une ressource (telle qu'une application Web), Tivoli Federated Identity Manager présente un formulaire de connexion. Ce dernier est fourni avec Tivoli Federated Identity Manager.

Un utilisateur non authentifié qui émet une demande de connexion unique sur une ressource de fournisseur de services sera authentifié sur le registre d'utilisateurs configuré pour WebSphere Application Server.

Un exemple de cette configuration est présenté dans la figure 1.

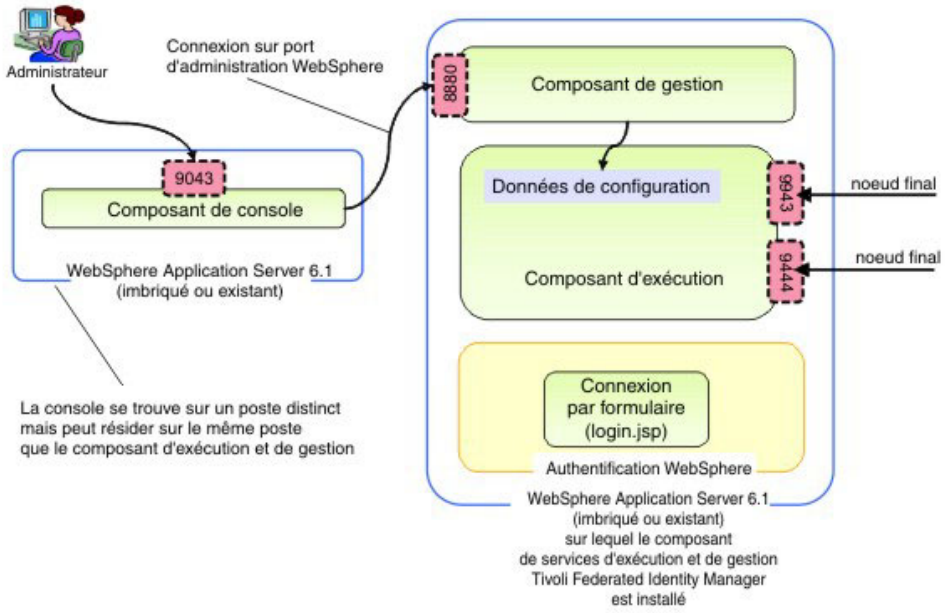


Figure 1. Exemple de WebSphere Application Server doté de la fonction d'authentification par formulaires

Remarques sur la configuration :

- Il est à noter que l'instance de WebSphere Application Server peut être soit un déploiement existant de WebSphere (avec le niveau approprié de groupes de correctifs appliqués), soit la version intégrée de WebSphere Application Server version 6.1 distribuée avec Tivoli Federated Identity Manager.
- Un formulaire de connexion présenté par le serveur WebSphere Application Server sur lequel Tivoli Federated Identity Manager est installé. Le formulaire de connexion est fourni.

Suivez les tâches indiquées à la section «Configuration de l'authentification par formulaires», à la page 77.

Authentification à partir du bureau Windows via le support SPNEGO TAI à l'aide de Microsoft Active Directory

Cette configuration utilise un support TAI (Trust Association Interceptor) WebSphere qui prend en charge une authentification en mode silencieux à l'aide du protocole SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism), qui est fourni avec WebSphere Application Server. Cette configuration permet à Tivoli Federated Identity Manager d'acquérir en toute sécurité l'identité du bureau de l'utilisateur, qui sert ensuite à créer l'assertion de la connexion unique fédérée.

Le fournisseur d'identité utilise Microsoft Active Directory en tant que registre d'utilisateurs, ainsi que l'authentification de domaine Microsoft Windows. Windows doit être configuré en tant que contrôleur de domaine. Tous les utilisateurs du fournisseur d'identité doivent exister dans le registre d'utilisateurs Active Directory. Pour établir une connexion unique à une application Web, les utilisateurs ont recours à leurs données d'identification sur le bureau Windows.

Un exemple de cette configuration est présenté dans la figure 2.

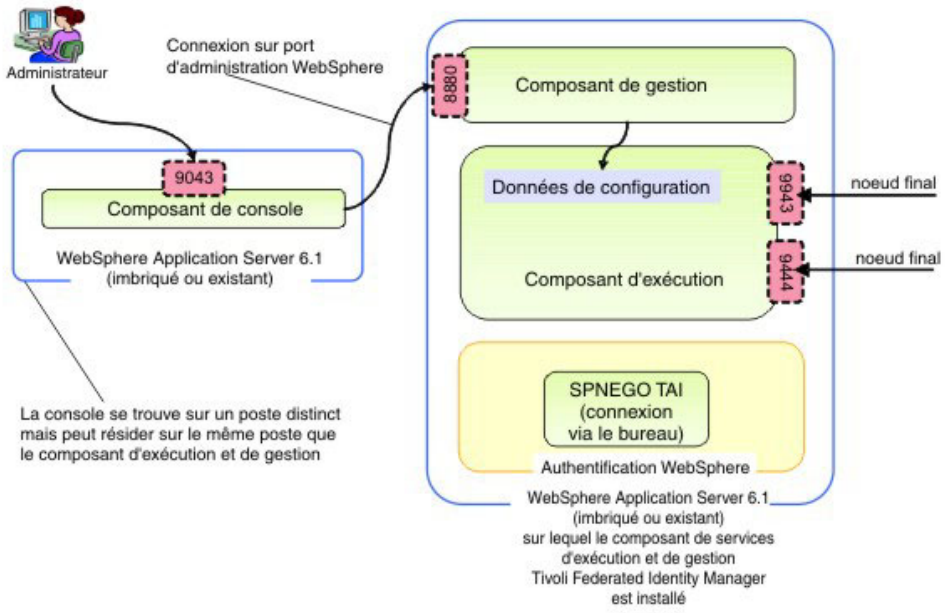


Figure 2. Exemple de WebSphere Application Server doté de l'authentification SPNEGO TAI

Remarques sur la configuration :

- Il est à noter que l'instance de WebSphere Application Server peut être soit un déploiement existant de WebSphere (avec le niveau approprié de groupes de correctifs appliqués), soit la version intégrée de WebSphere Application Server version 6.1 distribuée avec Tivoli Federated Identity Manager.
- Microsoft Active Directory doit être utilisé en tant que registre d'utilisateurs. Utilisez une version prise en charge par Microsoft Windows Server 2003. Le registre d'utilisateurs doit inclure un utilisateur d'administration WebSphere et un utilisateur pour l'identité Kerberos. En outre, un fichier de clés doit être généré pour chaque utilisateur. Vous avez besoin des propriétés de connexion LDAP pour le serveur Active Directory avant de configurer Tivoli Federated Identity Manager.

  Le registre d'utilisateurs doit également être configuré avant IBM WebSphere Application Server.
- L'authentification SPNEGO est fournie avec WebSphere Application Server via le module d'extension TAI (Trust Association Interceptor). Elle utilise Kerberos pour effectuer l'authentification.

- Les utilisateurs se connectent à l'aide de leur connexion bureau au domaine Windows. Cette méthode de connexion peut également être désignée par "connexion unique via le bureau."
- Les navigateurs des utilisateurs doivent être configurés de sorte que l'authentification Windows intégrée soit activée.

Suivez les tâches indiquées à la section «Configuration de l'authentification SPNEGO», à la page 81.

Configuration de l'authentification par formulaires

Si vous utilisez WebSphere Application Server comme serveur point de contact doté de la fonction d'authentification par formulaires, vous devez effectuer plusieurs tâches de configuration.

Pourquoi et quand exécuter cette tâche

Les tâches sont les suivantes :

1. «Sélection et installation du registre d'utilisateurs»
2. «Configuration du registre d'utilisateurs», à la page 78
3. «Ajout d'utilisateurs de connexion unique», à la page 78
4. «Ajout d'utilisateurs d'administration», à la page 78
5. «Configuration du registre d'utilisateurs pour embeddedWebSphere», à la page 79
6. «Configuration d'une connexion SSL au registre d'utilisateurs», à la page 80
7. «Personnalisation du formulaire de connexion», à la page 80

Sélection et installation du registre d'utilisateurs

Un registre d'utilisateurs est requis dans votre environnement de fournisseur d'identité. Le registre d'utilisateurs sert de référentiel pour les informations relatives aux utilisateurs auxquels vous fournissez des fonctionnalités de connexion unique et aux fournisseurs de services avec lesquels vous partagez une fédération. Il peut également servir de référentiel pour les informations relatives aux utilisateurs d'administration de votre environnement ou vous pouvez choisir de conserver les utilisateurs d'administration dans un registre d'utilisateurs distinct.

Avant de commencer

Vous pouvez choisir un registre d'utilisateurs compatible avec votre serveur point de contact IBM WebSphere Application Server et avec la méthode d'authentification utilisée.

Si vous utilisez l'authentification par formulaires, vous pouvez choisir un registre d'utilisateurs à partir de nombreuses options. Reportez-vous au centre de documentation de WebSphere Application Server 6.1 à l'adresse http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp. Recherchez ensuite des informations sur le choix d'un registre d'utilisateurs, en sélectionnant **WebSphere Application Server (Distributed platforms and Windows)** → **Securing applications and their environment** → **Authenticating users** → **Selecting a registry or repository**.

Pourquoi et quand exécuter cette tâche

Si vous utilisez une installation existante de WebSphere Application Server, il se peut qu'un registre d'utilisateurs compatible soit déjà installé et configuré.

Si vous utilisez une nouvelle installation de la version imbriquée de WebSphere Application Server, vous disposez des options suivantes :

- Utiliser le domaine de référentiel d'utilisateurs basé sur un fichier, qui a été installé avec la version imbriquée de WebSphere Application Server. L'utilisateur d'administration a été configuré dans ce registre pendant l'installation. Les autres tâches requises pour l'ajout des utilisateurs de connexion unique sont indiquées ultérieurement dans ce chapitre.
- Utiliser un registre d'utilisateurs différent. Pour plus d'informations sur vos options de registre d'utilisateurs, consultez la documentation de WebSphere Application Server. Ensuite, installez et configurez le registre d'utilisateurs choisi, si vous n'utilisez pas un registre d'utilisateurs déjà existant. Configurez ensuite WebSphere pour utiliser ce registre d'utilisateurs. Voir «Configuration du registre d'utilisateurs pour embeddedWebSphere», à la page 79.

Configuration du registre d'utilisateurs

La configuration du registre d'utilisateurs est une étape importante de la configuration globale.

Avant de commencer

Avant de procéder à cette tâche, vous devez sélectionner le registre d'utilisateurs à utiliser et l'installer selon la procédure décrite dans la section «Sélection et installation du registre d'utilisateurs», à la page 77.

Pourquoi et quand exécuter cette tâche

Dans votre registre d'utilisateurs, vous allez créer des utilisateurs auxquels fournir des fonctionnalités de connexion unique. Vous pouvez également créer des utilisateurs pour les administrateurs de votre environnement ou choisir de conserver les utilisateurs d'administration dans un référentiel distinct.

Ajout d'utilisateurs de connexion unique :

Dans l'environnement du fournisseur d'identité, le registre d'utilisateurs sert à authentifier les utilisateurs qui ont recours à la connexion unique. Ajoutez ces utilisateurs dans votre registre d'utilisateurs, à l'aide de la documentation correspondante.

Ajout d'utilisateurs d'administration :

Si vous avez installé la version imbriquée de WebSphere Application Server, un domaine de référentiel d'utilisateurs basé sur un fichier et désigné par *référentiel fédéré* a été configuré pour les utilisateurs d'administration de Tivoli Federated Identity Manager. Si vous préférez gérer les utilisateurs d'administration via le même registre d'utilisateurs que celui dans lequel vos utilisateurs de connexion unique sont configurés, vous devez les ajouter dans ce registre d'utilisateurs.

Avant de commencer

L'utilisateur administratif que vous avez pendant l'installation a été créé dans le référentiel d'utilisateurs par défaut lors de l'installation de Tivoli Federated Identity Manager.

Pourquoi et quand exécuter cette tâche

Pour ajouter cet utilisateur dans un registre d'utilisateurs différent, procédez comme suit :

Procédure

1. Créez l'utilisateur à l'aide de la documentation de votre registre d'utilisateurs. Pensez à utiliser l'ID nom et le mot de passe qui ont été utilisés pour l'administrateur lors de l'installation de Tivoli Federated Identity Manager.
2. Suivez les instructions de la section «Configuration du registre d'utilisateurs pour embeddedWebSphere».

Configuration du registre d'utilisateurs pour embeddedWebSphere

Si vous avez installé la version intégrée de WebSphere Application Server, cela signifie que le référentiel fédéré a été configuré en tant que registre d'utilisateurs. Si vous souhaitez utiliser un registre d'utilisateurs autre que le référentiel fédéré par défaut, vous devez modifier les paramètres de WebSphere Application Server.

Pourquoi et quand exécuter cette tâche

Pour permettre à WebSphere d'utiliser votre registre d'utilisateurs, procédez comme suit :

Procédure

1. Connectez-vous à la console. Sélectionnez **Sécurité → Administration, application et infrastructure sécurisées**. L'onglet Configuration s'affiche.
2. Cliquez sur **Assistant de configuration des paramètres de sécurité** pour modifier le registre d'utilisateurs utilisé par le composant d'exécution WebSphere.
3. Le panneau **Spécifier l'étendue de la protection** apparaît. Vérifiez que la case **Activer la sécurité des applications** est cochée. Cliquez sur **Suivant**.
4. Le panneau **Sécuriser l'environnement de traitement des applications** apparaît. Sélectionnez l'option correspondant au registre d'utilisateurs de votre choix :
   - **Référentiels fédérés**
   - **Registre LDAP autonome**
   - **Système d'exploitation local**
   - **Registre personnalisé autonome**
5. Cliquez sur **Suivant**. Le panneau **Configurer le référentiel d'utilisateurs** s'affiche. Indiquez des valeurs pour chaque paramètre de configuration du registre. Pour obtenir une description des zones présentées, consultez l'aide en ligne.
6. Cliquez sur **Suivant** et quittez l'assistant. Sauvegardez les modifications apportées à votre configuration.
7. Arrêtez, puis redémarrez WebSphere Application Server. Vous devez utiliser le nom d'administrateur que vous avez choisi pour vous connecter et effectuer ces modifications.
8. Dans la console, sélectionnez **Tivoli Federated Identity Manager → Gestion de la configuration → Propriétés du domaine**.

9. Dans la section Sécurité WebSphere du panneau, mettez à jour les valeurs suivantes :

   Nom de l'utilisateur d'administration
   Remplacez l'entrée existante par le nom de compte administrateur LDAP entré à l'étape précédente. Par exemple, `ldapadmin`

   Mot de passe d'administration
   Entrez le mot de passe de l'administrateur LDAP.
10. Sauvegardez les modifications.
11. Arrêtez WebSphere Application Server.
12. Redémarrez WebSphere Application Server.

Configuration d'une connexion SSL au registre d'utilisateurs

Après avoir configuré votre registre d'utilisateurs, activez SSL pour protéger la connexion entre SSL et le serveur.

Pourquoi et quand exécuter cette tâche

Pour obtenir des instructions, consultez le centre de documentation de WebSphere Application Server 6.1 à l'adresse http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp. Pour plus d'informations sur la création de connexions SSL, sélectionnez **WebSphere Application Server (Distributed platforms and Windows) → Securing applications and their environment → Securing communications**.

Il peut être également nécessaire de consulter la documentation de votre registre d'utilisateurs.

Exemple

Personnalisation du formulaire de connexion

Si vous utilisez une authentification sur la base de formulaires pour authentifier les utilisateur via une connexion unique, un formulaire de connexion et une page d'erreur liée à celui-ci sont affichés à votre intention.

Pourquoi et quand exécuter cette tâche

Le formulaire de connexion et la page d'erreur dont partie des pages de réponse générées par Tivoli Federated Identity Manager. Vous pouvez personnaliser les pages afin de les rendre conformes aux besoins de votre environnement et de modifier leur aspect. Les identificateurs de ces pages sont les suivants :

proper/login/formlogin.html
La page de connexion s'affiche côté client Web lorsque la connexion unique est déclenchée chez le fournisseur d'identité par un utilisateur non authentifié.

proper/login/formloginerror.html
En cas d'incident d'authentification, la page d'erreur s'affiche.

Configuration de l'authentification SPNEGO

Si vous utilisez WebSphere Application Server comme serveur point de contact doté de la fonction d'authentification SPNEGO, vous devez effectuer plusieurs tâches de configuration.

Pourquoi et quand exécuter cette tâche

Ces tâches de configuration sont les suivantes :

Procédure

1. Configuration de Microsoft Active Directory, notamment les tâches suivantes :
   a. Création d'un utilisateur Active Directory pour l'administrateur WebSphere.
   b. Création d'un utilisateur contenant le nom principal de service (SPN) du serveur Tivoli Federated Identity Manager.
   c. Génération d'un fichier de clés Kerberos et attribution du nom SPN pour l'utilisateur Active Directory créé à l'étape 1b.
   d. Collecte des paramètres de configuration d'Active Directory
2. Configuration du domaine et des connexions utilisateur Windows.
3. Configuration de WebSphere Application Server, notamment les tâches suivantes :
   a. Configuration de la sécurité d'administration, en utilisant Active Directory comme type de registre d'utilisateurs LDAP.
   b. Configuration d'une connexion SSL sur Active Directory (facultatif).
4. Activation de WebSphere SPNEGO et du support TAI (Trust Association Interceptor), à l'aide d'Integrated Solutions Console. Le cas échéant, vous pouvez personnaliser les attributs TAI, en fonction des besoins de votre environnement.
5. Instructions fournies à vos utilisateurs pour la configuration d'Internet Explorer, comme suit :
   a. Ajout du nom d'hôte sous forme d'hôte sécurisé dans la zone intranet.
   b. Activation de l'authentification intégrée de Windows.

Configuration d'Active Directory pour SPNEGO

Avant de pouvoir utiliser WebSphere Application Server avec l'authentification SPNEGO, vous devez configurer Microsoft Active Directory en tant que registre d'utilisateurs. Vous devez effectuer plusieurs tâches de configuration dans Microsoft Active Directory :

Avant de commencer

- Créez un d'utilisateur pour l'administration de WebSphere.
- Créez un utilisateur contenant le nom principal de service (SPN) du serveur Tivoli Federated Identity Manager.
- Générez un fichier de clés Kerberos et attribuez le nom SPN à l'utilisateur Active Directory qui a été créé à cet effet.
- Collectez les paramètres de connexion d'Active Directory.

Microsoft Active Directory est un composant requis dans un environnement de fournisseur d'identité dans lequel IBM WebSphere Application Server, doté de l'authentification SPNEGO, est utilisé en tant que serveur point de contact. Il convient que votre instance de Microsoft Active Directory soit installée et configurée pour votre réseau avant que vous ne commenciez cette tâche.

Pourquoi et quand exécuter cette tâche

Pour plus de détails sur l'exécution des étapes de cette procédure, reportez-vous à la documentation de Microsoft Active Directory.

Procédure

1. A l'aide de la console des configuration des utilisateurs et ordinateurs Active Directory, créez un utilisateur Active Directory pour l'administrateur WebSphere. Cet utilisateur correspond à un compte utilisateur classique dans Active Directory, sans aucun privilège de compte particulier. Employez un nom d'utilisateur reflétant le rôle de cet utilisateur. Vous pouvez par exemple utiliser le nom `wasadmin`.
2. A l'aide de la console des configuration des utilisateurs et ordinateurs Active Directory, réez un utilisateur contenant le nom principal de service (SPN) de votre serveur Tivoli Federated Identity Manager. Le nom d'utilisateur de ce compte n'est pas important. Le nom de principal de service de cet utilisateur sera défini à l'aide de l'utilitaire ktpass dans une étape ultérieure. Attribuez à cet utilisateur un mot de passe très sécurisé et définissez ce dernier de sorte qu'il n'arrive jamais à expiration.
3. Exécutez la commande ktpass pour générer un fichier keytab pour l'utilisateur Kerberos de WebSphere. L'utilitaire ktpass est inclus dans le module d'outils de support de Microsoft Windows 2003 Server Support Tools package. Utilisez les paramètres suivants avec la commande :

Tableau 8. Paramètres à utiliser avec la commande Microsoft Windows ktpass

Paramètre	Exemple de valeur	Description
-out	`was1-krb5.keytab`	Nom de fichier dans lequel est stockée la clé confidentielle qui sera utilisée ultérieurement pour la validation de l'authentification Kerberos sur le serveur WebSphere. Ce fichier sera chargé sur le serveur WebSphere lorsque vous activerez SPNEGO. Voir «Activation et configuration de l'authentification SPNEGO», à la page 87.
-princ	`HTTP/ibm-fim611-1.fimtest. example.com@FIMTEST .EXAMPLE.COM`	Nom de principal de service Kerberos à utiliser pour la génération de la clé. Ce nom fait la distinction entre les majuscules et les minuscules et doit obligatoirement commencer par `HTTP/`. La portion située après l'instruction `HTTP/` doit correspondre au nom de domaine DNS qualifié complet de l'adresse URL que les utilisateurs verront s'afficher dans leur navigateur lorsqu'ils accéderont au serveur WebSphere.
-pass	*	Mot de passe à définir pour le principal Kerberos. Lorsqu'une valeur de * est indiquée, l'utilisateur est invité à entrer le mot de passe. Le mot de passe doit correspondre à l'utilisateur créé à l'étape 2.

Tableau 8. Paramètres à utiliser avec la commande Microsoft Windows ktpass (suite)

Paramètre	Exemple de valeur	Description
-mapuser	`was-1`	Utilisateur Active Directory vers lequel le principal de service Kerberos sera mappé. Il convient que la valeur définie ici correspondre au nom d'utilisateur créé à l'étape 2, à la page 82.
-mapOp	`set`	Indique que le nom SPN doit remplacer toutes les valeurs existantes mappées pour cet utilisateur Active Directory.

L'exemple suivant illustre une exécution de la commande ktpass. Il explique également comment utiliser la commande setspn pour répertorier des noms de principal de service pour l'utilisateur was-1, à titre d'information et de vérification.

```
C:\Program Files\Support Tools>ktpass -out was1-krb5.keytab
 -princ HTTP/ibm-fim611-1.fimtest.example.com@FIMTEST.EXAMPLE.COM
 -pass * -mapuser was-1 -mapOp set

Targeting domain controller: ibm-fimtest-ad.fimtest.example.com

Successfully mapped HTTP/ibm-fim611-1.fimtest.example.com:

Type the password again to confirm:

Key created.

Output keytab to was1-krb5.keytab:

Keytab version:0x502

keysize 76 HTTP/ibm-fim-611-1.fimtest.example.com@FIMTEST.EXAMPLE.COM
 ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x3 (DES-CBC-MD5)
 keylength 8 (0x799b26bfe9ad3ba4)

Account was-1 has been set for DES-only encryption.

C:\Program Files\Support Tools>setspn -1 was-1

Registered ServicePrincipalNames for
CN=was-1,CN-Users,DC=fimtest,DC=ibm,DC=com:

   HTTP/ibm-fim611-1.fimtest.ibm.com
```

Figure 3. Exemple de commande ktpass

Le fichier keytab créé au cours de cette étape est chargé sur le serveur Tivoli Federated Identity Manager durant la configuration de WebSphere Application Server (voir «Configuration de WebSphere pour SPNEGO», à la page 85).

4. Collectez les informations de configuration de la connexion Active Directory permettant d'utiliser la configuration WebSphere Application Server en procédant comme suit :
   a. Recherchez les informations suivantes dans l'arborescence LDAP d'Active Directory.

      Nom d'hôte
      Nom d'hôte du serveur Active Directory.

Port Numéro de port du serveur Active Directory.

DN de base
Nom distinctif (DN) de recherche de base pour les utilisateurs Active Directory.

DN BIND
DN Active Directory d'un utilisateur d'administration pour l'exécution de recherches LDAP. Cette valeur ne doit pas nécessairement correspondre au nom distinctif du compte d'administration de domaine, mais plutôt à celui d'un utilisateur valide d'Active Directory.

Mot de passe Bind
Mot de passe de l'utilisateur représenté par le DN BIND.

b. Si une connexion SSL est requise par Active Directory, WebSphere doit être configuré avec le certificat de l'autorité de certification émettrice du contrôleur de domaine. Si le composant Windows Certificate Services a été installé sur le contrôleur de domaine, il s'agit du certificat de CA lié à Certificate Services sur ce contrôleur de domaine. Pour exporter le certificat de CA vers un fichier, procédez comme suit :
   1) Ouvrez **Outils d'administration → Certification Authority**. Cliquez ensuite à l'aide du bouton droit de la souris sur le nom de l'autorité de certification (CA) de niveau supérieur, puis cliquez sur **Properties**.
   2) Cliquez sur l'onglet **General** puis sur **View Certificate**.
   3) Cliquez sur l'onglet **Details**, puis sur **Copy to File**.
      Le fichier est enregistré au format binaire DER. Vous serez amené à utiliser ce fichier dans le cadre de la configuration de WebSphere, si l'authentification sur le serveur SSL est nécessaire pour établir le contact avec le serveur Active Directory via l'interface LDAP/SSL.

Configuration du domaine Windows et des connexions utilisateur

Pour utiliser la connexion unique via le bureau Windows, les connexions bureau des utilisateurs doivent être authentifiées pour le domaine Windows.

Pourquoi et quand exécuter cette tâche

L'utilisation de la connexion unique via le bureau Windows au serveur Tivoli Federated Identity Manager nécessite que les utilisateurs se connectent à leur bureau en tant que membres d'un domaine Windows. En particulier, le domaine Windows doit prendre en charge l'authentification Kerberos auprès d'un service Microsoft Active Directory. Pour plus de détails sur la création de cet environnement, consultez la documentation Microsoft.

Cette configuration permet au fournisseur d'identité de prendre en charge les utilisateurs internes qui sont connectés au site intranet du fournisseur d'identité, à l'aide d'une connexion bureau à un domaine Windows. Cependant, un fournisseur d'identité peut également être amené à prendre en charge des utilisateurs externes qui ne possèdent pas de connexion au domaine Windows. Ces utilisateurs externes doivent s'authentifier à l'aide d'un formulaire de connexion.

Par défaut, le support SPNEGO TAI dans Tivoli Federated Identity Manager affiche un formulaire de connexion si un utilisateur qui ne s'est pas authentifié via la connexion bureau tente une connexion unique. Par défaut, le formulaire de connexion est l'exemple de formulaire de connexion fourni avec Tivoli Federated

Identity Manager. Vous pouvez personnaliser la présentation de ce formulaire, selon la procédure décrite dans la section «Personnalisation du formulaire de connexion», à la page 80. Si vous ne souhaitez pas afficher ce formulaire de connexion, vous pouvez modifier les attributs TAI selon la procédure décrite dans la section «Configuration des attributs TAI personnalisés», à la page 90.

Configuration de WebSphere pour SPNEGO

Avant de pouvoir utiliser WebSphere Application Server avec SPNEGO, vous devez configurer la sécurité des applications WebSphere en définissant Active Directory en tant que référentiel d'utilisateurs.

Pourquoi et quand exécuter cette tâche

Les étapes sont les suivantes :

- (Facultatif) Chargement du certificat racine de CA du serveur Active Directory afin d'activer le protocole SSL entre le serveur et Active Directory.
- Activation de la sécurité des applications WebSphere avec Active Directory en tant que registre d'utilisateurs.
- Configuration des caractéristiques du répertoire LDAP autonome de sorte que celui-ci pointe sur le serveur Active Directory.

Procédure

1. Facultatif : Chargez le certificat racine de CA du serveur Active Directory. Cette étape n'est requise que si vous utilisez LDAP/SSL pour communiquer avec le serveur Active Directory. Avant de poursuivre cette procédure, veillez à effectuer les étapes de la section «Configuration d'Active Directory pour SPNEGO», à la page 81, notamment l'étape 4b, à la page 84. Si vous n'utilisez pas le protocole, passez à l'étape suivante.
   a. Connectez-vous à la console.
   b. Cliquez sur **Certificat SSL et gestion des clés**.
   c. Dans le panneau Certificat SSL et gestion des clés, cliquez sur **Magasins de clés et certificats**.
   d. Dans le panneau Magasins de clés et certificats, cliquez sur **NodeDefaultTrustStore**.
   e. Dans le panneau NodeDefaultTrustStore, cliquez sur **Certificats de signataires**.
   f. Dans le panneau Certificats de signataires, cliquez sur **Ajouter** pour ajouter un nouveau signataire.
   g. Complétez les caractéristiques du certificat de signataire, puis cliquez sur **OK**. Utilisez les valeurs suivantes :

Tableau 9. Caractéristiques du certificat de signataire dans l'environnement SPNEGO

Nom de zone	Valeur
Alias	Nom d'alias du certificat de CA issu d'Active Directory. Par exemple, vous pouvez utiliser le nom du contrôleur de domaine Active Directory.
Nom de fichier	Chemin et nom de fichier du certificat. Il est à noter que ce chemin d'accès, ainsi que le nom du fichier, sont définis sur le serveur où WebSphere Application Server est installé, et non sur le serveur qui exécute le navigateur. Cela signifie que le fichier doit être copié sur le serveur WebSphere avant la réalisation de cette étape.

Tableau 9. Caractéristiques du certificat de signataire dans l'environnement SPNEGO (suite)

Nom de zone	Valeur
Type de données	Format de fichier du certificat. Utilisez le même format que celui de l'étape 4b, à la page 84.

Une fois que le chargement du certificat aboutit, ce dernier s'affiche dans la liste des certificats de signataire.

2. Activez la sécurité des applications WebSphere avec Active Directory en tant que registre d'utilisateurs.

   Remarque : Pour effectuer cette étape, vous devez être en mesure d'accéder au serveur Active Directory à l'aide du port 389 (c'est-à-dire, sans utiliser SSL). Pendant cette étape, l'assistant de configuration de la sécurité effectue un test de connexion qui ne prend pas en charge SSL. Si ce test échoue, la configuration n'aboutit pas. Vous pouvez activer LDAP/SSL une fois que le test et la configuration ont été terminés.

   a. Dans la console, cliquez sur **Sécurité → Administration, applications et infrastructure sécurisées**.
   b. Cliquez ensuite sur le bouton **Assistant de Configuration des paramètres de sécurité** pour démarrer l'assistant de configuration des paramètres de sécurité.
   c. Cliquez sur **Suivant**.
   d. A l'étape 1 de l'assistant, assurez-vous que la case **Activer la sécurité des applications** est cochée, puis cliquez sur **Suivant**.
   e. A l'étape 2 de l'assistant, sélectionnez **Répertoire LDAP autonome**, puis cliquez sur **Suivant**.
   f. A l'étape 3 de l'assistant, entrez les paramètres ci-dessous, puis cliquez sur **Suivant**.

Tableau 10. Paramètres du répertoire LDAP dans l'environnement SPNEGO

Nom de zone	Valeur
Nom de l'utilisateur administratif primaire	Utilisez le nom d'administrateur WebSphere créé dans Active Directory.
Type de serveur LDAP	Microsoft Active Directory
Hôte	Nom d'hôte du serveur Active Directory. Par exemple : `ibm-fimtest-ad.fimtest.example.com`
Port	Tant que vous n'exécutez pas l'étape de test de cet assistant de configuration, utilisez un port ne faisant pas appel à SSL. Par exemple, utilisez 389.
Nom distinctif (DN) de base	Nom distinctif (DN) de recherche de base pour les entrées utilisateur. Par exemple : `cn=users,dc=fimtest,dc=ibm,dc=com.`
Nom distinctif (DN) BIND	Nom distinctif d'un utilisateur Active Directory valide. Par exemple : `cn=administrator,cn=users,dc=fimtest,dc=ibm,dc=com.`
Mot de passe Bind	Mot de passe Active Directory de l'utilisateur représenté par le DN BIND.

   g. A l'étape 4 de l'assistant, la connexion au serveur Active Directory est testée. Cliquez sur **Terminer** pour mettre fin à l'assistant.

3. Configurez les caractéristiques du répertoire LDAP autonome de sorte que celui-ci pointe sur le serveur Active Directory.
   a. Dans la console, cliquez sur **Sécurité → Administration, applications et infrastructure sécurisées**.
   b. Dans la liste des définitions de domaine disponibles, sélectionnez **Registre LDAP autonome**, puis cliquez sur **Configurer**.
   c. Complétez les caractéristiques de votre configuration, y compris SSL et le port SSL si nécessaire, puis cliquez sur **OK** et enregistrez les modifications.

Activation et configuration de l'authentification SPNEGO

Avant de pouvoir utiliser WebSphere Application Server avec SPNEGO, vous devez activer l'authentification SPNEGO dans Tivoli Federated Identity Manager et configurer ses propriétés.

Pourquoi et quand exécuter cette tâche

Vous utiliserez la console pour effectuer cette procédure, qui comprend les étapes suivantes :

- Activation de SPNEGO aux fins d'utilisation avec Tivoli Federated Identity Manager.
- Configuration du client WebSphere Kerberos.
- Configuration du fichier de propriétés TAI.
- Configuration des paramètres de démarrage JVM.

Procédure

1. Connectez-vous à la console. Cliquez sur **Tivoli Federated Identity Manager → Gestion de la configuration → Point de contact**.
2. Sélectionnez le profil du serveur point de contact que vous utilisez dans votre environnement.
3. Cliquez sur le bouton **Avancé**. Le panneau Paramètres de sécurité de noeud final SOAP s'affiche.
4. Cliquez sur **Paramètres d'authentification SPNEGO**.
5. Cochez la case **Activer l'authentification SPNEGO**.
6. Entrez vos informations de configuration dans les zones du panneau. Pour la description des zones, voir l'aide en ligne.
7. Importez le fichier de clés Kerberos que vous avez créé à l'aide de l'option -out de l'utilitaire ktpass, en procédant comme suit :
   a. Cliquez sur le bouton **Importer le fichier de clés**.
   b. Dans la zone **Emplacement du fichier de clés**, entrez le chemin d'accès du fichier ou indiquez son emplacement à l'aide du bouton **Parcourir**.
   c. Cliquez sur **Terminer**.
8. Cliquez sur **OK**.

Configuration du support TAI (Trust Association Interceptor)

Si vous activez et configurez SPNEGO à l'aide de la console, le support TAI est automatiquement activé dans les paramètres de WebSphere Application Server.

Pourquoi et quand exécuter cette tâche

En règle générale, aucune autre configuration n'est nécessaire. Le fichier `tai.properties.template` contient des valeurs par défaut pour tous les instances TAI SPNEGO de WebSphere. Pour plus d'informations sur ces valeurs, voir «Attributs de configuration SPNEGO TAI».

Remarque : Pour apporter des modifications à ces valeurs par défaut, suivez les instructions figurant dans la section «Configuration des attributs TAI personnalisés», à la page 90.

Attributs de configuration SPNEGO TAI :

Les attributs de configuration personnalisée SPNEGO (Simple and Protected GSS-API Negotiation Mechanism) TAI (Trust Association Interceptor) contrôlent les différents aspects opérationnels de la méthode SPNEGO TAI. Ces attributs sont stockés dans le fichier `tai.properties.template`.

Contenu

Le fichier se trouve dans le répertoire par défaut suivant :

AIX, Linux ou Solaris

```
/opt/IBM/FIM/etc/tai.properties.template
```

Windows

```
C:\Program Files\IBM\FIM\etc\tai.properties.template
```

En général, il n'est pas nécessaire de modifier ce fichier. Vous pouvez configurer la méthode TAI à l'aide de la console, selon la procédure décrite dans la section «Configuration du support TAI (Trust Association Interceptor)». Cependant, si vous devez apporter des modifications supplémentaires nécessitant la mise à jour du fichier `tai.properties.template`, utilisez les instructions figurant dans la section «Configuration des attributs TAI personnalisés», à la page 90.

Remarque : La version du fichier tai.properties.template installée en même temps que Tivoli Federated Identity Manager contient des attributs complémentaires non fournis avec WebSphere Application Server 6.1. Si votre environnement nécessite l'utilisation d'attributs qui ne sont pas décrits ici, consultez le centre de documentation de WebSphere Application Server 6.1 pour obtenir la liste de tous les attributs disponibles en vue de la personnalisation de la configuration TAI SPNEGO. Le centre de documentation se trouve à l'emplacement suivant : http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp.

La figure ci-dessous décrit le contenu du fichier `tai.properties.template`.

```
#########################################################
# Fichiers de propriétés modèles pour SPNEGO TAI
#
# Où les valeurs par défaut possibles ont été fournies.
#
#########################################################
#---------------------------------------------------------
# Nom d'hôte
#---------------------------------------------------------
com.ibm.ws.security.spnego.SPN1.hostName=@POCHOST@

#---------------------------------------------------------
# (Facultatif) SpnegoNotSupportedPage
#---------------------------------------------------------
com.ibm.ws.security.spnego.SPN1.spnegoNotSupportedPage=file:///@SPNEGOFAILED@

#---------------------------------------------------------
# (Facultatif) NTLMTokenReceivedPage
#---------------------------------------------------------
com.ibm.ws.security.spnego.SPN1.NTLMTokenReceivedPage=file:///@SPNEGOFAILED@

#---------------------------------------------------------
# (Facultatif) FilterClass
#---------------------------------------------------------
#com.ibm.ws.security.spnego.SPN1.filterClass=com.ibm.ws.spnego.HTTPHeaderFilter

#---------------------------------------------------------
# (Facultatif) Filter
#---------------------------------------------------------
com.ibm.ws.security.spnego.SPN1.filter=request-url%=/sps/wasauth

#---------------------------------------------------------
# (Facultatif) Credential Delegation
#---------------------------------------------------------
#com.ibm.ws.security.spnego.SPN1.enableCredDelegate

#---------------------------------------------------------
# (Facultatif) Credential Delegation
#---------------------------------------------------------
#com.ibm.ws.security.spnego.SPN1.trimUserName=
```

Figure 4. Fichier tai.properties.template

Macros

Les macros ci-dessous sont utilisées dans le fichier `tai.properties.template`.

Tableau 11. Macros utilisées dans le fichier tai.properties.template

Macro	Description	Valeur par défaut
`@POCHOST@`	Nom d'hôte complet du serveur point de contact. Ce nom d'hôte est utilisé dans l'adresse URL du serveur point de contact.	`poc.example.com`
`@SPNEGOFAILED@`	Chemin complet d'un fichier HTML qui est envoyé au navigateur lorsque la négociation de l'authentification SPNEGO n'aboutit pas. Ce fichier HTML redirige automatiquement le navigateur vers l'exemple de page de connexion fournie par Tivoli Federated Identity Manager.	*répertoire_installation*`/etc/spnego_failed.html` Ce paramètre ne peut pas être configuré à l'aide de la console. Le chemin correct est configuré lors de la configuration de SPNEGO.

Configuration des attributs TAI personnalisés :
Avant de commencer

Le support TAI est activé automatiquement lorsque vous activez SPNEGO à l'aide de la console, selon la procédure décrite dans la section «Activation et configuration de l'authentification SPNEGO», à la page 87. Cependant, pour personnaliser les attributs TAI, vous devez modifier le fichier tai.properties.template.

Pourquoi et quand exécuter cette tâche

Consultez le contenu du fichier tai.properties.template dans la section «Attributs de configuration SPNEGO TAI», à la page 88.

Procédure

1. Recherchez le fichier et faites-en une copie de sauvegarde. Le fichier se trouve dans le répertoire par défaut suivant :

   AIX, Linux ou Solaris
   ```
   /opt/IBM/FIM/etc/tai.properties.template
   ```

   Windows
   ```
   C:\Program Files\IBM\FIM\etc\tai.properties.template
   ```
2. Ouvrez le fichier dans un éditeur de texte.
3. Apportez les modifications appropriées pour votre environnement.
4. Enregistrez, puis fermez le fichier.

Configuration des navigateurs pour SPNEGO

Les utilisateurs doivent faire appel à la connexion unique via le bureau pour accéder au serveur Tivoli Federated Identity Manager une fois que l'authentification SPNEGO est configurée.

Avant de commencer

Conditions requises :

- Le navigateur de l'utilisateur reconnaît le serveur Tivoli Federated Identity Manager en tant que *site intranet*.
- Le navigateur de l'utilisateur est activé pour l'authentification intégrée de Windows.

Les instructions de cette procédure sont destinées à Internet Explorer version 6 et ultérieure. Pour les autres types de navigateur, tels que Mozilla, consultez la documentation correspondante.

Pourquoi et quand exécuter cette tâche

En général, la configuration du navigateur pour SPNEGO implique les opérations suivantes :

- Ajoutez dans la liste des sites intranet locaux le nom d'hôte du poste WebSphere Application Server utilisé avec Tivoli Federated Identity Manager Business.
- Vérifiez que l'option d'authentification intégrée de Windows est sélectionnée dans les paramètres de sécurité avancés du navigateur.

Procédure

1. Ajoutez le nom d'hôte :
   a. Démarrez Internet Explorer et cliquez sur **Outils → Options Internet**.
   b. Cliquez sur l'onglet **Sécurité** puis sur **Intranet local**.
   c. Cliquez sur le bouton **Sites**. Assurez-vous que la case **Inclure tous les sites locaux (intranet) non mentionnés dans d'autres zones** est cochée. Cliquez ensuite sur le bouton **Avancé**.
   d. Ajoutez les sites Web de WebSphere Application Server, tels qu'ils sont affichés dans le navigateur, à l'aide de http ou https, en fonction de vos besoins.

      Remarque : Ce nom d'hôte doit correspondre au nom principal configuré pour le fichier de clés.
      Par exemple :

      ```
      http://ibm-fim611-1.fimtest.example.com
      ```

      ```
      https://ibm-fim611-1.fimtest.example.com
      ```
2. Vérifiez que l'authentification intégrée de Windows est activée :
   a. Démarrez Internet Explorer et cliquez sur **Outils → Options Internet**.
   b. Cliquez sur l'onglet **Avancé** et faites défiler la page jusqu'à la section Sécurité.
   c. Assurez-vous que la case **Activer l'authentification intégrée de Windows (nécessite un redémarrage)** est cochée.
   d. Enregistrez les modifications, puis redémarrez le navigateur, si nécessaire.

Serveur point de contact WebSphere pour un fournisseur de services

Si vous devez être le fournisseur de services de votre fédération, vous disposez de plusieurs options pour votre configuration.

Si vous utilisez WebSphere Application Server en tant que serveur point de contact, vous pouvez définir n'importe lequel des types de serveurs suivants pour héberger les applications Web cible auxquelles les utilisateurs accéderont par le biais d'une connexion unique :

- IBM WebSphere Application Server 5.1, 6.0 ou version supérieure (dans la plupart des cas, les applications Web sont hébergées sur une installation de WebSphere Application Server distincte du serveur sur lequel Tivoli Federated Identity Manager est installé. Toutefois, si vous avez installé la version 6.1 de WebSphere Application Server et que cette installation répond aux exigences d'installation de Tivoli Federated Identity Manager ainsi que pour l'hébergement de vos applications Web, vous pouvez utiliser le même serveur à la fois pour Tivoli Federated Identity Manager et pour vos applications).
- Microsoft Internet Information Service 6.0
- IBM HTTP Server 6.1
- Apache HTTP Server 2.0 et 2.2

Si vous sélectionnez un serveur autre que WebSphere Application Server en tant qu'hôte pour vos applications, vous devez installer le plug-in du serveur Web Tivoli Federated Identity Manager sur votre serveur d'applications. La figure suivante montre un exemple d'environnement Tivoli Federated Identity Manager dans lequel les applications sont hébergées par un serveur Web séparé.

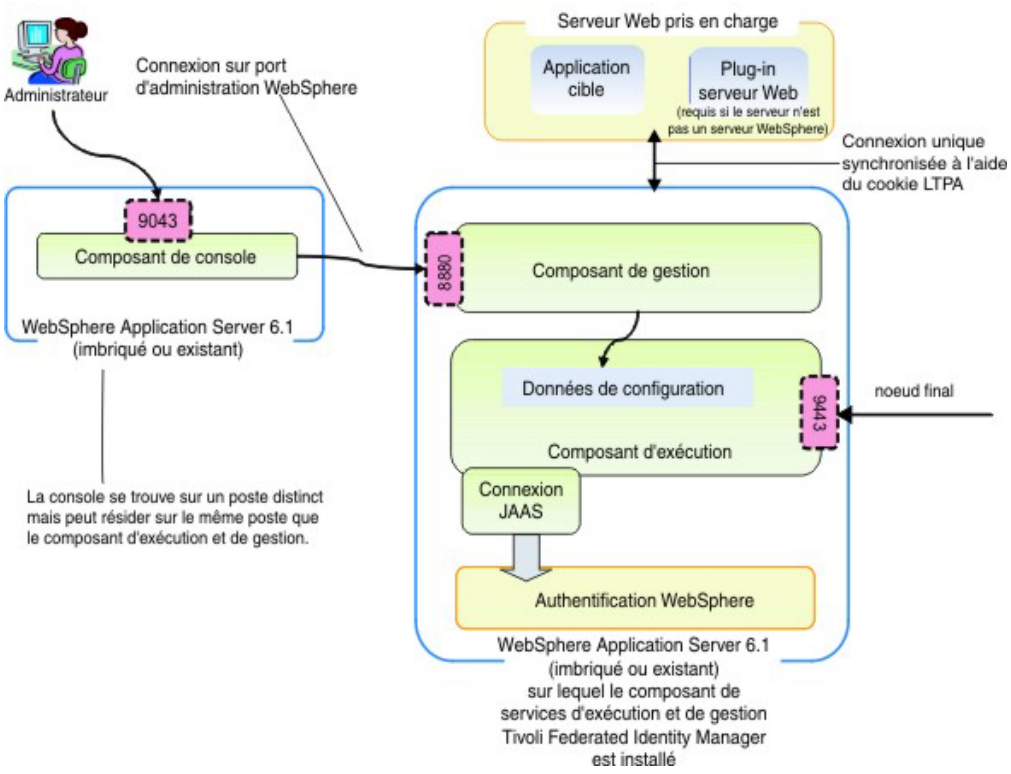


Figure 5. Exemple de Tivoli Federated Identity Manager avec un serveur d'applications Web

Dans la configuration illustrée, l'application cible est hébergée par un serveur distinct du serveur Tivoli Federated Identity Manager. L'utilisateur s'authentifie auprès du fournisseur d'identité, puis les droits d'accès sont transférés du fournisseur d'identité vers Tivoli Federated Identity Manager, où le fournisseur de services valide le jeton et renvoie un cookie LTPA contenant l'identité de l'utilisateur, ainsi que les attributs qui sont éventuellement contenus dans le jeton ou ajoutés par les règles de mappage du fournisseur de services. L'utilisateur est redirigé (par le biais d'un protocole de connexion unique) vers l'application cible sur laquelle le cookie LTPA est transféré du noeud Tivoli Federated Identity Manager vers celui du serveur Web. La clé LTPA doit être partagée entre ces noeuds pour que le cookie soit reconnu.

Si le serveur Web n'est pas un une instance de WebSphere Application Server, le plug-in du serveur Web Tivoli Federated Identity Manager doit être installé sur ce serveur. Le module d'extension extrait les données d'identité et les attributs du cookie LTPA, puis les fournit à l'application cible via un(e) ou plusieurs en-têtes HTTP ou variables de serveurs.

Exigences liées à l'environnement

Les applications cible peuvent être hébergées par l'un des serveurs suivants :

- WebSphere Application Server 5.1, 6.0 ou version supérieure
- Microsoft Internet Information Server 6.0
- IBM HTTP Server 6.1
- Apache HTTP Server 2.0 et 2.2

Avertissement : Si vous choisissez d'héberger les applications cible sur un serveur autre que WebSphere Application Server, vous devez installer le plug-in du serveur Web Tivoli Federated Identity Manager sur ce serveur.

- Les applications doivent être capables d'accepter l'identité des utilisateurs au moyen d'un en-tête HTTP ou d'une variable de serveur.
- Un registre d'utilisateurs est requis dans votre environnement à la fois pour votre serveur point de contact et votre serveur d'applications. Les utilisateurs auxquels vous allez fournir les fonctionnalités de connexion unique doivent exister dans les deux registres d'utilisateurs. Si votre application cible est destinée à être hébergée sur un serveur séparé, tel qu'une autre instance de WebSphere Application Server ou un serveur pris en charge doté d'un module d'extension tel qu'un serveur IHS, IIS ou Apache, vous devez également configurer un registre d'utilisateurs pour ce serveur. Sélectionnez un registre d'utilisateurs exploitable par votre serveur point de contact et votre serveur Web afin de réduire le nombre de registres d'utilisateurs que vous devrez gérer dans votre environnement

Exigences applicables aux modules d'extension

Vous devez vous assurer que votre environnement répond aux exigences suivantes :

- Les applications doivent être capables d'accepter l'identité des utilisateurs au moyen d'un en-tête HTTP ou d'une variable de serveur.
- Le nom d'utilisateur utilisé pour chaque connexion unique doit exister à la fois dans le registre d'utilisateurs deWebSphere Application Server (où Tivoli Federated Identity Manager est installé) et dans le registre d'utilisateurs du serveur Web.
- Le serveur Tivoli Federated Identity Manager et le serveur Web doivent figurer dans le même domaine DNS et le cookie LTPA doit être configuré en tant que cookie de domaine.
- Le fichier de clés et le mot de passe LTPA doivent résider à la fois sur le serveur Tivoli Federated Identity Manager et sur le serveur Web sur lequel le module d'extension est installé.

Configuration de WebSphere

Pour configurer le serveur point de contact WebSphere Application Server, reportez-vous à la rubrique «Configuration d'un serveur point de contact WebSphere Application Server (fournisseur de services)».

Configuration d'un serveur point de contact WebSphere Application Server (fournisseur de services)

Si vous utilisez WebSphere Application Server pour votre serveur point de contact doté, vous devez effectuer plusieurs tâches de configuration.

Pourquoi et quand exécuter cette tâche

Avertissement : Avant d'accomplir les tâches décrites dans la présente section, assurez-vous que les paramètres sont corrects en appliquant la procédure «Confirmation des propriétés de sécurité de WebSphere Application Server», à la page 71.

Configuration du cookie LTPA

En général, la connexion unique fédérée n'est disponible que si ces applications partagent un nom de domaine commun avec le noeud final du service d'assertion client du fournisseur de services. Pour vous assurer que vos applications partagent le nom de domaine correct, vous devez configurer le cookie LTPA sous forme de cookie e domaine, à l'aide du domaine de votre noeud final de service d'assertion client.

Procédure

1. Connectez-vous à la console.
2. Cliquez sur **Sécurité → Administration, applications et infrastructure sécurisées → Sécurité Web**.
3. Cliquez sur **connexion unique**.
4. Pour restreindre le cookie LTPA aux sessions SSL, sélectionnez l'option **SSL requis**.
5. Reseignez la zone Nom de domaine. Faites précéder d'un point (.) le nom du domaine. La définition du nom de domaine permet de garantir que le LTPA est mis à la disposition de tous les serveurs Web membres du domaine spécifié.
6. Désélectionnez la case à cocher **Mode d'interopérabilité**. Le mode d'interopérabilité entraîne la création de deux cookies (un cookie LPTA version 1 et un cookie LTPA version 2) dans le navigateur. Le plug-in de serveur Web de Tivoli Federated Identity Manager prend uniquement en charge les cookies LTPA version 2.
7. Cliquez sur **OK**, puis sur **Enregistrer**.

Que faire ensuite

Des informations sur la configuration correcte du domaine peuvent être consultées dans la rubrique relative à la mise en oeuvre d'une connexion unique en vue de minimiser les authentifications utilisateur sur le Web, dans le centre de documentation de WebSphere Application Server 6.1, à l'adresse http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp.

Définition des attributs du jeton LTPA

Par défaut, tous les attributs disponibles sont inclus dans le jeton LTPA. Si vous souhaitez restreindre les attributs à certains attributs spécifiques, vous devez modifier les paramètres de filtrage des attributs sur l'instance WebSphere Application Server.

Pourquoi et quand exécuter cette tâche

Remarque : Votre application cible doit être configurée de manière à utiliser les attributs inclus dans le jeton LTPA. Pour plus d'informations sur les rubriques relatives au développement, consultez les liens aux documents developerWorks sur la page de bienvenue du centre de documentation à l'adresse suivante : http://publib.boulder.ibm.com/infocenter/tiv2help/index.jsp.

Procédure

1. Connectez-vous à la console.
2. Cliquez sur **Sécurité → Sécuriser l'administration, les Applications et les infrastructures**.
3. Développez la liste des rubriques **JAAS (Java Authentication and Authorization Service)**. Puis, cliquez sur **Connexions système** (System logins).

4. Dans le panneau des connexions système JAAS, sélectionnez **FIM_OUTBOUND**.
5. Dans la section Propriétés Supplémentaires du panneau FIM_OUTBOUND, cliquez sur **Modules de connexion JAAS**.
6. Sélectionnez le nom de classe du module de connexion pour le mappage d'attributs avec le point de contact WebSphere.

   ```
   com.tivoli.am.fim.fedmgr2.was.jaas.login.
            WASPocAttributesMapLoginModule
   ```

   La liste des propriétés de configuration s'affiche.

   Remarque : Si vous souhaitez supprimer tous les attributs, cochez la case située en regard de l'option **ssoAttributeNames** et cliquez sur **Supprimer**. Sinon, pour modifier les attributs, exécutez les étapes restantes.
7. Cliquez sur **ssoAttributeNames** pour afficher les propriétés par défaut. Le paramètre **ssoAttributeNames** est configuré par défaut avec la valeur " * " dans la zone **Valeur**, ce qui signifie que tous les attributs doivent être inclus dans le jeton.
8. Si vous souhaitez modifier les attributs, supprimer la valeur " * " et entrez un nom d'attribut, tel que `AuthenticationMethod`, ou plusieurs noms d'attributs tels que `AuthenticationMethod,AuthenticationInstant`. Si vous spécifiez des attributs multiples, séparez-les par une virgule (,).

   Remarque : Les attributs que vous pouvez spécifier dépendent du niveau de personnalisation et de configuration de votre application cible.
9. Cliquez sur **OK**.

Sélection et installation d'un registre d'utilisateurs

Un registre d'utilisateurs est requis si vous utilisez WebSphere Application Server comme serveur point de contact. Le registre d'utilisateurs sert de référentiel pour les informations relatives aux utilisateurs auxquels vous fournissez des fonctionnalités de connexion unique. Il peut également servir de référentiel pour les informations relatives aux utilisateurs d'administration de votre environnement ou vous pouvez choisir de conserver les utilisateurs d'administration dans un registre d'utilisateurs distinct.

Avant de commencer

Dans la mesure où vous utilisez WebSphere Application Server en tant que serveur point de contact, vous pouvez choisir un registre d'utilisateurs à partir de nombreuses options. Reportez-vous au centre de documentation de WebSphere Application Server 6.1 à l'adresse http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp. Recherchez ensuite des informations sur le choix d'un registre d'utilisateurs, en sélectionnant **WebSphere Application Server (Distributed platforms and Windows)** → **Securing applications and their environment** → **Authenticating users** → **Selecting a registry or repository**.

- Si vous utilisez une installation existante de WebSphere Application Server, il se peut qu'un registre d'utilisateurs compatible soit déjà installé et configuré.
- Si vous utilisez une nouvelle installation de la version imbriquée de WebSphere Application Server, vous disposez des options suivantes :
  - Utiliser le domaine de référentiel d'utilisateurs basé sur un fichier, qui a été installé avec la version imbriquée de WebSphere Application Server. L'utilisateur d'administration a été configuré dans ce registre pendant

l'installation. Les autres tâches requises pour l'ajout des utilisateurs de connexion unique sont indiquées ultérieurement dans ce chapitre.

– Utiliser un registre d'utilisateurs différent. Pour plus d'informations sur vos options de registre d'utilisateurs, consultez la documentation de WebSphere Application Server. Ensuite, installez et configurez le registre d'utilisateurs choisi, si vous n'utilisez pas un registre d'utilisateurs déjà existant. Configurez ensuite WebSphere pour utiliser ce registre d'utilisateurs. Voir «Configuration de WebSphere pour l'utilisation du registre d'utilisateurs», à la page 97.

Remarque : Si votre application cible est destinée à être hébergée sur un serveur séparé, tel qu'une autre instance de WebSphere Application Server ou un serveur pris en charge doté d'un module d'extension tel qu'un serveur IHS, IIS ou Apache, vous devez également configurer un registre d'utilisateurs pour ce serveur. Sélectionnez un registre d'utilisateurs exploitable par votre serveur point de contact et votre serveur d'applications cible afin de réduire le nombre de registres d'utilisateurs que vous devrez gérer dans votre environnement

Configuration du registre d'utilisateurs

La configuration du registre d'utilisateurs est une étape importante de la configuration globale.

Avant de commencer

Avant de procéder à cette tâche, vous devez sélectionner le registre d'utilisateurs à utiliser et l'installer selon la procédure décrite dans la section «Sélection et installation d'un registre d'utilisateurs», à la page 95.

Pourquoi et quand exécuter cette tâche

Dans votre registre d'utilisateurs, vous allez créer des utilisateurs auxquels fournir des fonctionnalités de connexion unique. Vous pouvez également créer des utilisateurs pour les administrateurs de votre environnement ou choisir de conserver les utilisateurs d'administration dans un référentiel distinct.

Ajout d'utilisateurs de connexion unique :

Dans l'environnement du fournisseur de services, le registre d'utilisateurs est utilisé lors de la création de l'identité locale qui est nécessaire pour que les utilisateurs accèdent à l'application cible. Ajoutez ces utilisateurs dans votre registre d'utilisateurs, à l'aide de la documentation correspondante.

Ajout d'utilisateurs d'administration :

Si vous avez installé la version imbriquée de WebSphere Application Server, un domaine de référentiel d'utilisateurs basé sur un fichier et désigné par *référentiel fédéré* a été configuré pour les utilisateurs d'administration de Tivoli Federated Identity Manager. Si vous préférez gérer les utilisateurs d'administration via le même registre d'utilisateurs que celui dans lequel vos utilisateurs de connexion unique sont configurés, vous devez les ajouter dans ce registre d'utilisateurs.

Avant de commencer

Un utilisateur d'administration a été créé dans le référentiel d'utilisateurs par défaut pendant l'installation de Tivoli Federated Identity Manager.

Pourquoi et quand exécuter cette tâche

Pour ajouter cet utilisateur dans un registre d'utilisateurs différent, procédez comme suit :

Procédure

1. Créez l'utilisateur à l'aide de la documentation de votre registre d'utilisateurs.
2. Suivez les instructions de la section «Configuration de WebSphere pour l'utilisation du registre d'utilisateurs».

Configuration d'une connexion SSL au registre d'utilisateurs :

Après avoir configuré votre registre d'utilisateurs, activez SSL pour protéger la connexion entre SSL et le serveur.

Pourquoi et quand exécuter cette tâche

Pour obtenir des instructions, consultez le centre de documentation de WebSphere Application Server 6.1 à l'adresse http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp. Pour plus d'informations sur la création de connexions SSL, sélectionnez **WebSphere Application Server (Distributed platforms and Windows) → Securing applications and their environment → Securing communications**.

Il peut être également nécessaire de consulter la documentation de votre registre d'utilisateurs.

Exemple

Configuration de WebSphere pour l'utilisation du registre d'utilisateurs

Si vous avez installé la version intégrée de WebSphere Application Server, cela signifie que le référentiel fédéré a été configuré en tant que registre d'utilisateurs. Si vous souhaitez utiliser un registre d'utilisateurs autre que le référentiel fédéré par défaut, vous devez modifier les paramètres de WebSphere Application Server.

Avant de commencer

Avant de poursuivre cette tâche, consultez les informations de la section «Sélection et installation du registre d'utilisateurs», à la page 77. Vérifiez que vous avez sélectionné et installé l'option de registre d'utilisateurs appropriée pour votre environnement.

Pourquoi et quand exécuter cette tâche

Pour permettre à WebSphere d'utiliser votre registre d'utilisateurs, procédez comme suit :

Procédure

1. Connectez-vous à la console. Sélectionnez **Sécurité → Administration, application et infrastructure sécurisées**. L'onglet Configuration s'affiche.
2. Cliquez sur **Assistant de configuration des paramètres de sécurité** pour modifier le registre d'utilisateurs utilisé par le composant d'exécution WebSphere.

3. Le panneau **Spécifier l'étendue de la protection** apparaît. Vérifiez que la case **Activer la sécurité des applications** est cochée. Cliquez sur **Suivant**.
4. Le panneau **Sécuriser l'environnement de traitement des applications** apparaît. Sélectionnez l'option correspondant au registre d'utilisateurs de votre choix :
   - **Référentiels fédérés**
   - **Registre LDAP autonome**
   - **Système d'exploitation local**
   - **Registre personnalisé autonome**
5. Cliquez sur **Suivant**. Le panneau **Configurer le référentiel d'utilisateurs** s'affiche. Indiquez des valeurs pour chaque paramètre de configuration du registre. Pour obtenir une description des zones présentées, consultez l'aide en ligne.
6. Cliquez sur **Suivant** et quittez l'assistant. Sauvegardez les modifications apportées à votre configuration.
7. Arrêtez, puis redémarrez WebSphere Application Server. Vous devez utiliser le nom d'administrateur que vous avez choisi pour vous connecter et effectuer ces modifications.
8. Dans la console, sélectionnez **Tivoli Federated Identity Manager → Gestion de la configuration → Propriétés du domaine**.
9. Dans la section Sécurité WebSphere du panneau, mettez à jour les valeurs suivantes :

   Nom de l'utilisateur d'administration
   Remplacez l'entrée existante par le nom de compte administrateur LDAP entré à l'étape précédente. Par exemple, `ldapadmin`

   Mot de passe d'administration
   Entrez le mot de passe de l'administrateur LDAP.
10. Sauvegardez les modifications.
11. Arrêtez WebSphere Application Server.
12. Redémarrez WebSphere Application Server.

Exportation de la clé LTPA à partir du serveur point de contact

Si vous envisagez d'utiliser votre serveur point de contact WebSphere Application Server avec une application cible hébergée par un autre système WebSphere Application Server ou par un serveur sur lequel un plug-in de Tivoli Federated Identity Manager est installé, vous devez exporter votre clé LTPA pour la partager avec l'application cible.

Avant de commencer

Vérifiez que les serveurs d'exportation et d'importation de la clé ont les mêmes paramètres de date et d'heure. Si la date ou l'heure est différente, le serveur d'importation risque d'interpréter à tort la clé comme étant arrivée à expiration.

Procédure

1. Connectez-vous à la console.
2. Cliquez sur **Sécurité → Administration, applications et infrastructure sécurisées → Mécanismes d'authentification et expiration**.
3. Dans les zones Mot de passe et Confirmer le mot de passe, entrez le mot de passe utilisé pour chiffrer la clé LTPA. Retenez-le afin de pouvoir l'utiliser plus tard pour importer la clé sur l'autre serveur.

4. Dans la zone **Nom complet du fichier de clés**, indiquez le chemin d'accès complet de l'emplacement dans lequel vous souhaitez enregistrer la clé LTPA exportée. Utilisez le nom de fichier de clés par défaut, `ltpa.keys`. Vous devez posséder un droit d'accès en écriture à ce fichier.
5. Cliquez sur **Exporter les clés** pour exporter la clé vers l'emplacement indiqué dans la zone **Nom complet du fichier de clés**.
6. Indiquez l'**ID de serveur interne** utilisé pour la communication interprocessus entre les serveurs. L'ID de serveur est protégé à l'aide d'un jeton LTPA lorsqu'il est envoyé par un système distant. Par défaut, il correspond au nom de cellule.
7. Cliquez sur **OK**.

Que faire ensuite

Une fois la clé exportée, vous devez la partager avec votre application cible. Reportez-vous aux instructions appropriées :

- Si vous utilisez une instance séparée de WebSphere Application Server, reportez-vous à la rubrique «Importation de la clé LTPA dans WebSphere Application Server», à la page 106.
- Si vous utilisez un serveur Apache, IHS ou IIS, reportez-vous à la rubrique «Configuration de la clé LTPA sur le serveur Web», à la page 109.

Chapitre 10. Configuration d'un plug-in de serveur Web

L'installation du plug-in de serveur Web est requise sur votre serveur Web *uniquement* s'il s'agit d'une instance prise en charge autre que WebSphere Application Server. La principale fonction du module d'extension consiste à extraire les informations d'identité des utilisateurs à parti du cookie LTPA contenu dans une requête Web, afin de mettre ces informations d'identification à la disposition de l'application cible hébergée par le serveur Web, au moyen soit d'en-têtes HTTP, soit de variables de serveur (si celles-ci sont prises en charge par le serveur Web).

Traitement des requêtes Web

Pour vous assurer que vous pouvez configurer de façon appropriée le plug-in du serveur Web et l'utiliser pour intégrer votre application, il est utile de comprendre la manière ont les requêtes Web sont traitées par le module d'extension.

Lorsqu'une requête d'application Web est reçue par le serveur, elle est transmise au module d'extension en vue du traitement, que celui-ci accomplit par les actions suivantes :

1. Extrait l'adresse URL de la requête Web.
2. Extrait de de la requête le cookie du jeton LTPA, le cas échéant.
3. Vérifie sa configuration pour déterminer si la fonctionnalité du plug-in est activée. Si ce n'est pas le cas, le traitement prend fin. Si l'activation est effective, les actions suivantes sont exécutées :
   a. Vérifie si l'adresse URL contenue dans la requête correspond à l'une des adresses URL configurées dans le fichier de configuration du plug-in. Cette possibilité permet d'appliquer un traitement spécifique à des applications également spécifiques.
   b. Identifie la liste des en-têtes HTTP à supprimer de la requête. Le fichier de configuration du plug-in identifie les en-têtes HTTP à éliminer et empêche les attaques consistant pour un client à ajouter de "faux" en-têtes.
   c. Le cookie du jeton LTPA est ensuite examiné et l'une des actions suivantes est appliquée :
      - Si la requête ne contient pas de cookie de jeton LTPA valide, le module d'extension identifie la liste des cookies de session (s'ils existent) qui doivent être éliminés de la requête, d'après la configuration spécifiée dans le fichier de configuration du plug-in. Les cookies sont éliminés uniquement si le cookie de jeton LTPA est manquant, a expiré ou est codé de façon inappropriée. Les cookies de session sont présents uniquement à la suite d'une connexion unique fédérée, qui est indiquée par la présence d'un cookie de jeton LTPA. Un cookie de session sans cookie de jeton LTPA valide implique que le cookie de session n'est plus applicable. Le traitement prend fin.
      - Si la requête contient un cookie de jeton LPTA valide, ce cookie est décodé.

        En cas d'échec du décodage, ou si le jeton LTPA arrive à expiration, aucun traitement supplémentaire n'a lieu. La requête est transmise à l'application Web sans qu'aucun en-tête HTTP ne soit ajouté et la gestion de la condition est transférée à l'application.

Si le décodage du jeton LTPA aboutit, le traitement se poursuit et le module d'extension crée une liste des en-têtes HTTP à définir dans le requête. Celui-ci crée une liste à l'appui de la configuration spécifiée dans le fichier de configuration du plug-in et des valeurs d'attributs LTPA contenues dans le jeton. Pour plus d'informations sur l'attribut LTPA et le processus de mappage d'en-tête HTTP, consultez la rubrique «Mappage d'attribut LTPA avec un en-tête HTTP».

Remarque : Les jetons LTPA décodés sont sauvegardés dans une mémoire cache interne jusqu'à épuisement de leur délai d'expiration. Lorsqu'une requête est reçue, le module d'extension recherche la présence d'un jeton valide dans la mémoire cache. Si tel est le cas, celui-ci est réutilisé. Sinon, le jeton est décodé et ajouté en mémoire cache. La taille de la mémoire cache est limitée par le nombre d'entrées qu'elle comporte. Vous pouvez définir sa taille dans le fichier de configuration du plug-in.

d. Au cours de l'étape de traitement finale, le plug-in crée une liste des variables et valeurs du serveur, si celles-ci sont présentes et prises en charge par le serveur Web.

Remarque : L'usage des variables de serveur n'est pas pris en charge dans les environnements IIS.

4. La requête Web terminée est ensuite envoyée à l'application Web pour traitement.

Mappage d'attribut LTPA avec un en-tête HTTP

Pour pouvoir mapper les informations de cookie LTPA avec un en-tête HTTP, le module d'extension s'appuie sur un fichier de configuration spécial (itfimwebpi.xml) chargé de créer, puis modifier ou éliminer les en-têtes HTTP dans la requête HTTP finale qui est envoyée à l'application cible. La figure suivante illustre la façon dont le fichier de configuration est utilisé pour déterminer la requête HTTP finale. Il est à noter que cette figure est valable uniquement à titre d'exemple. Les attributs et en-têtes LTPA sont spécifiques à chaque application qui est exploitée dans un environnement.

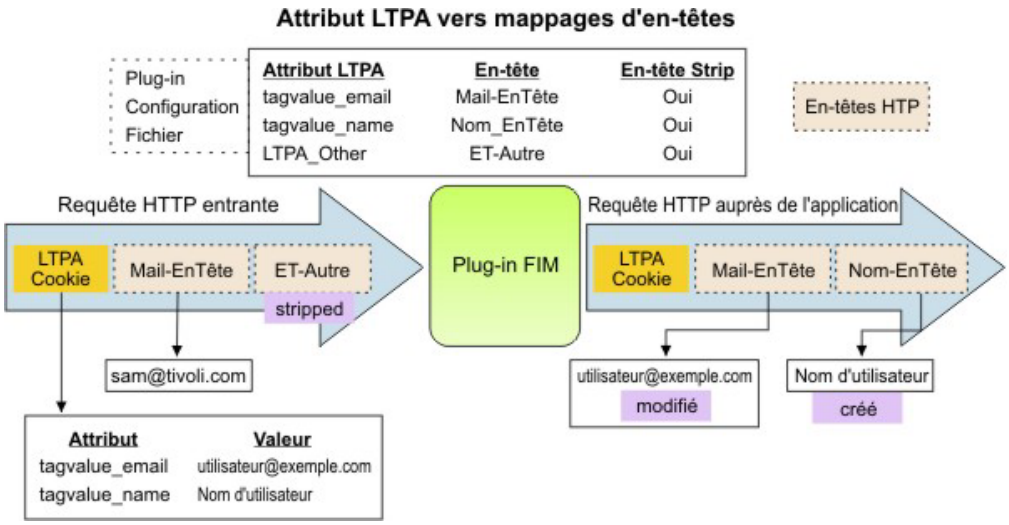


Figure 6. Exemple de mappage entre un attribut LPTA et un en-tête HTTP

1. La requête d'entrée HTTP de la figure précédente contient :

- Le cookie LTPA créé par le fournisseur de services configuré dans Tivoli Federated Identity Manager
- deux en-têtes HTTP : 'Header-mail' et 'Other'.

2. Les instructions du fichier de configuration de plug-in pour le mappage des attributs LTPA se présentent comme suit :
   - Attribut LTPA 'tagvalue_email' → Header-mail (éliminé si absent de LTPA)
   - Attribut LTPA 'tagvalue_name' → Header-Name (éliminé si absent de LTPA)
   - Attribut LTPA 'LTPA_Other' → Hdr-Other (éliminé si absent de LTPA)

   Pour tous ces en-têtes, si l'attribut LTPA correspondant n'existe pas, il convient que tout en-tête contenant le nom configuré soit éliminé. A titre d'exemple, dans la figure, la valeur LTPA 'LTPA_Other' est absente, aussi l'en-tête d'entrée HTTP 'Hdr-Other' est-il éliminé. La valeur LTPA 'tagvalue_email' est présente, donc l'en-tête 'Header_mail' existant est modifié de manière à contenir la valeur issue du cookie LTPA : "user@example.com". La valeur LTPA 'tagvalue_name' est présente, donc l'en-tête 'Header_Name' est créé avec la valeur issue du cookie LTPA : "User_Name". Les en-têtes non listés dans le fichier de configuration restent inchangés. Si un cookie LTPA est absent, tous les en-têtes comportant la mention "strip=yes" sont supprimés.

Le module d'extension offre également la possibilité d'éliminer des cookies si le cookie LTPA n'est pas présenté, ainsi que la possibilité de mapper des attributs LTPA avec des variables de serveur, mais ces scénarios ne sont pas illustrés sur la figure.

Pour plus d'informations sur la configuration de votre environnement de fournisseur de services, ainsi que sur le fichier de configuration du plug-in, voir «Configuration des composants du fournisseur de services».

Configuration des composants du fournisseur de services

Si vous devez être le fournisseur de services partenaire et que vous utilisez WebSphere Application Server en tant que serveur point de contact, vous devez effectuer des tâches de configuration spécifiques avant de créer une fédération. Des tâches de configuration spécifiques sont également requises sur le serveur destiné à héberger votre application cible.

Pourquoi et quand exécuter cette tâche

Exécutez les tâches suivantes :

1. Configurez le serveur d'applications destiné à héberger vos applications cible, comme décrit à la rubrique «Configuration de votre serveur Web».
2. Configurez votre application cible comme décrit à la rubrique «Configuration de l'application cible», à la page 113.

Configuration de votre serveur Web

Vous disposez de plusieurs options, suivant le type de serveurs que vous utilisez pour héberger les applications auxquelles les utilisateurs accèdent par le biais d'une connexion unique (ces applications sont appelées *applications cible* car elles sont ciblées par la demande de connexion unique).

Pourquoi et quand exécuter cette tâche

Les options applicables aux serveurs de votre environnement Tivoli Federated Identity Manager incluent :

- IBM WebSphere Application Server 5.1, 6.0 ou version supérieure

  Remarque : Les serveurs décrits ici sont généralement dédiés à l'hébergement de l'application cible. Toutefois, il vous est également possible d'héberger votre application cible sur la même instance de WebSphere Application Server que celle sur laquelle vous avez installé le composant d'exécution de Tivoli Federated Identity Manager. L'installation de votre composant d'exécution doit avoir été effectuée sur l'une des versions suivantes de WebSphere :

  – WebSphere Application Server version 6.1

  – La version intégrée de WebSphere Application Server 6.1, fournie avec Tivoli Federated Identity Manager
- Microsoft Internet Information Service 6.0
- IBM HTTP Server 6.1
- Apache HTTP Server 2.0 ou 2.2

Lors de la configuration de votre serveur, assurez-vous que l'environnement de Tivoli Federated Identity et le serveur Web se trouvent dans le même domaine DNS, afin de permettre le transfert du cookie LTPA entre ces deux composants.

Pour configurer le serveur Web de sorte qu'il puisse être utilisé avec l'environnement Tivoli Federated Identity Manager, accomplissez les tâches suivantes :

Procédure

1. Sélectionnez et installez un registre d'utilisateurs pour le serveur, comme décrit à la rubrique «Sélection et installation d'un registre d'utilisateurs».
2. Configurez une connexion SSL au registre d'utilisateurs, comme décrit à la rubrique «Configuration du registre d'utilisateurs pour l'application cible», à la page 105.
3. «Configuration d'une connexion SSL au registre d'utilisateurs», à la page 105
4. Si votre application cible est hébergée par une instance de WebSphere Application Server distincte du serveur sur lequel Tivoli Federated Identity Manager est installé, exécutez la procédure indiquée à la rubrique «Configuration d'une instance séparée de WebSphere Application Server pour l'hébergement d'applications», à la page 106.
5. Si votre application cible est destinée à être hébergée sur un serveur IIS, IHS ou Apache, exécutez la procédure indiquée à la rubrique «Configuration d'un serveur IIS, IHS ou Apache en vue d'héberger l'application», à la page 109.

Sélection et installation d'un registre d'utilisateurs

Un registre d'utilisateurs est requis dans votre environnement à la fois pour votre serveur point de contact et votre serveur d'applications. Les utilisateurs auxquels vous allez fournir les fonctionnalités de connexion unique doivent exister dans les deux registres d'utilisateurs.

Avant de commencer

Dans la plupart des cas, il est souhaitable que votre serveur d'applications exploite le même registre d'utilisateurs que celui que vous avez configuré pour votre

serveur point de contact. Si vous exploitez le même registre d'utilisateurs, assurez-vous qu'il est compatible à la fois avec le serveur point de contact et le serveur d'applications.

Toutefois, si vous exploitez un registre d'utilisateurs distinct, assurez-vous que celui-ci répond aux exigences applicables au serveur hébergeant votre application. Pour plus d'informations, reportez-vous à la documentation de votre serveur. Si, par exemple, vous hébergez votre application sur WebSphere Application Server, consultez la bibliothèque de WebSphere Application Server et recherchez le centre de documentation de la version que vous utilisez : http://www.ibm.com/software/webservers/appserv/was/library/. Sur le centre de documentation approprié, recherchez les rubriques concernant la configuration d'un registre d'utilisateurs.

Configuration du registre d'utilisateurs pour l'application cible

La configuration du registre d'utilisateurs est une étape importante de la configuration globale.

Avant de commencer

Avant de procéder à cette tâche, vous devez sélectionner le registre d'utilisateurs à utiliser et l'installer selon la procédure décrite dans la section «Sélection et installation d'un registre d'utilisateurs», à la page 104.

Pourquoi et quand exécuter cette tâche

Si vous utilisez le même registre d'utilisateurs que celui que vous avez configuré sur le serveur point de contact, aucune configuration supplémentaire du registre n'est nécessaire. Toutefois, si vous utilisez un registre séparé, créez des utilisateurs auxquels fournir des fonctionnalités de connexion unique. Il peut s'agit ici des mêmes utilisateurs que ceux que vous avez définis dans le registre du serveur point de contact. Pour plus d'informations sur l'ajout d'utilisateurs, reportez-vous à la documentation relative à votre registre d'utilisateurs.

Configuration d'une connexion SSL au registre d'utilisateurs

Après avoir configuré votre registre d'utilisateurs, activez SSL pour protéger la connexion entre SSL et le serveur.

Pourquoi et quand exécuter cette tâche

Si vous utilisez le même registre d'utilisateurs pour votre serveur point de contact que pour le serveur d'applications, il est possible que vous ayez déjà effectué cette tâche. Si vous utilisez un registre d'utilisateurs séparé, reportez-vous à la documentation relative à ce registre d'utilisateurs pour plus d'informations sur la configuration SSL.

Que faire ensuite

Une fois que vous avez configuré SSL, poursuivez avec les étapes appropriées pour le serveur sur lequel seront hébergées vos applications cible :

- «Configuration d'une instance séparée de WebSphere Application Server pour l'hébergement d'applications», à la page 106
- «Configuration d'un serveur IIS, IHS ou Apache en vue d'héberger l'application», à la page 109

Configuration d'une instance séparée de WebSphere Application Server pour l'hébergement d'applications

Un environnement Tivoli Federated Identity Manager vous permet d'héberger vos applications cible sur la même instance de WebSphere Application Server que celle qui sert de serveur point de contact, ou sur une instance distincte de WebSphere Application Server.

Pourquoi et quand exécuter cette tâche

Pour configurer une instance séparée de WebSphere Application Server afin qu'elle puisse héberger les applications hôtes auxquelles accèdent les utilisateurs par le biais d'une connexion unique, procédez comme suit :

Procédure

1. Importez la clé LTPA depuis le serveur point de contact WebSphere Application Server, comme décrit à la rubrique «Importation de la clé LTPA dans WebSphere Application Server».
2. Désactivez la génération automatique des clés LTPA, comme décrit à la rubrique «Désactivation de la génération automatique d'une clé LTPA», à la page 107.
3. Configurez WebSphere Application Server en vue d'utiliser le registre d'utilisateurs, comme décrit à la rubrique «Configuration de WebSphere pour l'utilisation du registre d'utilisateurs», à la page 107.

Importation de la clé LTPA dans WebSphere Application Server

Si votre application cible est hébergée sur un serveur WebSphere Application Server distinct de votre serveur point de contact WebSphere, vous devez importer la clé LTPA sur le serveur d'applications cible à partir du serveur point de contact.

Avant de commencer

Avant de commencer cette tâche, vous devez exécuter la procédure suivante :

- Vérifiez que l'heure des serveurs est synchronisée.
- Copiez les clés LTPA de l'emplacement où vous les aviez exportées vers un emplacement de votre serveur d'applications cible.
- Procurez-vous le mot de passe des clés LTPA. Un mot de passe a été associé aux clés lors de leur exportation du serveur point de contact WebSphere.

Procédure

1. Connectez-vous à la console du *serveur d'applications cible*. Ne vous connectez pas à votre console Tivoli Federated Identity Manager pour exécuter cette procédure.
2. Cliquez sur **Sécurité → Administration, applications et infrastructure sécurisées → Mécanismes d'authentification et expiration**.
3. Dans les zones **Mot de passe** et **Confirmer**, entrez le mot de passe utilisé pour chiffrer les clés LTPA. Ce mot de passe doit correspondre à celui qui a été utilisé lors de l'exportation des clés.
4. Dans la zone **Nom complet du fichier de clés**, indiquez le chemin d'accès complet de l'emplacement des clés LTPA. Vous devez posséder un droit d'accès en écriture à ce fichier.
5. Cliquez sur **Importer les clés** pour importer les clés.

6. Cliquez sur **OK**, puis sur **Enregistrer** pour enregistrer les modifications dans la configuration principale.

Que faire ensuite

Ensuite, désactivez la génération automatique des clés LTPA sur le serveur d'applications cible, comme décrit à la rubrique «Désactivation de la génération automatique d'une clé LTPA».

Désactivation de la génération automatique d'une clé LTPA

Par défaut, WebSphere Application Server génère automatiquement une clé LTPA. Toutefois, si vous utilisez une instance de WebSphere Application Server autre que le serveur point de contact pour héberger votre application cible, vous devez utiliser la clé LTPA du serveur point de contact sur votre serveur d'applications. Vous devez donc désactiver la génération automatique de clé afin d'éviter tout conflit.

Avant de commencer

Pour exécuter cette tâche, vous devez connaître le nom du jeu de clés et la portée de la gestion dans laquelle ce jeu a été défini.

Procédure

1. Connectez-vous à la console du *serveur d'applications cible*. Ne vous connectez pas à votre console Tivoli Federated Identity Manager pour exécuter cette procédure.
2. Cliquez sur **Sécurité → Certificat SSL et gestion des clés → Gérer les configurations de sécurité des noeuds finals**.
3. Développez l'arborescence de la portée de gestion entrante et sortante qui contient le jeu de clés, puis cliquez sur le lien de la portée.
4. Sous l'option Articles liés, cliquez sur **Jeux de clés**.
5. Cliquez sur le jeu de clés que vous souhaitez désactiver.
6. Effacez la case à cocher **Générer les clés automatiquement**.
7. Cliquez sur **OK**, puis sur **Enregistrer** pour enregistrer les modifications dans la configuration principale.

Que faire ensuite

Poursuivez avec les étapes indiquées à la section «Configuration de WebSphere pour l'utilisation du registre d'utilisateurs».

Configuration de WebSphere pour l'utilisation du registre d'utilisateurs

Assurez-vous que l'instance de WebSphere Application Server que vous utilisez pour héberger votre application ciblé est configurée pour prendre en compte le registre d'utilisateurs que vous avez sélectionné et installé.

Avant de commencer

Avant de poursuivre cette tâche, consultez les informations de la section «Sélection et installation du registre d'utilisateurs», à la page 77. Vérifiez que vous avez sélectionné et installé l'option de registre d'utilisateurs appropriée pour votre environnement.

Pourquoi et quand exécuter cette tâche

Pour permettre à WebSphere d'utiliser votre registre d'utilisateurs, procédez comme suit :

Procédure

1. Connectez-vous à la console *de votre application cible*. Ne vous connectez pas à votre console Tivoli Federated Identity Manager pour exécuter cette procédure.
2. Sélectionnez **Sécurité → Administration, application et infrastructure sécurisées**. L'onglet Configuration s'affiche.
3. Cliquez sur **Assistant de configuration des paramètres de sécurité** pour modifier le registre d'utilisateurs utilisé par le composant d'exécution WebSphere.
4. Le panneau **Spécifier l'étendue de la protection** apparaît. Vérifiez que la case **Activer la sécurité des applications** est cochée. Cliquez sur **Suivant**.
5. Le panneau **Sécuriser l'environnement de traitement des applications** apparaît. Sélectionnez l'option correspondant au registre d'utilisateurs de votre choix :
   - **Référentiels fédérés**
   - **Registre LDAP autonome**
   - **Système d'exploitation local**
   - **Registre personnalisé autonome**
6. Cliquez sur **Suivant**. Le panneau **Configurer le référentiel d'utilisateurs** s'affiche. Indiquez des valeurs pour chaque paramètre de configuration du registre. Pour obtenir une description des zones présentées, consultez l'aide en ligne.
7. Cliquez sur **Suivant** et quittez l'assistant. Sauvegardez les modifications apportées à votre configuration.
8. Arrêtez, puis redémarrez WebSphere Application Server. Vous devez utiliser le nom d'administrateur que vous avez choisi pour vous connecter et effectuer ces modifications.
9. Dans la console, sélectionnez **Tivoli Federated Identity Manager → Gestion de la configuration → Propriétés du domaine**.
10. Dans la section Sécurité WebSphere du panneau, mettez à jour les valeurs suivantes :

    Nom de l'utilisateur d'administration
    Remplacez l'entrée existante par le nom de compte administrateur LDAP entré à l'étape précédente. Par exemple, `ldapadmin`

    Mot de passe d'administration
    Entrez le mot de passe de l'administrateur LDAP.
11. Sauvegardez les modifications.
12. Arrêtez WebSphere Application Server.
13. Redémarrez WebSphere Application Server.

Que faire ensuite

Une fois terminé, poursuivez en sélectionnant l'étape appropriée selon votre environnement:

- Si vous prévoyez d'héberger des applications sur un serveur IHS, IIS ou Apache, passez à l'étape «Configuration d'un serveur IIS, IHS ou Apache en vue d'héberger l'application».
- Si vous prévoyez d'héberger des applications uniquement sur votre serveur WebSphere, la configuration est terminée. Poursuivez vers l'étape de configuration des applications cible à la rubrique «Configuration de l'application cible», à la page 113.

Configuration d'un serveur IIS, IHS ou Apache en vue d'héberger l'application

Si vos applications cible sont destinées à être hébergées sur un serveur Microsoft Internet Information Services, une instance IBM HTTP Server ou une instance Apache HTTP Server, vous devez accomplir des tâches de configuration spécifiques.

Avant de commencer

Avant de poursuivre ces tâches, vous devez avoir procédé à l'installation du module d'extension (plug-in).

Assurez-vous que :

- Le plug-in est installé sur le serveur qui héberge l'application cible.
- Le serveur se trouve sur le même domaine que le serveur Tivoli Federated Identity Manager.

Puis, assurez-vous d'avoir exécuté les étapes de la section «Configuration de votre serveur Web», à la page 103, notamment :

- «Sélection et installation d'un registre d'utilisateurs», à la page 104
- «Configuration du registre d'utilisateurs pour l'application cible», à la page 105
- «Configuration d'une connexion SSL au registre d'utilisateurs», à la page 105

Pourquoi et quand exécuter cette tâche

Pour préparer votre environnement de plug-in, procédez comme suit :

Procédure

1. Copiez la clé LTPA sur votre serveur, en suivant la procédure décrite dans «Configuration de la clé LTPA sur le serveur Web».
2. Créez le fichier de configuration du plug-in, selon la procédure décrite dans la section «Création du fichier de configuration de plug-ins», à la page 110.
3. Copiez le fichier de configuration du plug-in sur le serveur, en suivant la procédure décrite dans «Copie de la configuration d'un plug-in sur le serveur», à la page 111.

Configuration de la clé LTPA sur le serveur Web

La clé LTPA utilisée par WebSphere Application Server sur votre serveur point de contact doit être partagée par le serveur sur lequel le plug-in est installé.

Avant de commencer

Avant de poursuivre avec la procédure de copie de la clé LTPA sur votre serveur, vérifiez que vous avez exécuté les tâches suivantes :

- Installé le module d'extension sur le serveur Web.

- Complété la configuration de votre serveur point de contact comme décrit à la rubrique «Configuration d'un serveur point de contact WebSphere Application Server (fournisseur de services)», à la page 93.
- Exporté les clés LTPA depuis votre serveur point de contact, en suivant la procédure décrite dans «Exportation de la clé LTPA à partir du serveur point de contact», à la page 98.
- Vérifié la synchronisation de la date et de l'heure du serveur point de contact et du serveur sur lequel vous copiez la clé LTPA.

Procédure

1. Copiez la clé LTPA, normalement nommée `ltpa.keys`, à partir de l'emplacement dans lequel vous l'avez exportée.
2. Collez-la dans le répertoire webpi du serveur d'applications. Par exemple :

   Sur un serveur IHS ou Apache :
   `/opt/IBM/FIM/webpi/etc`

   Sur un serveur IIS :
   `C:\Program Files\IBM\FIM\webpi\etc`

Que faire ensuite

Passez à l'étape «Création du fichier de configuration de plug-ins».

Création du fichier de configuration de plug-ins

Après avoir installé le module d'extension et préparé votre environnement pour l'utilisation de celui-ci, vous devez le configurer au moyen des informations spécifiques relatives aux applications Web auxquelles les utilisateurs accéderont par le biais d'une connexion unique.

Avant de commencer

Pour exécuter cette tâche, vous devez disposer des informations suivantes :

- Le mot de passe utilisé pour chiffrer la clé en vue de son exportation.
- Le nom et l'adresse URL de chaque application cible hébergée par ce serveur.
- Les mappages corrects de l'en-tête HTTP et de l'attribut LTPA de votre environnement. Vous devez savoir quel attribut LTPA vous souhaitez mapper avec quel en-tête HTTP ou quelle variable de serveur. L'en-tête HTTP et les variables de serveur correspondent aux valeurs requises par l'application cible.
- La liste des cookies à supprimer si le cookie LTPA est absent ou non valide, ce qui indique généralement qu'il ne s'agit pas d'un utilisateur fédéré disposant d'une connexion unique.
- La liste des mappages entre les noms de variables de serveur et des noms d'attributs de jeton LTPA. Les variables de serveur peuvent être utilisées à la place des en-têtes HTTP pour présenter les attributs LTPA à l'application.

  Remarque : Le plug-in IIS ne prend pas en charge l'utilisation de variables de serveur.

Pour plus d'informations sur l'en-tête HTTP et les mappages d'attributs LTPA, ainsi que le mode de fonctionnement du plug-in dans l'environnement, consultez le Chapitre 10, «Configuration d'un plug-in de serveur Web», à la page 101.

Procédure

1. Connectez-vous à la console.

2. Cliquez sur **Tivoli Federated Identity Manager → Gestion de la configuration → Configuration du plug-in de serveur Web**. Le panneau Configuration de la connexion unique du plug-in de serveur Web s'affiche.
3. Entrez les informations requises pour votre serveur dans les sections **Configuration de la connexion unique du plug-in de serveur Web** et **Configuration de la consignation du plug-in de serveur Web**. Pour la description des zones, voir l'aide en ligne. **Remarque :** Assurez-vous que le mot de passe LTPA spécifié dans la zone correspond à celui que vous avez créé lors de l'exportation du fichier ltpa.keys. ne fois que vous avez renseigné toutes les zones, cliquez sur **Enregistrer**.
4. Dans **Configuration des applications du plug-in de serveur Web**, définissez une application pour la configuration de connexion unique en cliquant sur **Créer**. Le panneau Propriétés de l'application s'affiche.
   a. Entrez les informations relatives à l'application à laquelle vos utilisateurs disposant d'une connexion unique peuvent accéder.
   b. Cliquez sur **Appliquer**.
   c. Cliquez sur **Mappages de l'en-tête HTTP à l'attribut LTPA**.
   d. Pour accepter les paramètres par défaut, cliquez sur **Appliquer**. Pour les modifier, cliquez sur **Créer**.
   e. Une fois les zones de ce panneau remplies, cliquez sur **Appliquer**.
   f. Cliquez sur **Cookies client à supprimer**.
   g. Pour accepter les paramètres par défaut, cliquez sur **Appliquer**. Pour les modifier, cliquez sur **Créer**.
   h. Une fois les zones de ce panneau remplies, cliquez sur **Appliquer**.
   i. Cliquez sur **Mappages des variables de serveur à l'attribut LTPA**.
   j. Pour accepter les paramètres par défaut, cliquez sur **Appliquer**. Pour les modifier, cliquez sur **Créer**.
   k. Une fois les zones de ce panneau remplies, exécutez l'une des actions ci-dessous :
      - Pour ajouter d'autres applications, cliquez sur **Appliquer**, puis répétez la procédure précédente pour chaque nouvelle application.
      - Si vous avez terminé l'ajout de l'application au serveur, cliquez sur **OK**.
5. Cliquez sur **Sauvegarder**.
6. Cliquez sur **Exporter le fichier de configuration du plug-in de serveur Web**. Ensuite, procédez comme suit :
   a. Cliquez sur **Enregistrer** dans la fenêtre en incrustation pour sauvegarder la configuration dans un fichier nommé `itfimwebpi.xml`.
   b. Sélectionnez le répertoire d'installation du plug-in de serveur Web. Par exemple, enregistrez le fichier `itfimwebpi.xml` sous `/opt/IBM/FIM/webpi/etc`.

Que faire ensuite

Passez à l'étape «Copie de la configuration d'un plug-in sur le serveur».

Copie de la configuration d'un plug-in sur le serveur

Après avoir créé le fichier de configuration d'un plug-in, vous devez copier cette configuration sur votre serveur Web.

Procédure

1. Recherchez le fichier de configuration que vous avez créé à l'aide de la procédure décrite dans «Création du fichier de configuration de plug-ins», à la page 110. Le fichier, qui porte le nom `itfimwebpi.xml`, est créé dans le répertoire que vous avez spécifié lors de l'exportation du fichier.
2. Copiez le fichier, puis collez-le dans le répertoire webpi de votre serveur Web :

   Sur un serveur IHS ou Apache :
   ```
   /opt/IBM/FIM/webpi/etc
   ```

   Sur un serveur IIS :
   ```
   C:\Program Files\IBM\FIM\webpi\etc
   ```
3. Redémarrez votre serveur Web pour que les modifications soient prises en compte.

Que faire ensuite

La configuration de votre serveur est terminée. Poursuivez vers l'étape de configuration des applications cible à la rubrique «Configuration de l'application cible», à la page 113.

Vérification de la configuration du module d'extension sur Apache ou IBM HTTP Server

Après avoir configuré le plug-in sur un serveur HTTP Apache ou une instance IBM HTTP Server, vous pouvez vérifier que la configuration a abouti.

Avant de commencer

Avant de poursuivre cette tâche, assurez-vous que vous avez effectué la tâche ci-après :

- «Configuration d'un serveur point de contact WebSphere Application Server (fournisseur de services)», à la page 93
- «Configuration d'un serveur IIS, IHS ou Apache en vue d'héberger l'application», à la page 109

Procédure

1. Sur le serveur, localisez le fichier httpd.conf. L'emplacement de ce fichier dépend de votre installation. Par exemple :

   ```
   /etc/httpd/conf/httpd.conf
   ```
2. Ouvrez le fichier dans un éditeur de texte et recherchez la ligne relative au module d'extension que vous utilisez :

   Apache HTTP Server 2.2 :

   ```
   LoadModule fimwebpi_module /opt/IBM/FIM/webpi/lib/libitfimwebpi-apache22.so
   ```

   Apache HTTP Server 2.0 ou IBM HTTP Server :

   ```
   LoadModule fimwebpi_module /opt/IBM/FIM/webpi/lib/libitfimwebpi-apache20.so
   ```

   Assurez-vous que le module webpi (`libitfimwebpi-apache22.so` ou `libitfimwebpi-apache20.so`) peut accéder en écriture au chemin d'accès du fichier journal définie dans le fichier de configuration de votre plug-in (`itfimwebpi.xml`).

Que faire ensuite

Poursuivez avec les étapes indiquées à la section «Configuration de l'application cible», à la page 113.

Configuration de l'application cible

En tant que fournisseur de services, votre rôle dans la fédération consiste à fournir un service, tel qu'une application Web, à l'utilisateur final.

Pourquoi et quand exécuter cette tâche

Dans le cadre de ce rôle, vous devez vous assurer que l'application (appelée *application cible*) que vous fournissez aux utilisateurs est configurée de façon appropriée pour fonctionner dans l'environnement Tivoli Federated Identity Manager :

- L'application doit être capable d'accepter les informations sur l'identité des utilisateurs au moyen d'en-têtes HTTP ou de variables de serveur.
- L'environnement Tivoli Federated Identity Manager et l'application doivent se trouver dans le même domaine DNS.
- L'application doit être hébergée par un serveur Web pris en charge tel que :
  - Serveur Microsoft Internet Information Services (IIS) 6.0, avec module d'extension Tivoli Federated Identity Manager installé
  - IBM HTTP Server 6.1, avec plug-in Tivoli Federated Identity Manager installé
  - Serveur Apache HTTP 2.0 ou 2.2 avec plug-in Tivoli Federated Identity Manager installé
  - WebSphere Application Server version 5.1
  - WebSphere Application Server version 6.0 ou supérieure

    Remarque : Vous pouvez également définir, en tant qu'hôte des applications cibles, la même instance de WebSphere Application Server que celle sur laquelle vous avez installé le composant d'exécution de Tivoli Federated Identity Manager. Cette version de WebSphere Application Server peut être l'une des suivantes :
    - WebSphere Application Server version 6.1 avec fix pack 15
    - Version intégrée de WebSphere Application Server, fournie avec Tivoli Federated Identity Manager

Pour plus d'informations sur la configuration de votre application cible, reportez-vous à la documentation relative au serveur destiné à héberger l'application. Si, par exemple, vous hébergez l'application cible sur WebSphere Application Server, reportez-vous au centre de documentation relatif à la version de WebSphere Application Server que vous utilisez, en consultation la bibliothèque du site http://www.ibm.com/software/webservers/appserv/was/library/.

Configuration de la connexion pour votre application

Avant d'utiliser Tivoli Federated Identity Manager, vous avez probablement employé une méthode de connexion qui était spécifique à votre application. Par exemple, il est possible que vous ayez fourni à vos utilisateurs une adresse URL qui leur a permis d'accéder à un formulaire de connexion ou que vous ayez demandé l'authentification client. Dans votre environnement Tivoli Federated Identity Manager, votre fournisseur d'identité partenaire sera responsable de l'authentification des utilisateurs. Par conséquent, en fonction de la configuration de votre fédération, il est probablement nécessaire d'acheminer vos utilisateurs vers une nouvelle adresse URL (comme celle hébergée par votre fournisseur d'identité partenaire) ou de les réacheminer à partir de votre site vers la méthode de connexion appropriée utilisée par votre fournisseur d'identité partenaire.

Pourquoi et quand exécuter cette tâche

Discutez avec votre fournisseur d'identité partenaire de la configuration de connexion requise. Assurez-vous ensuite que votre environnement est configuré de sorte que les utilisateurs soient envoyés à l'emplacement de connexion approprié.

Instructions destinées aux utilisateurs pour l'activation des cookies

Les utilisateurs doivent activer des cookies dans leurs navigateurs lors de l'utilisation de la connexion unique à un fournisseur de services qui utilise WebSphere Application Server comme serveur point de contact.

Pourquoi et quand exécuter cette tâche

Conseillez aux utilisateurs de suivre les instructions relatives à l'activation des cookies pour leurs navigateurs.

Chapitre 11. Configuration de la base de données de service d'alias

SAML 2.0 prend en charge l'usage d'identificateurs (ou alias) pour la communication des identités d'utilisateurs entre les partenaires. Les alias ont pour rôle d'élever le niveau de confidentialité dont bénéficie un utilisateur lorsqu'il accède aux ressources d'un fournisseur de services. Lorsque des alias sont utilisés, un identificateur reconnu à la fois par le fournisseur d'identité et le fournisseur de services est envoyé à la place du nom de compte effectif de l'utilisateur. La création et l'enregistrement des alias a lieu durant l'opération d'association des comptes (fédération). Une fois l'association de compte effectuée, l'alias est inscrit dans tous les messages échangés entre les partenaires. Un alias différent est utilisé pour chaque partenaire. De plus, l'alias utilisé dans une direction (par exemple du fournisseur d'identité vers le fournisseur de services) peut être différent de celui qui est utilisé dans la direction opposée (du fournisseur de services vers le fournisseur d'identité). L'utilisation des alias est optionnelle dans SAML 2.0.

Pourquoi et quand exécuter cette tâche

Dans la configuration par défaut du service d'alias, les ID utilisés sont persistants.

Un service de Tivoli Federated Identity Manager, appelé *service d'alias*, génère de nouveaux alias, associe des alias avec des utilisateurs locaux et effectue des mappages bidirectionnels entre alias et utilisateurs.

La plupart des alias sont persistants et doivent être conservés pendant une durée prolongée. L'utilisation de certains types de base de données est donc nécessaire pour les stocker. Vous avez deux options pour le type de base de données à utiliser :

- Une base de données JDBC, telle que la base de données Derby de WebSphere Application Server
- Une base de données LDAP, telle qu'IBM Tivoli Directory Server (composant fourni séparément)

Les tâches nécessaires pour configurer la base de données de votre service d'alias sont variables selon que vous avec installé la version intégrée de WebSphere Application Server, ou que vous utilisez une version existante de WebSphere Application Server avec votre installation du composant d'exécution et de gestion de services de Tivoli Federated Identity Manager.

Version intégrée de WebSphere

Les options pour la base de données sont les suivantes :

- **Base de données JDBC**

  Si vous avez installé la version intégrée de WebSphere Application Server, une base de données JDBC (Cloudscape 10, également appelée Derby) a été configurée sur WebSphere Application Server pour les besoins du stockage des informations d'alias. Aucune configuration supplémentaire de la base de données n'est nécessaire.

- **Base de données LDAP**

  Vous avez la possibilité d'utiliser une base de données LDAP, telle que IBM Tivoli Directory Server, que vous avez achetée, installée et

configurée séparément de Tivoli Federated Identity Manager. Reportez-vous aux informations de la section «Configuration d'une base de données de service d'alias LDAP», à la page 118. Puis, pour pouvoir utiliser la base de données LDAP avec Tivoli Federated Identity Manager, vous devez modifier les paramètres du service d'alias comme décrit à la section «Modification des paramètres du service d'alias», à la page 118.

Version existante de WebSphere Application Server

Les options pour la base de données sont les suivantes :

- **Base de données JDBC**

  Si vous avez installé Tivoli Federated Identity Manager sur une version existante de WebSphere Application Server et que vous souhaitez exploiter une base de données JDBC, vous devez créer et configurer manuellement la base de données ne suivant une procédure similaire à celle décrite ci-dessous pour Cloudscape 10 (Derby). Voir la rubrique «Configuration d'une base de données d'alias JDBC» (comme indiqué précédemment, si vous avez installé la version intégrée de WebSphere Application Server, ces étapes ont déjà été accomplies automatiquement).

- **Base de données LDAP**

  Vous avez la possibilité d'utiliser une base de données LDAP, telle qu'IBM Tivoli Directory Server, que vous avez achetée, installée et configurée séparément de votre installation de Tivoli Federated Identity Manager. Reportez-vous aux informations de la section «Configuration d'une base de données de service d'alias LDAP», à la page 118. Puis, pour pouvoir utiliser la base de données LDAP avec Tivoli Federated Identity Manager, vous devez modifier les paramètres du service d'alias comme décrit à la section «Modification des paramètres du service d'alias», à la page 118.

Configuration d'une base de données d'alias JDBC

Si vous avez installé Tivoli Federated Identity Manager sur une version existante de WebSphere Application Server et que vous souhaitez exploiter une base de données JDBC, vous devez créer et configurer manuellement ces paramètres en suivant la procédure ci-dessous. Si vous avez installé la version intégrée de WebSphere Application Server, ces étapes ont déjà été accomplies automatiquement.

Pourquoi et quand exécuter cette tâche

Les instructions qui suivent expliquent comment créer et utiliser la base de données JDBC Derby fournie avec WebSphere Application Server. La création de la base de données Derby s'effectue via un outil Apache appelé "ij". Celui-ci est mis en oeuvre avec la classe Java org.apache.derby.tools.ij.

Procédure

1. Créez la base de données FIMAliases et importez le schéma :
   a. Ouvrez une invite de commande et démarrez l'outil ij accessible dans le répertoire /derby/bin/embedded dans lequel vous avez installé WebSphere Application Server.

      Sous AIX, HP-UX, Linux ou Solaris, entrez *$was_home*/derby/bin/embedded/ij.sh.

      Sous Windows, entrez *$was_home*/derby/bin/embedded/ij.bat.

b. A partir de la ligne de commande ij, créez la base de données et le schéma en exécutant les commandes suivantes :

```
connect 'jdbc:derby:FIMAliases;create=true';
run '/opt/IBM/FIM/etc/Table.ddl';
quit;
```

Remarque : Le fichier `Table.ddl` se trouve dans le répertoire d'installation de Tivoli Federated Identity Manager. Si vous avez défini un répertoire d'installation différent, spécifiez-le lors de l'exécution de la commande. Sous Windows, le répertoire d'installation par défaut est `C:\Program Files\IBM\FIM`.

2. Vérifiez la base de données et le schéma :
   a. Ouvrez une invite de commande et accédez au répertoire *$was_home*/derby/FIMAliases.
   b. Vérifiez que le fichier SQL de sortie contient le schéma FIMAliases.

      Sous AIX, HP-UX, Linux ou Solaris, entrez :

```
$was_home/derby/bin/embedded/dblook.sh -d jdbc:derby:FIMAliases -o FIMAliase.sql
```

      Sous Windows, entrez :

```
$was_home/derby/bin/embedded/dblook.bat -d jdbc:derby:FIMAliases -o FIMAliases.sql
```

3. Créez le fournisseur JDBC Derby intégré et la source de données associée :
   a. Ouvrez la console d'administration WebSphere et cliquez sur **Ressources → JDBC → Fournisseurs JDBC**.
   b. Cliquez sur **Nouveau**.
   c. Complétez les zones requises comme suit :

      Type de base de données
      Sélectionnez **Derby**.

      Type de fournisseur
      Sélectionnez **Fournisseur JDBC Derby**.

      Type d'implémentation
      Sélectionnez **Source de données du pool de connexions**.

      Nom Spécifiez un nom indiquant le fournisseur JDBC du service d'alias pour Tivoli Federated Identity Manager. Spécifiez par exemple : ITFIM Alias Service JDBC Provider.

   d. Cliquez sur **Suivant**, puis sur **Terminer**.
4. Créez une source de données pour ce fournisseur JDBC :
   a. Ouvrez la console d'administration WebSphere et cliquez sur **Ressources → JDBC → fournisseurs JDBC → ITFIM Alias Service JDBC Provider → Sources de données → Nouveau**.
   b. Complétez les zones requises comme suit :

      Nom de la source de base de données
      Entrez un nom identifiant la source de données, tel que `ITFIM Alias Service Datasource`.

      Nom JNDI
      Entrez `jdbc/IdServiceJdbc`.

      Avertissement : Spécifiez ce nom exactement comme indiqué, afin que mappages entre le service d'alias et la source de données s'établissent automatiquement.

   c. Cliquez sur **Suivant**.

d. Indiquez un nom pour la base de données, tel que `FIMAliases`.
e. Cliquez sur **Suivant**, puis sur **Terminer**.

5. Pour vérifier la connexion à la base de données, sélectionnez la source de données que vous avez configurée et cliquez sur **Test de la connexion**.

Modification des paramètres du service d'alias

Pourquoi et quand exécuter cette tâche

Pour modifier la configuration de la base de données de l'identificateur de noms, procédez comme suit :

Procédure

1. Connectez-vous à la console, puis cliquez sur **Tivoli Federated Identity Manager → Gestion de la configuration → Paramètres du service d'alias**. Le portlet Paramètres du service d'alias s'affiche.
2. Sélectionnez **Fournisseur et source de données JDBC**

   Utilisez cette option si vous envisagez de stocker les informations relatives à l'identificateur de nom dans une base de données JDBC.
3. Cliquez sur **Appliquer**, puis sur **OK**.

Configuration d'une base de données de service d'alias LDAP

Si vous installez Tivoli Federated Identity Manager avec la version intégrée de WebSphere, une base de données JDBC constitue l'option de base de données par défaut pour le service d'alias dans Tivoli Federated Identity Manager. Toutefois, vous pouvez choisir de la remplacer par une base de données LDAP.

Avant de commencer

Si vous installez Tivoli Federated Identity Manager avec un déploiement WebSphere existant, il se peut qu'une base de données LDAP soit déjà utilisée en tant que registre d'utilisateurs. Lors de l'utilisation de WebSEAL en tant que serveur point de contact, l'installation a lieu dans un environnement qui inclut Tivoli Access Manager. Le déploiement LDAP effectué le plus couramment avec Tivoli Access Manager est IBM Tivoli Directory Server.

Le service d'alias Tivoli Federated Identity Manager stocke les informations relatives aux alias dans un registre d'utilisateurs. Le service d'alias prend en charge les registres d'utilisateurs suivants :

- IBM Tivoli Directory Server
- Sun ONE

Remarque :

Vous pouvez développer votre propre service d'alias en vue de l'utiliser avec d'autres registres tels que Lotus Domino ou Microsoft Active Directory.

Le service d'alias nécessite un emplacement dans LDAP pour le stockage des informations requises et la fonction Tivoli Federated Identity Manager services d'exécution et de gestion a besoin d'un compte sur le serveur LDAP dans lequel rechercher les informations d'alias.

Si aucune base de données n'est encore installée sur votre système, vous devez installer un logiciel pour pouvoir utiliser le service d'alias.

Si vous avez besoin de LDAP, vous pouvez utiliser le produit IBM Tivoli Directory Server, qui peut être téléchargé sur le site http://www-306.ibm.com/software/tivoli/resource-center/security/code-directory-server.jsp.

Pourquoi et quand exécuter cette tâche

Si vous utilisez une base de données LDAP, les tâches de configuration suivantes sont requises :

- «Utilisation de tfimcfg pour configurer LDAP dans le service d'alias»

  Tivoli Federated Identity Manager est doté d'un utilitaire permettant d'automatiser ce processus lors de l'utilisation avec IBM Tivoli Directory Server ou Sun ONE Directory Server.Configuration du registre d'utilisateurs LDAP pour le service d'alias
- «Création d'un suffixe LDAP», à la page 123
- «Modification des paramètres du service d'alias», à la page 118

Utilisation de tfimcfg pour configurer LDAP dans le service d'alias

Pourquoi et quand exécuter cette tâche

L'utilitaire tfimcfg vous permet d'automatiser la configuration LDAP pour le service d'alias. Ce guide d'installation explique comment exécuter l'utilitaire tfimcfg pour les besoins de la configuration du service d'alias.

L'utilitaire tfimcfg fait appel à un fichier de données intitulé ldapconfig.properties pour sélectionner les actions à entreprendre. Vous pouvez modifier le comportement de l'utilitaire tfimcfg en éditant les valeurs contenues dans ce fichier via un éditeur de texte. Il vous est possible de spécifier si des ensembles de propriétés LDAP doivent ou non être définis. Pour chaque ensemble que vous choisissez de créer, vous pouvez spécifier les valeurs des propriétés individuelles.

Pour permettre à l'utilitaire tfimcfg de configurer le protocole LDAP par voie de programme, vous devez lui fournir certaines informations relatives à LDAP, telles que le nom d'hôte et le numéro de port LDAP, ainsi que les informations relatives au compte de l'administrateur. Le fichier ldapconfig.properties contient des entrées pour chacune de ces propriétés. Des valeurs par défaut sont fournies. Vous devez modifier ces valeurs afin de les adapter aux exigences de votre environnement de déploiement.

La procédure suivante permet de dresser la liste des propriétés pour lesquelles il convient de définir une valeur.

Procédure

1. Obtenez une copie du fichier ldapconfig.properties. Vous pouvez visualiser le contenu du fichier de l'une des manières suivantes :
   - En affichant la liste de fichiers par défaut dans Annexe A, «Référence de tfimcfg», à la page 533

- En accédant au logiciel d'installation (CD ou répertoire d'installation) et en affichant le fichier par défaut :

  AIX, Solaris, HP-UX ou Linux

  ```
  /opt/IBM/FIM/tools/tamcfg/ldapconfig.properties
  ```

  Windows

  ```
  C:\Progra~1\IBM\FIM\tools\tamcfg\ldapconfig.properties
  ```

  z/OS

  ```
  /usr/lpp/FIM/tools/tamcfg/ldapconfig.properties
  ```

2. Indiquez si tfimcfg doit ajouter des suffixes au serveur LDAP, le cas échéant.

   Valeur par défaut :

   ```
   ldap.suffix.add=true
   ```

   L'utilitaire tfimcfg ajoute un certain nombre de suffixes, sur la base d'autres paramètres contenus dans le fichier ldapconfig.properties. Pour ignorer la création des suffixes, définissez la valeur 'false'.

   Les suffixes pouvant être créés sont les suivants :

   - Un suffixe de hiérarchie permettant de conserver les informations du service d'alias (alias d'identité des utilisateurs)

     Valeur par défaut : cn=itfim
   - Un suffixe utilisé par les serveurs Tivoli Access Manager

     Valeur par défaut : secAuthority=Default
   - Un suffixe de hiérarchie pour le stockage des informations relatives aux personnes et aux groupes

     Valeur par défaut : dc=com

3. Indiquez si l'utilitaire tfimcfg doit créer des conteneurs LDAP pour stocker les utilisateurs et groupes Tivoli Federated Identity Manager.

   Les utilisateurs et groupes Tivoli Federated Identity Manager sont les suivants :

   Valeur par défaut :

   ```
   ldap.suffix.user.configuration=true
   ldap.organization.configuration=true
   ```

   - Lorsque `ldap.suffix.user.configuration=true`, tfimcfg ajoute un suffixe LDAP `dc=com` et crée un objet associé. L'utilitaire définit également des propriétés complémentaires telles que spécifiées dans le fichier ldapconfig.properties. La liste des propriétés, ainsi que leurs valeurs par défaut, est la suivante :

     ```
     ldap.suffix.user.dn=dc=com
     ldap.suffix.user.name=com
     ldap.suffix.user.attributes=dc
     ldap.suffix.user.objectclasses=domain
     ```

   - Lorsque `ldap.organization.configuration=true`, tfimcfg définit des propriétés complémentaires. Ces propriétés sont spécifiées dans le fichier ldapconfig.properties. La liste des propriétés, ainsi que leurs valeurs par défaut, est la suivante :

     ```
     ldap.user.container.dn=cn=users,dc=exemple,dc=com
     ldap.group.container.dn=cn=groups,dc=exemple,dc=com
     ldap.organization.dn=dc=exemple,dc=com
     ldap.organization.name=exemple
     ldap.organization.attributes=dc
     ldap.organization.objectclasses=domain
     ldap.user.objectclasses=person,organizationalPerson,inetOrgPerson
     ldap.group.objectclasses=groupOfUniqueNames
     ldap.user.shortname.attributes=cn,sn,uid
     ```

Vous pouvez modifier les valeurs de ces conteneurs LDAP à l'aide d'un éditeur de texte.

4. Indique si tfimcfg crée un suffixe LDAP pour stocker les alias de connexion unique.

   Valeur par défaut :

   `ldap.suffix.alias.configuration=true`

   Si vous ne souhaitez pas que l'utilitaire spécifie un nouveau suffixe, définissez la valeur `false`.

   Lorsque cette propriété est définie sur `true`, tfimcfg utilise la valeur configurée dans la propriété suivante :

   `ldap.suffix.alias.dn=cn=itfim`

   Vous pouvez modifier la valeur du nom distinctif à l'aide d'un éditeur de texte. La valeur de cette propriété doit commencer par `cn=`.

5. Indiquez si tfimcfg doit créer le suffixe `secAuthority=Default` pour Tivoli Access Manager.

   Ce suffixe est utilisé par Tivoli Access Manager pour définir une hiérarchie LDAP exploitée par les serveurs Tivoli Access Manager. Ce suffixe est généralement créé par les scripts d'installation de Tivoli Access Manager. L'utilitaire tfimcfg ajoute le suffixe si celui-ci n'existe pas déjà.

   Valeur par défaut :

   `ldap.suffix.tam.configuration=true`

   - Si Tivoli Access Manager est déjà configuré, entrez `false` pour cette valeur.
   - Si Tivoli Access Manager n'utilise pas ce serveur LDAP, entrez `false` pour cette valeur.

   Remarque : Lorsque le suffixe secAuthority=Default existe déjà, le programme tfimcfg ignore la valeur de la propriété ldap.suffix.tam.configuration.

6. Indiquez si tfimcfg doit configurer LDAP pour le service d'alias Tivoli Federated Identity Manager.

   Valeur par défaut :

   `ldap.fim.configuration=true`

   Valeur par défaut : `true`.

   Lorsque la valeur 'true' est définie, tfimcfg configure les propriétés suivantes, comme spécifié dans le fichier ldapconfig.properties :

   - Nom distinctif, nom abrégé et mot de passe que le composant serveur Tivoli Federated Identity Manager (service d'exécution et de gestion) utilise pour se connecter au serveur LDAP. Valeurs par défaut :

     ```
     ldap.fim.server.bind.dn=uid=fimserver,cn=users,dc=exemple,dc=com
     ldap.fim.server.bind.shortname=fimserver
     ldap.fim.server.bind.password=passw0rd
     ```

   - Nom distinctif et nom abrégé du groupe auquel appartient l'identité de l'utilisateur du serveur Tivoli Federated Identity Manager (fimserver). Valeurs par défaut :

     ```
     ldap.fim.admin.group.dn=cn=fimadmins,cn=groups,dc=exemple,dc=com
     ldap.fim.admin.group.shortname=fimadmins
     ```

   L'utilitaire tfimcfg ajoute ensuite l'utilisateur suivant :

   `uid=fimserver,cn=users,dc=example,dc=com`

   au groupe suivant :

   `cn=fimadmins,cn=groups,dc=example,dc=com`

7. Indiquez si tfimcfg connecte les listes de contrôle d'accès appropriées au serveur LDAP.

   Valeur par défaut :

   `ldap.modify.acls=true`

   Lorsque ce paramètre est défini sur `false`, vous devez connecter les listes de contrôle d'accès manuellement.

   Ces listes octroient l'accès en écriture et en lecture aux administrateurs Tivoli Federated Identity Manager créés par tfimcfg.

   A titre d'exemple, lorsque `ldap.modify.acls=true` et que tfimcfg est exécuté à l'aide des valeurs par défaut pour la création de suffixes, des listes de contrôle d'accès sont définies pour les suffixes suivants :

   - cn=itfim
   - secAuthority=Default
   - dc=com

   Remarque : L'outil tfimcfg connecte des listes de contrôle d'accès pour les serveurs IBM LDAP et Sun ONE. Pour les autres serveurs LDAP, vous devez connecter ces listes manuellement.
8. Indiquez des valeurs pour chacune des propriétés qui décrivent votre déploiement LDAP.

   Des valeurs par défaut sont fournies pour la plupart des propriétés. Modifiez les propriétés afin de les rendre conformes à votre déploiement. Lorsque la sécurité LDAP est activée, entrez le nom du fichier de clés Java contenant le certificat utilisé par SSL, puis le mot de passe utilisé par le service de gestion de Tivoli Federated Identity Manager.

Tableau 12. Propriétés LDAP à modifier pour tfimcfg

Propriété	Description	Votre valeur
ldap.hostname	Système qui héberge le serveur LDAP. La valeur par défaut est `localhost`.	
ldap.port	Numéro du port LDAP. La valeur par défaut est `389` pour la communication non SSL.	
ldap.admin.dn	Nom de l'administrateur LDAP. Valeur par défaut : `cn=root`	
ldap.admin.password	Mot de passe de l'administrateur LDAP.	
ldap.security.enabled	Valeur booléenne qui indique si la sécurité LDAP est activée. Cette valeur est désactivée par défaut.	
ldap.security.trusted.jks.filename	Nom du fichier de clés Java contenant le signataire du certificat SSL présenté par LDAP lors des communications sécurisées. Il n'existe pas d'entrée par défaut.	
ldap.fim.server.bind.password	Mot de passe pour les serveurs qui communiquent avec les serveurs LDAP. Vous pouvez remplacer les valeurs par défaut par les valeurs utilisées dans votre déploiement.	

9. Pour configurer le serveur LDAP, voir Annexe A, «Référence de tfimcfg», à la page 533.

Création d'un suffixe LDAP

Vous devez créer un suffixe LDAP tel que `cn=itfim` pour permettre au service d'alias d'accéder au registre d'utilisateurs LDAP.

Avant de commencer

Les instructions suivantes s'appliquent à IBM Tivoli Directory Server. Avant de passer aux étapes suivantes, assurez-vous d'avoir installé IBM Tivoli Directory Server et d'avoir procédé à la configuration initiale comme décrit dans la documentation.

Procédure

1. Arrêtez le serveur LDAP d'IBM.

   AIX, HP-UX, Linux ou Solaris :

   ```
   # ibmdirctl -D cn=root -w passw0rd stop
   ```

   Windows

   Utilisez l'icône Services.
2. Ajoutez le suffixe : `# idscfgsuf -s "cn=itfim"`.
3. Démarrez le serveur LDAP d'IBM.

   AIX, HP-UX, Linux et Solaris :

   ```
   # ibmdirctl -D cn=root -w passw0rd start
   ```

   Windows

   Utilisez l'icône Services.
4. Utilisez **ldapmodify** pour mettre à jour le fichier du schéma LDAP. Par exemple, sous Linux :

   ```
   ldapmodify -D cn=root -w passw0rd -f
     /opt/IBM/FIM/etc/itfim-secuser.ldif
   ```

Planification de la configuration des propriétés du service d'alias

Suivez ces instructions pour spécifier les propriétés du service d'alias permettant d'accéder à un ou plusieurs serveurs LDAP.

Pourquoi et quand exécuter cette tâche

Le service d'alias gère les alias en accédant à un registre d'utilisateurs LDAP. Un certain nombre d'informations relatives à l'environnement LDAP est nécessaire au service d'alias pour fonctionner dans celui-ci. La console de gestion est dotée d'une interface graphique que vous pouvez exploiter pour spécifier les propriétés nécessaires. Les propriétés sont stockées dans un fichier de propriétés Tivoli Federated Identity Manager spécifique au domaine Tivoli Federated Identity Manager en cours d'utilisation.

La présente rubrique décrit les propriétés que vous avez besoin de spécifier et fournit une feuille de travail vous permettant de saisir les valeurs applicables à votre environnement. Dans de nombreux cas, vous aurez la possibilité de spécifier une valeur par défaut.

La valeur à définir pour certaines de ces propriétés correspond aux valeurs spécifiées antérieurement, lorsque vous avez planifié l'usage de l'utilitaire tfimcfg. Lors de cette étape, vous avez identité les valeurs à éditer dans le fichier ldapconfig.properties. Les tables présentées dans la séquence de tâches suivante

identifient les zones de l'interface graphique qui contiennent des valeurs censées correspondre aux propriétés du fichier ldapconfig.properties.

Procédure

1. Déterminez la valeur de la propriété de recherche LDAP.

   La table suivante décrit le suffixe principal, la propriété de recherche LDAP configurable via l'interface graphique. Vous pouvez gérer la configuration en identifiant, à ce stade, la valeur appropriée pour votre environnement de déploiement.

Tableau 13. Propriétés de recherche LDAP

Propriété	Description	Votre valeur
Suffixe principal	Indique le suffixe racine dans lequel des paramètres du service d'alias sont écrits. Cette propriété ne peut comporter qu'une seule valeur (suffixe). La valeur de cette propriété correspond à la valeur de la propriété suivante dans ldapconfig.properties : `ldap.suffix.alias.dn` Par exemple : `cn=itfim`.	

2. Déterminez les valeurs des propriétés de l'environnement LDAP.

Tableau 14. Propriétés de l'environnement LDAP

Propriété	Description	Votre valeur
SSL activé	Case à cocher indiquant si les communications entre le service d'alias et les serveurs LDAP doivent être sécurisées grâce au protocole SSL (Secure Socket Layer). Lorsque les serveurs LDAP sont configurés pour utiliser SSL, le service d'alias doit également utiliser ce protocole lorsqu'il communique avec eux. La valeur de cette propriété correspond à la propriété suivante dans le fichier ldapconfig.properties : `ldap.security.enabled` Lors de l'utilisation de liaisons SSL, il convient de cocher la case **SSL activé** et de définir la propriété ldap.security.enabled sur la valeur `true`.	
Fichier de clés	Lorsque que la case **SSL activé** est cochée, vous devez sélectionner un fichier de clés dans le menu **Fichier de clés**. Il s'agit du nom du fichier de clés sécurisé contenant le certificat de CA du serveur LDAP. Les certificats de CA de tous les serveurs LDAP doivent se trouver dans le même fichier de clés. La valeur de cette propriété correspond à la propriété suivante dans le fichier ldapconfig.properties : `ldap.security.trusted.jks.filename`	

3. Déterminez les valeurs des propriétés du serveur LDAP

Tableau 15. Propriétés du serveur LDAP

Propriété	Description	Votre valeur
Nom d'hôte LDAP	La boîte **Hôtes LDAP** contient la liste des serveurs configurés, par ordre de préférence. Le service d'alias tente d'abord de contacter le serveur figurant au début de la liste. S'il ne parvient pas à établir le contact, il essaie avec le serveur suivant. La valeur de cette propriété inclut la propriété suivante dans le fichier ldapconfig.properties : `ldap.hostname` Le fichier ldapconfig.properties ne contient qu'une seule valeur pour cette propriété, mais vous pouvez en définir plusieurs pour le nom d'hôte LDAP.	
Port	Port sur lequel le serveur LDAP écoute. La valeur de cette propriété correspond à la propriété suivante dans le fichier ldapconfig.properties : `ldap.port` Port par défaut pour les communications autres que SSL : `389` Port par défaut pour les communications SSL : `636`	
Nom distinctif de la connexion	Nom distinctif utilisé par le service d'alias pour établir une liaison avec le serveur LDAP. La valeur de cette propriété correspond à la propriété suivante dans le fichier ldapconfig.properties : `ldap.fim.server.bind.dn` Le panneau graphique indique la valeur par défaut : cn=root. Toutefois, les droits d'accès de l'utilisateur root ne sont pas requis pour définir cette liaison. Vous pouvez spécifier le nom distinctif du service d'alias. Valeur par défaut : `uid=fimserver`	
Mot de passe BIND	Mot de passe du nom distinctif indiqué dans la zone **DN Bind**. La valeur de cette propriété correspond à la propriété suivante dans le fichier ldapconfig.properties : `ldap.fim.server.bind.password`	
Mode	Par défaut, le mode d'accès en lecture-écriture est configuré. Dans le cas de la configuration de serveurs LDAP multiples, il convient qu'une seule entité soit accessible en lecture-écriture. Dans le présent scénario, les autres serveurs LDAP sont généralement déployés pour les nécessités liées à la reprise en ligne et sont donc censés être dotés de copies du registre d'utilisateurs accessibles en lecture seule.	
Nombre minimal de connexions	Nombre de connexions (binds ou liaisons) minimal que le service d'alias peut établir avec le serveur LDAP. La plus petite valeur acceptée est zéro (0). La valeur maximale acceptée correspond à la valeur maximale prise en charge par le type de données. La valeur par défaut est 2. Utilisez-la, sauf si vous devez l'augmenter.	
Nombre maximal de connexions	Nombre de connexions (binds ou liaisons) maximal que le service d'alias peut établir avec le serveur LDAP. La valeur maximale acceptée correspond à la valeur maximale prise en charge par le type de données. La valeur par défaut est 10. Utilisez-la, sauf si vous avez besoin de l'augmenter.	

Modification des paramètres du service d'alias pour LDAP

Pourquoi et quand exécuter cette tâche

Pour modifier la configuration de la base de données de l'identificateur de noms, procédez comme suit :

Procédure

1. Connectez-vous à la console, puis cliquez sur **Tivoli Federated Identity Manager → Gestion de la configuration → Paramètres du service d'alias**. Le portlet Paramètres du service d'alias s'affiche.
2. Sélectionnez **LDAP**.

   Spécifiez les propriétés à insérer dans le formulaire suivant la section «Planification de la configuration des propriétés du service d'alias», à la page 123
3. Si vous avez sélectionné le mode de communication SSL avec LDAP, vous devez sélectionner le nom du fichier de clés sécurisé contenant le certificat de CA du serveur LDAP. Si vous n'avez pas encore déplacé l'autorité de certification LDAP vers le service de clés de Tivoli Federated Manager, vous pouvez extraire le certificat sur SSL en procédant comme suit :
   a. Sur la console; cliquez sur **Tivoli Federated Identity Manager → Service de clés**.
   b. Sélectionnez le fichier de clés certifiées dans lequel vous voulez stocker le certificat dans le tableau des fichiers de clés. Le bouton Afficher les clés est activé.
   c. Cliquez sur **Extraire le certificat de SSL**. Le panneau Mot de passe s'affiche.
   d. Entrez le mot de passe du fichier de clés certifiées, puis cliquez sur **OK**.
   e. Remplissez les zones prévues pour le nom d'hôte et le nom de port à partir desquels vous devez récupérer le certificat. Vous pouvez également cliquer sur Afficher les informations sur le signataire pour visualiser le certificat avant de le récupérer.
   f. Entrez dans la zone Alias le nom à attribuer au certificat. Cliquez ensuite sur **OK**. Le certificat est ajouté au fichier de clés certifiées.
4. Cliquez sur **Appliquer**, puis sur **OK**.

Chapitre 12. Planification du mappage des identités d'utilisateur

Présentation des tâches :

1. Consultez cette série de rubrique sur le mappage des identités d'utilisateur
2. Vérifiez les fichiers de règles de mappage par défaut disponibles pour votre protocole. Déterminez s'ils peuvent vous être utiles tels quels ou après des modifications adaptées à votre déploiement.
3. Si les exigences liées à votre déploiement ne peuvent être satisfaites au moyen d'une règle de mappage, vous pouvez sélectionner l'une des options suivantes :
   - Utilisez le module de mappage de Tivoli Directory Integrator fourni avec Tivoli Federated Identity Manager.
   - Développez un module de mappage personnalisé.

L'une des fonctions principales du service d'accréditation Tivoli Federated Identity Manager consiste à transférer les informations sur l'identité des utilisateurs (données d'identification) entre les partenaires au sein d'une fédération à connexion unique. Ce transfert nécessite plusieurs changements du format des informations sur l'identité des utilisateurs pour passer des formats locaux de chaque partenaire au format de jeton convenu pour échanger les données d'identification.

Ce transfert d'informations d'identité comprend un mappage d'identité. Lors de cette étape, les informations utilisateur sont effectivement mappées depuis la structure fournie par un type de jeton ou de données d'identification vers la structure requise par un autre type de jeton.

Pour effectuer cette étape de mappage, vous devez sélectionner l'une des options suivantes :

- Créez une règle de mappage d'identité
- Déployez le module de mappage Tivoli Directory Integrator

  L'utilisation de ce module nécessite une bonne connaissance des fonctionnalités et de la configuration de Tivoli Directory Integrator. Consultez la documentation relative à Tivoli Directory Integrator.

  Tivoli Federated Identity Manager fournit une interface graphique permettant de définir certaines propriétés de configuration. Voir «Module de mappage d'identité Tivoli Directory Integrator», à la page 135.
- Développez un module de mappage personnalisé.

  Cette tâche de développement a pour objectif de créer un module conçu pour répondre sur mesure aux besoins des applications de votre déploiement. Voir «Création d'un module de mappage personnalisé», à la page 145.

Si vous choisissez de créer une règle de mappage d'identité, vous devez utiliser le langage XSL (eXtensible Stylesheet Language) et sauvegarder le fichier XSL sur disque. Lors de la création d'une fédération, l'assistant de fédération vous invite à indiquer le nom du fichier de règles de mappage. L'assistant va importer ce fichier dans la configuration de la fédération.

Chaque fichier de règles de mappage est spécifique à un rôle et à une fédération en particulier. Par exemple, la règle de mappage à utiliser lors de la création d'une fédération SAML pour un fournisseur d'identité est différente de celle qu'on

utilisera pour un fournisseur de services. De même, la règle de mappage d'identité d'une fédération Liberty correspondant à un fournisseur d'identité est différente de celle d'une fédération SAML correspondant à un tel fournisseur.

Vous devez donc créer et enregistrer un fichier de règles de mappage avant de créer une fédération.

Remarque : Les règles de mappage d'identité indiquent les attributs associés aux données d'identification d'un utilisateur. Les utilisateurs peuvent accéder à plusieurs applications après s'être authentifiés. Par conséquent, vous devez vérifier que votre règle définit les attributs appropriés pour toutes les applications accessibles à l'utilisateur.

La console de gestion de Tivoli Federated Identity Manager fournit un assistant de fédération qui vous guide dans la configuration d'une fédération de connexion unique. Cet assistant contient un écran Mappage d'identité qui invite l'administrateur à fournir le nom d'un fichier de règles de mappage d'identité. L'assistant importe le fichier puis l'utilise lors de la génération de la configuration de la chaîne de modules d'accréditation qui est spécifique à la fédération.

L'administrateur doit créer le fichier de mappage d'identité avant d'utiliser l'assistant pour configurer la fédération. L'assistant s'attend à ce que l'administrateur crée un fichier XSL (eXtensible Stylesheet Language) décrivant les règles de mappage d'identité. Celles-ci servent à convertir les données échangées via la fédération entre les partenaires (fournisseur d'identité et fournisseur de services). Chaque règle de mappage d'identité doit fournir :

- la structure de données dont la génération est requise par le jeton de sécurité ;
- le contenu des données (attributs d'identité) qui est requis par les applications utilisant la fédération.

Pour écrire une règle de mappage d'identité, vous devez comprendre :

- le rôle du module de mappage d'identité ;
- l'expression des données d'identification d'utilisateur dans les fichiers XML ;
- l'utilisation du langage XSL pour la spécification des règles permettant de manipuler les données d'identification d'utilisateur.

Généralités sur le mappage d'identité

Lors de l'échange de jetons de sécurité avec des partenaires, il ne suffit pas de simplement comprendre la différence entre les normes des jetons. Il est également tout aussi primordial de savoir quelles informations un partenaire particulier s'attend à trouver dans les jetons provenant de vos sites, et quelles informations vous vous attendez à recevoir de la part de vos partenaires. Les fonctions de mappage d'identité et le service d'accréditation de Tivoli Federated Identity Manager permettent de personnaliser le format et le contenu des jetons entrants et sortants afin qu'ils répondent aux exigences de chaque partenaire.

Dans une fédération de connexion unique, un fournisseur d'identité est responsable de l'authentification de l'utilisateur final, dont il résulte la création de données d'identification de l'utilisateur dans l'environnement du fournisseur d'identité. Par exemple, il est possible que le fournisseur d'identité exige l'authentification des utilisateurs à l'aide d'un nom d'utilisateur et d'un mot de passe. Les informations utilisateur sont validées d'après le registre d'utilisateurs du fournisseur d'identité et des droits d'accès locaux contenant les données d'appartenance à un groupe sont générées, de même que les attributs facultatifs relatifs à l'utilisateur. Dans le cas le

plus général d'utilisation de SAML 2.0, le nom d'utilisateur n'est pas inclus dans l'assertion. L'utilisateur est, au lieu de cela, représenté par un alias.

Un fournisseur de services aura également des exigences spécifiques concernant les données d'identification de ses utilisateurs, qui sont requises pour que ces derniers accèdent aux applications. Dans la plupart des cas, les données d'identification requises par le fournisseur de services diffèrent quant au format ou au contenu des données d'identification créées par le fournisseur d'identité. Il se peut, par exemple, que le fournisseur de services souhaite inclure un attribut spécifique, tel que le numéro d'assuré social de l'utilisateur, dans les droits d'accès. Par conséquent, il est peut-être nécessaire de mapper les données d'identification entre le fournisseur d'identité et le fournisseur de services. Dans Tivoli Federated Identity Manager, côté fournisseur d'identité, l'utilisateur authentifié en local (identité d'entrée) peut être mappé vers un utilisateur différent avant la création du jeton de connexion unique (identité de sortie). De même, côté fournisseur de services, l'identité reçue du jeton de connexion (identité d'entrée) peut être mappée vers une identité locale qui est nécessaire pour l'accès aux applications du fournisseur de services (identité de sortie). Le processus de mappage est présenté dans la figure 7.

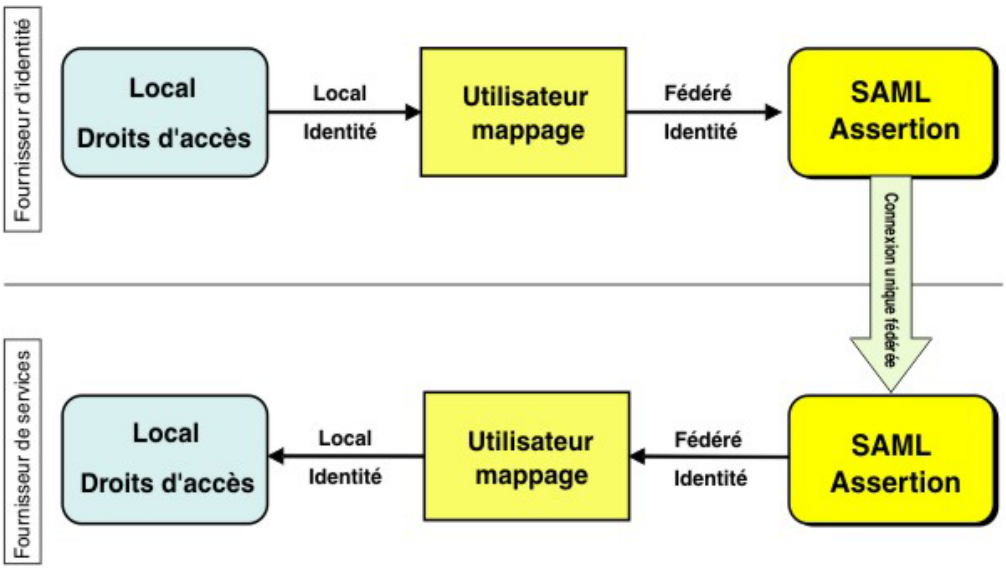


Figure 7. Exemple de mappage d'identité

Plusieurs méthodes sont possible pour générer l'identité sortante requise lors du mappage utilisateur. Des informations codées en dur peuvent par exemple être ajoutées au jeton sortant, ou un code Java peut être développé en vue d'acquérir les informations provenant de sources externes afin de les ajouter au jeton sortant. Cette souplesse est permise par les *règles de mappage d'identité*, qui sont définies de l'un ou l'autre des manières suivantes :

- Un fichier XSLT (eXtensible Stylesheet Language Transformation) est traité par le module de mappage d'identité de Tivoli Federated Identity Manager.
- Un module de mappage personnalisé créé à l'aide de Java.

Avant que vous ne décidiez quelle méthode employer, vous devez comprendre le mode de représentation des identités d'utilisateurs dans Tivoli Federated Identity Manager, le mode de traitement des jetons, ainsi que la manière dont les identités sont mappées entre partenaires.

Document relatif à l'utilisateur universel STS (Security Token Service)

Pour garantir qu'un jeton entrant est correctement converti en un jeton sortant qui intègre le contenu et le format requis par le partenaire, Tivoli Federated Identity Manager crée un document intermédiaire dans un format XML générique, contenant les informations d'identité. Ce document s'appelle l'utilisateur universel STS (STS Universal User) ou STSUU. Le document STSUU comprend trois sections :

- Informations principales
- Informations de groupe
- Informations d'attribut

Pour créer le document STSUU, Tivoli Federated Identity Manager utilise un schéma XML qui spécifie la structure. Le schéma est défini dans le fichier stsuuser.xsd. L'exemple de code ci-dessous contient la totalité du contenu du schéma XML d'utilisateur universel STS (Secure Token Service).

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
targetNamespace="urn:ibm:names:ITFIM:1.0:stsuuser"
xmlns:stsuuser="urn:ibm:names:ITFIM:1.0:stsuuser"
elementFormDefault="qualified">

 <xsd:element name="STSUniversalUser">
  <xsd:complexType>
   <xsd:sequence>
     <xsd:element name="Principal" type="stsuuser:PrincipalType"
             minOccurs="1" maxOccurs="1"/>
     <xsd:element name="GroupList" type="stsuuser:GroupListType"
             minOccurs="0" maxOccurs="1"/>
     <xsd:element name="AttributeList" type="stsuuser:AttributeListType"
             minOccurs="0" maxOccurs="1"/>
     <xsd:element name="RequestSecurityToken" type="stsuuser:RequestSecurityTokenType"
             minOccurs="0" maxOccurs="1"/>
   </xsd:sequence>
   <xsd:attribute name="version" type="xsd:string" use="required"/>
  </xsd:complexType>
 </xsd:element>

 <xsd:complexType name="PrincipalType">
  <xsd:sequence>
   <xsd:element name="Attribute" type="stsuuser:AttributeType"
         minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
 </xsd:complexType>

 <xsd:complexType name="RequestSecurityTokenType">
  <xsd:sequence>
   <xsd:element name="Attribute" type="stsuuser:AttributeType"
         minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
 </xsd:complexType>

 <xsd:complexType name="AttributeType">
                 <xsd:sequence>
                  <xsd:element name="Value" type="xsd:string"
                        minOccurs="0" maxOccurs="unbounded"/>
                  </xsd:sequence>
                 <xsd:attribute name="name" type="xsd:string" use="required"/>
                 <xsd:attribute name="type" type="xsd:string" use="optional" />
                 <xsd:attribute name="nickname" type="xsd:string" use="optional" />
                  <xsd:attribute name="preferEncryption" type="xsd:boolean" use="optional" />
 </xsd:complexType>

 <xsd:complexType name="AttributeListType">
  <xsd:sequence>
   <xsd:element name="Attribute" type="stsuuser:AttributeType"
         minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
 </xsd:complexType>

 <xsd:complexType name="GroupListType">
  <xsd:sequence>
   <xsd:element name="Group" type="stsuuser:GroupType"
         minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
 </xsd:complexType>

 <xsd:complexType name="GroupType">
  <xsd:sequence>
   <xsd:element name="Attribute" type="stsuuser:AttributeType"
         minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
  <xsd:attribute name="name" type="xsd:string" use="required" />
  <xsd:attribute name="type" type="xsd:string" use="optional" />
 </xsd:complexType>

</xsd:schema>
```

Figure 8. Schéma du document STSUU

Bien que le schéma serve de base à tous les documents STSUU, es informations exactes contenues dans n'importe quel document STSUU sont fonction du type de

jeton de sécurité qui a été utilisé en entrée. Les informations requises dans un document STSUU à la suite d'une transformation par le mappage d'identité sont fonction :

- du type de jeton à générer ;
- de la règle de mappage spécifique utilisée pour la conversion.

Lors du traitement d'un jeton dans le cadre d'une configuration de connexion unique typique, deux documents STSUU sont créés. L'un d'eux est le document STSUU d'entrée créé à partir du jeton d'entrée d'origine. L'autre est le STSUU de sortie créé une fois les règles de mappage d'identité appliquées. Pour plus d'informations, voir «Traitement des jetons».

Traitement des jetons

Dans une configuration typique de connexion unique, les jetons sont traités par le service d'accréditation Tivoli Federated Identity Manager, ainsi que trois types spécifiques de modules. Lorsque ces modules sont utilisés en combinaison, on par le *chaîne d'accréditation*. La figure 9 fournit un diagramme du traitement des jetons. A l'entrée de la chaîne d'accréditation se trouve le jeton de sécurité d'entrée. La création de ce jeton a lieu sur la base des droits d'accès locaux reçus au moment où l'utilisateur se connecte. Le premier module de la chaîne d'accréditation convertit le jeton d'entrée en document STSUU. Tous les attributs contenus dans le jeton d'entrée sont disponibles dans le document STSUU. Le document STSUU est alors utilisé comme entrée du module de mappage d'identité. Ce module peut être le module de mappage de Tivoli Federated Identity Manager qui est utilisé avec un fichier XSLT, ou bien un module de mappage personnalisé que vous avez créé. Un module de mappage donné peut être utilisé conjointement par de nombreux partenaires de la fédération, ou bien être associé à un partenaire spécifique. En sortie du module de mappage, un autre document STSUU est généré. Ce document STSUU "de sortie" est utilisé comme entrée du troisième module de traitement des jetons, qui convertit le STSUU de sortie en jeton de sortie. Le jeton de sortie est ensuite envoyé au partenaire.

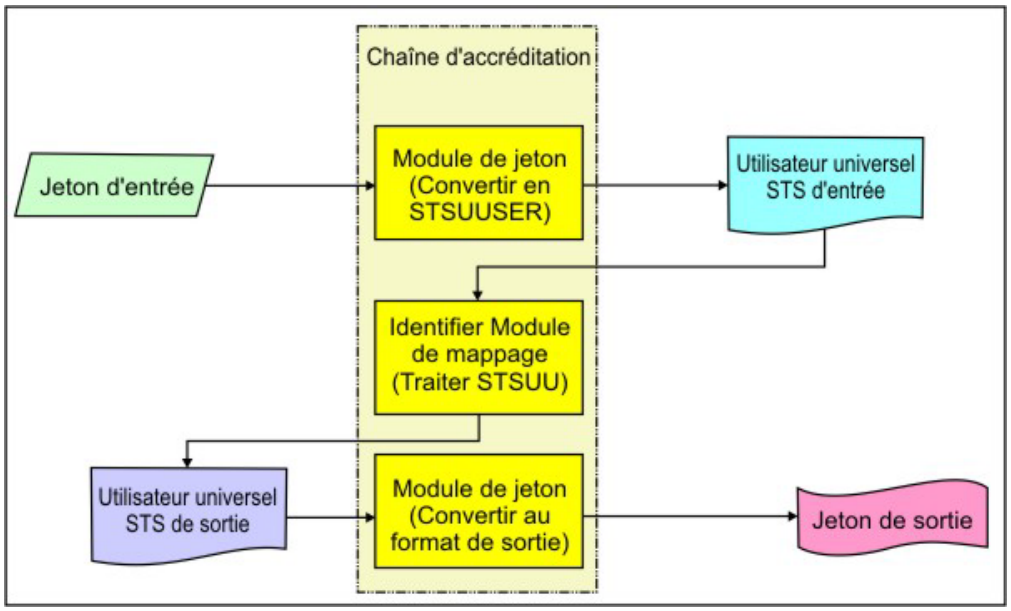


Figure 9. Traitement des jetons

Utilisation du langage XSL pour la création de fichiers de règles de mappage

Le module de mappage d'identité utilise l'API Java d'analyse syntaxique XML (JAXP) pour transformer le document d'entrée, en fonction de la configuration XSL que vous définissez dans un fichier XSL.

XSL est un langage qui permet de transformer (mettre en forme) les documents. XSL sert à définir des feuilles de style pour HTML et à mettre en forme des données XML de sorte qu'elles puissent s'afficher dans un navigateur Web. Une partie de la norme XSL définit des transformations permettant de convertir des données d'un format à l'autre. Le langage de transformation peut inclure des instructions conditionnelles, des variables et des appels de programmes Java.

Le service d'accréditation utilise XSL sous la forme d'un langage permettant de créer des règles de mappage expliquant comment transformer un document d'utilisateur universel STS d'entrée en un document d'utilisateur universel STS de sortie pouvant servir à générer un jeton de sortie. L'analyseur syntaxique XSL traite les documents XSL en recherchant des modèles correspondants. Une fois qu'un modèle est détecté, le contenu de celui-ci est traité.

Voici les principales tâches qui sont exécutées dans les règles de mappage :

- Déplacement de données d'identification d'un élément à l'autre
- Remise en forme des données d'identification
- Ajout de nouveaux éléments dotés de nouvelles données d'identification
- Suppression de données d'identification non souhaitées

Vous pouvez utiliser l'outil IBM Rational Application Developer pour exécuter un débogueur XSL à partir d'une ligne de commande. Cet outil permet de tester le code XSL sans avoir à exécuter le service d'accréditation.

Tivoli Federated Identity Manager fournit deux jeux de modèles de fichiers de mappage d'identité. Le premier jeu affiche le contenu minimal de chaque type de mappage. L'emplacement de ces fichiers de mappage est le suivant :

```
/opt/IBM/FIM/examples/mapping_rules/
```

Le tableau 16 répertorie les exemples de fichiers de règles de mappage :

Tableau 16. Exemples de règles de mappage

Nom de fichier	Description du mappage
ip_liberty.xsl	Données d'identification Tivoli Access Manager vers jeton Liberty
ip_saml_1x.xsl	Mappe une identité d'utilisateur local avec un jeton SAML 1.0 ou SAML 1.1
ip_saml_20.xsl	Mappe une identité d'utilisateur local avec un jeton SAML 2.0 au moyen d'un jeton
ip_saml_20_email_nameid.xsl	Mappe une identité d'utilisateur local avec un jeton SAML 2.0 au moyen de l'adresse électronique de l'utilisateur pour définir l'identité sans alias.
ip_wsfederation.xsl	Données d'identification Tivoli Access Manager vers jeton SAML
ip_infocard.xsl	Jeton entrant pour un jeton SAML 1.1

Tableau 16. Exemples de règles de mappage (suite)

Nom de fichier	Description du mappage
ip_openid.xsl	Jeton IVCred pour un jeton STSUU (Security Token Service Universal User)
rp_infocard.xsl	Jeton SAML 1.1 pour jeton IVCred
sp_liberty.xsl	Jeton Liberty vers données d'identification Tivoli Access Manager
sp_saml_20.xsl	Mappe un jeton SAML 2.0.x avec une identité d'utilisateur local
sp_saml_1x.xsl	Mappe un jeton 1.0 ou 1.1 avec une identité d'utilisateur local
sp_saml_1x_ext.xsl	Mappe un jeton 1.0 ou 1.1 avec une identité d'utilisateur local et vérifie l'acceptabilité de la méthode d'authentification. Ceci permet de démontrer que le fournisseur de services peut exiger que l'authentification définie auprès du fournisseur d'identité se situe à un certain niveau. Selon cette règle de mappage, l'authentification par mot de passe n'est pas acceptée. Une exception est lancée en cas d'utilisation d'une authentification par mot de passe.
sp_wsfederation.xsl	Jeton SAML vers données d'identification Tivoli Access Manager
sp_tagvalue.xsl	Jeton SAML vers données d'identification Tivoli Access Manager IV Cred avec attributs de balises et valeurs WebSEAL
username_ivcred.xsl	Jeton de nom d'utilisateur vers données d'identification Tivoli Access Manager

Remarque : Pour plus d'informations sur les examples de règles de mappage destinées à chaque protocole, reportez-vous aux instructions de configuration spécifiques à chaque protocole énoncées dans le présent manuel.

L'application de démonstration fournit des exemples de fichiers de règles de mappage d'identité XSL. Ces fichiers développent les règles de mappage minimales décrites ci-dessus, afin d'exécuter le mappage qui est personnalisé pour les comptes utilisateur créés par les scripts de configuration de l'application de démonstration.

L'emplacement des exemples de scripts de mappage de l'application de démonstration est le suivant :

```
/opt/IBM/FIM/examples/demo/scripts/demo_rules/
```

Remarque : Les noms de fichiers sont identiques aux règles de mappage minimales, mais les fichiers se trouvent dans un répertoire différent.

Les exemples de fichier de mappage sont installés automatiquement durant l'installation.

Le tableau 17 répertorie les fichiers pour chaque type de fédération sur chaque type de fournisseur.

Tableau 17. Exemples de fichiers de règles de mappage de l'application de démonstration

Fournisseur	Type de fédération	Fichier de règles de mappage
Fournisseur d'identité	Liberty	`ip_liberty.xsl`
	SAML 1.0	`ip_saml_10.xsl`
	SAML 1.1	`ip_saml_11.xsl`
	SAML 2.0	`ip_saml_20.xsl`
	WS-Federation	`ip_wsfederation.xsl`
	Carte d'information	`ip_openid.xsl`
	OpenID	`ip_infocard.xsl`
Fournisseur de services	Liberty	`sp_liberty.xsl`
	SAML 1.0 ou 1.1	`sp_saml_1x.xsl`
	SAML 2.0	`sp_saml_20.xsl`
	WS-Federation	`sp_wsfederation.xsl`
	Carte d'information	`rp_infocard.xsl`
	OpenID	`sp_openid.xsl`

Module de mappage d'identité Tivoli Directory Integrator

Ce module permet d'effectuer des opérations de mappage d'attributs et d'utilisateur génériques. Une ligne d'assemblage s'exécutant sur un serveur Tivoli Directory Integrator (TDI) est appelée pour effectuer le mappage des données d'utilisateur et d'attribut dans un STSUniversalUser. Les données peuvent être résolues à partir de diverses sources de données prises en charge nativement par TDI, y compris LDAP et les bases de données relationnelles. Le code personnalisé est également pris en charge via les connecteurs JavaScript™.

Tivoli Federated Identity Manager fournit un exemple de fichiers de mappage pour Tivoli Directory Integrator. Le fichier se trouve dans le même répertoire que les autres fichiers d'exemple. Par exemple, sous Linux ou UNIX, le fichier se trouve à l'emplacement suivant

`/opt/IBM/FIM/examples/tdi_mappings/tdi_demo_mappings.xml`

Le déploiement de ce module nécessite les éléments suivants :

- Configuration des paramètres du module d'accréditation TDI
- Configuration du serveur TDI
- Configuration des communications SSL entre le serveur TDI et le client (module d'accréditation TDI)

Suivez les instructions de configuration des rubriques :

- «Configuration du module d'accréditation TDI», à la page 136
- «Configuration du serveur TDI», à la page 137
- «Configuration du protocole SSL pour le module d'accréditation de Tivoli Directory Integrator», à la page 139

Configuration du module d'accréditation TDI

Lorsque vous sélectionnez le module de jetons de sécurité TDI durant la création d'une chaîne d'accréditation, vous êtes invité à spécifier un certain nombre de propriété de configuration. Les propriétés sont décrites dans la présente rubrique, qui contient également une feuille de travail que vous pouvez consulter lors de la configuration de votre module via la console d'administration.

Propriétés de configuration

Nom d'hôte du serveur
Nom d'hôte ou adresse IP de l'ordinateur sur lequel le serveur Tivoli Directory Integrator est exécuté. La valeur par défaut est localhost. Par exemple, `tdiserver.company.com`.

Port du serveur
Numéro de port sur lequel le serveur Tivoli Directory Integrator est configuré pour l'exécution. La valeur par défaut est 1099.

Taille du pool de gestionnaires de chaîne d'assemblage
Nombre de gestionnaires de chaîne d'assemblage à prendre en charge pour cette chaîne d'accréditation. La valeur doit être un entier positif. La valeur par défaut est 10.

Nombre d'unités d'exécution en attente
Nombre maximal d'unités d'exécution en attente de gestionnaire de chaîne d'assemblage pour cette chaîne. La valeur indiquée doit être un entier. La valeur par défaut est 0.

Durée d'attente des unités d'exécution avant qu'un gestionnaire de chaîne d'assemblage devienne disponible
Déterminez la durée d'attente des unités d'exécution avant qu'un gestionnaire de chaîne d'assemblage devienne disponible. Sélectionnez l'une de ces options.

Attendre indéfiniment
N'imposez pas de limite pour le temps d'attente des unités d'exécution avant qu'un gestionnaire de chaîne d'assemblage devienne disponible. Il s'agit de la sélection par défaut.

Ne pas attendre le gestionnaire de chaîne d'assemblage après la tentative initiale
N'autorisez pas l'attente d'un gestionnaire de chaîne d'assemblage par les unités d'exécution. Si aucun gestionnaire n'est disponible immédiatement, le module Tivoli Directory Integrator indique que le délai a expiré.

Utiliser la valeur d'attente maximale suivante
Spécifiez une valeur de durée d'attente maximale.

Durée d'attente maximale (millisecondes)
Durée d'attente maximale d'un gestionnaire de chaîne d'assemblage par une unité d'exécution avant l'émission d'un message d'expiration du délai. Cette valeur est spécifiée en millisecondes et doit être un entier positif.

Reconnaissance des paramètres de configuration
Utilisez le port et le nom d'hôte du serveur fournis précédemment dans ce panneau pour établir la connexion au serveur Tivoli Directory Integrator et effectuer la reconnaissance des configurations et des chaînes d'assemblage

disponibles. Vous devez entrer le port et le nom d'hôte du serveur avant de sélectionner cette option. Une fois cette option sélectionnée, deux menus déroulants sont disponibles.

Sélectionner le fichier de configuration
Sélectionnez le fichier de configuration à utiliser dans la liste.

Sélectionner la chaîne d'assemblage
Sélectionnez la chaîne d'assemblage à utiliser dans la liste. Cette liste est issue du fichier de configuration que vous avez sélectionné ci-dessus.

Entrer les paramètres de configuration manuellement
Entrez les paramètres de configuration manuellement en renseignant les zones suivantes :

Fichier de configuration
Nom de la solution ou nom du fichier de configuration à utiliser. Par exemple, `tdi_demo_mappings.xml`.

Nom de la chaîne d'assemblage
Nom de la chaîne d'assemblage à utiliser. Par exemple, `assemblyLine1`.

Tableau 18. Formulaire comportant les propriété de configuration de Tivoli Directory Integrator Module

Propriété	Votre valeur
Nom d'hôte du serveur	
Port du serveur	
Taille du pool de gestionnaires de chaîne d'assemblage	
Nombre d'unités d'exécution en attente	
Durée d'attente des unités d'exécution avant qu'un gestionnaire de chaîne d'assemblage devienne disponible	Trois options sont disponibles sur le panneau de configuration : • Attendre indéfiniment • Ne pas attendre le gestionnaire de chaîne d'assemblage après la tentative initiale • Utiliser la valeur d'attente maximale suivante : Durée d'attente maximale (millisecondes)
Méthode de sélection des paramètres de la ligne d'assemblage	Deux choix sont possibles : • Reconnaissance des paramètres de configuration • Entrer les paramètres de configuration manuellement
Fichier de configuration	
Nom de la chaîne d'assemblage	

Configuration du serveur TDI

Cette rubrique décrit la procédure minimale requise lors de la configuration d'une installation par défaut de du serveur TDI 6.1.1 en vue d'exécuter des chaînes d'assemblage avec Tivoli Federated Identity Manager et le module STS du serveur TDI. Le fichier tdi_demo_mappings.xml est utilisé à titre d'exemple pour la configuration.

Pour obtenir des instructions plus détaillées sur la configuration TDI, consultez le centre de documentation de Tivoli Directory Integrator : http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDI.doc_6.1.1/welcome.htm

L'installation TDI vous invite à préciser l'endroit où TDI doit rechercher le répertoire des solutions. Choix possibles :

- Utiliser un sous-répertoire TDI situé sous le répertoire principal (par défaut).
- Utiliser le répertoire d'installation
- Sélectionner un répertoire à utiliser

Cette procédure présuppose par défaut l'existence d'un sous-répertoire TDI situé sous le répertoire de base.

1. Etablissement des fichiers de solution

   Après l'installation initiale, un sous-répertoire subsiste dans le répertoire de base de l'utilisateur root : /root/TDI. Pour spécifier les fichiers de solution dans ce répertoire, démarrez le serveur TDI sans spécifier de paramètres. Les fichiers des solutions seront spécifiés comme suit :

   ```
   # /opt/IBM/TDI/V6.1.1/ibmdisrv
   ```

   Vous pouvez également choisir de démarrer l'éditeur de configuration TDI. Après le démarrage du serveur, un certain nombre de fichiers, dont le fichier solutions.properties, doivent se trouver dans le répertoire /root/TDI
2. Mettez à jour le fichier solution.properties.

   Apportez les modifications suivantes au fichier /root/TDI/solutions.properties :

   api.remote.on
   Cette propriété vous permet d'utiliser l'interface API du serveur distant utilisée par le module STS TDI. Changez la valeur par défaut 'false' en 'true'.

   api.remote.ssl.on
   Ces instructions illustrent la configuration de TDI sans SSL. La configuration de SSL sera présentée ultérieurement. Changez la valeur par défaut 'true' en 'false'.

   api.remote.nonssl.hosts
   Cette propriété est requis lorsque le serveur TDI est exécuté sur un hôte différent de celui du composant d'exécution de Tivoli Federated Identity Manager et que vous n'utilisez pas le protocole SSL entre le composant d'exécution de Tivoli Federated Identity Manager et le serveur Tivoli Directory Integrator. Spécifiez l'adresse IP de la machine exécutant le composant d'exécution (serveur d'accréditation).
3. Etablissez et alimentez le répertoire de configurations TDI.

   Le fichier solution.properties contient un paramètre décrivant l'emplacement des fichiers de configuration TDI pouvant être édités via l'API de serveur. Cette propriété, ainsi que sa valeur par défaut, sont les suivantes :

   ```
   api.config.folder=/opt/IBM/TDI/V6.1.1/configs
   ```

   Vous pouvez, si vous le souhaitez, choisir un répertoire différent, mais vous devez vous assurer que celui-ci a été créé et que fichier de configuration éventuellement utilisé par le module STS TDI se trouve bien dans ce répertoire. Vous pouvez, par exemple, créer le répertoire et copier l'exemple du fichier de configuration TDI dans ce répertoire, en procédant comme suit :

```
# mkdir /opt/IBM/TDI/V6.1.1/configs
# cp /opt/IBM/FIM/examples/tdi_mappings/tdi_demo_mappings.xml
    /opt/IBM/TDI/V6.1.1/configs
```

4. Démarrez le serveur TDI en mode démon.

   Entrez la commande suivante pour démarrer le serveur sans prise en charge SSL :

   ```
   # /opt/IBM/TDI/V6.1.1/ibmdisrv -d
   ```

   Le serveur doit normalement être en cours d'exécution et les informations de journal peuvent être visualisées dans le fichier /root/TDI/logs/ibmdi.log.

Le module STS TDI est maintenant prêt à charger et à exécuter des chaînes d'assemblage.

Configuration du protocole SSL pour le module d'accréditation de Tivoli Directory Integrator

Le module STS TDI agit en tant que client par rapport au serveur TDI. La configuration des communications SSL entre ces deux entités peut s'effectuer de nombreuses manières. La configuration du serveur et du client s'effectue séparément.

La sécurité en général, et la configuration SSL en particulier, sont traitées en détail dans le centre de documentation de Tivoli Directory Integrator. Plusieurs scénarios d'authentification sur l'API serveur sont disponibles, mais le présent document décrit uniquement les liaisons SSL authentifiées par processus réciproque. Il s'agit du modèle de déploiement recommandé et pris en charge pour les installations sécurisées impliquant le module STS TDI.

Configuration SSL pour le serveur TDI

Des informations complètes sont disponibles dans le document Tivoli Directory Integrator Administration Guide, notamment à la rubrique relative à la sécurité de l'instance de serveur TDI (TDI Server Instance Security).

Le serveur TDI a besoin de deux ensembles d'informations dans le cadre d'une configuration SSL à authentification mutuelle.

- Une clé privée et une clé publique, nécessaires pour établir l'identité du serveur
- Le certificat public ou le signataire accrédité par le client

Il convient que la clé privée et le certificat soient stockés dans un fichier de clés Java (JKS). Dans notre exemple, il s'agit de server_identity.jks. L'alias de certificat de la clé privée contenue dans ce fichier de clés porte le nom tdi_server.

Dans cet exemple, les fichiers JKS ont été créés via l'utilitaire IBM IKeyman, qui requiert un mot de passe pour le fichier de clés, mais ne génère pas de mot de passe de clé distinct pour la clé privée individuelle. Il s'agit d'un point essentiel lors de la création du fichier de dissimulation du serveur TDI. Dans cet exemple, le mot de passe du fichier de clés `passw0rd`, mais le mot de passe de la clé privée n'existe pas.

Il convient que le certificat public ou le signataire du client soit également consigné dans un fichier de clés Java. Dans notre exemple, il s'agit de client_signer.jks. L'alias de certificat du signataire accrédité n'est pas important pour cette configuration. Le mot de passe utilisé pour le fichier de clés est important. Dans cet exemple, nous utilisons la valeur `passw0rd`.

Le nom distinctif (DN) du certificat client est important. Dans cet exemple, le nom distinctif obtenu pour le certificat client est le suivant :

```
CN=tdi_client, O=ibm, C=US
```

Pour permettre l'authentification SSL mutuelle sur le serveur TDI, vous devez accomplir les tâches suivantes :

- Mise à jour des propriétés dans le fichier solution.properties
- Création du fichier de dissimulation pour le serveur TDI
- Mise à jour du registre du serveur TDI afin qu'il reconnaisse le nom distinctif du client en tant qu'administrateur
- Démarrage du serveur TDI et confirmation que le protocole SSL est actif

1. Modification du fichier solution.properties pour le support SSL du serveur TDI

   Mettez à jour les paramètres suivants dans le fichier solution.properties :

   com.ibm.di.server.keystore
   Spécifie le fichier de clés contenant la clé privée et le certificat du serveur TDI. Il convient que le fichier server_identity.jks se trouve dans le répertoire des solutions (c'est-à-dire /root/TDI dans notre exemple). Changez la valeur par défaut de testserver.jks en server_identity.jks

   com.ibm.di.server.key.alias
   Cette valeur est l'alias de certificat dans le fichier de clés du serveur, qui représente la clé privée du serveur. Changez la valeur par défaut pour le serveur en 'tdi_server'.

   api.truststore
   Définit un fichier de clés spécifiant les certificats de signataires accédités et l'autorité d'accréditation pour les clients de l'API de serveur. Il convient que le fichier client_signer.jks se trouve dans le répertoire des solutions (c'est-à-dire /root/TDI dans notre exemple). Changez la valeur par défaut 'testserver.jks' en 'client_signer.jks'.

   {protect}-api.truststore.pass
   Mot de passe du fichier de clés spécifié dans la propriété api.truststore. Si vous spécifiez le préfixe {protect}-, le mot de passe sera automatiquement chiffré au prochain démarrage du serveur. Changez la valeur par défaut {encr}-*key_string* sur `passw0rd`.

   api.remote.ssl.on
   Définissez ce paramètre sur la valeur 'true' pour activer SSL.

2. Création du fichier de dissimulation pour le serveur TDI.

   Le fichier de dissimulation pour le serveur TDI porte le nom idisrv.sth. Ce fichier se trouve dans le répertoire principal des solutions. Il peut contenir un ou deux mots de passe. Le premier mot de passe ouvre le fichier de clés contenant l'identité du serveur (server_identity.jks), tandis que le second (optionnel) correspond au mot de passe de la clé contenue elle-même dans ce fichier de clés. Si aucune valeur n'est spécifiée, le second mot de passe est supposé identique au premier.

   Lors de la création d'un certificat d'auto-signature dans un fichier de clés au moyen de l'utilitaire IBM iKeyman, le mot de passe du fichier de clés est spécifié manuellement lors de la création de celui-ci. Toutefois, il n'existe *aucun* mot de passe pour la clé privée. Vous devez donc créer le fichier de dissimulation du serveur TDI en définissant un mot de passe pour le fichier de clés et définir le mot de passe de la clé privée sur une valeur nulle (chaîne vide), comme suit :

   ```
   # /opt/IBM/TDI/V6.1.1/bin/createstash.sh passw0rd ""
   ```

3. Mettez à jour le registre du serveur TDI afin qu'il reconnaisse le nom distinctif du client en tant qu'administrateur.

   Le serveur TDI délivre une autorisation pour les requêtes d'API de serveur autorisées via un registre d'utilisateurs et les rôles assignés correspondants. Le registre par défaut est un fichier texte situé dans le répertoire :

   <répertoire_solutions>/serverapi/registry.txt

   Ajoutez le texte suivant au fichier registry.txt :

   ```
   [USER]
   [ID]:CN=tdi_client, O=ibm, C=US
   [ROLE]:admin
   [ENDUSER]
   ```

   Pour effectuer une configuration plus approfondie du registre, consultez le centre de documentation de Tivoli Directory Integrator.

4. Démarrez le serveur TDI et assurez-vous que le protocole SSL est actif.

   Démarrez le serveur TDI et approuvez le message de démarrage suivant, qui indique que le protocole SSL est en cours d'utilisation :

   ```
   # /opt/IBM/TDI/V6.1.1/ibmdisrv -d
   CTGDKD024I Remote API successfully started on port:1099,
   bound to:'SessionFactory'. SSL and Client Authentication
   are enabled.
   ```

La configuration SSL côté serveur est terminée.

Configuration SSL côté client

Le module STS TDI agit en tant que client SSL et peut fonctionner dans l'une des deux configurations suivantes :

- Il peut optimiser la configuration JSSE de WebSphere Application Server pour la prise en charge SSL.

  Remarque : Vous devez utiliser cette option avec la version intégrée de WebSphere.
- Vous pouvez spécifier des propriétés système Java chargées de contrôler quel fichier de clés et quel fichier de clés sécurisées doit être utilisé par l'API de serveur TDI.

  Remarque : Cette option ne fonctionne pas avec la version intégrée de WebSphere.

Pour ces deux options, le client a besoin de deux ensembles d'informations dans le cadre d'une configuration SSL à authentification mutuelle :

- Une clé privée et une clé publique, nécessaires pour établir l'identité du client.
- Le certificat public ou le signataire accrédité par le serveur.

Pour cet exemple, stockez la clé privée et le certificat dans un fichier de clésJava nommé client_identity.jks et stockez l'alias du certificat de la clé privée dans un fichier de clés appelé tdi_client. Dans cet exemple, le fichier JKS a été créé via l'utilitaire IBM IKeyman et le mot de passe du fichier de clés est 'passw0rd'. IKeyman n'attribut pas de second mot de passe affecté à la clé elle-même. Il est nécessaire d'affecter un mot de passe à la clé pour pouvoir démarrer correctement la machine JVM. Utilisez le même mot de passe que celui du fichier de clés. Vous pouvez modifier le fichier de clés qui a été créé à l'aide de l'utilitaire IKeyman en utilisant le paramètre d'outil de clé Java pour attribuer un mot de passe à la clé, en procédant comme suit :

```
# /opt/IBM/WebSphere/AppServer/java/bin/keytool -keypasswd
-alias tdi_client -new passw0rd -keystore client_identity.jks
-storepass passw0rd
```

Le certificat public ou le signataire du serveur est également stocké dans un fichier de clés Java. Dans notre exemple, il s'agit de server_signer.jks. L'alias de certificat du signataire accrédité n'est pas important pour cette configuration, mais le mot de passe du fichier de clés est requis. Définissez le mot de passe sur 'passw0rd'.

Nous allons utiliser le service de clés de Federated Identity Manager pour importer les deux fichiers de clés dans la partie Tivoli Federated Identity Manager du référentiel de configuration WebSphere, afin d'y faire référence ultérieurement.

Utilisez le menu Service de clés de la console d'administration pour importer les fichiers client_identity.jks et server_signer.jks.

Sur le panneau de l'interface graphique de client_identity.jks, indiquez le nom du fichier de clés tdi_client et spécifiez le type de clés de signature/chiffrement.

Sur le panneau de l'interface graphique de client_signer.jks, indiquez le nom du fichier de clés tdi_server et spécifiez le type de certificat de CA.

Les fichiers apparaissent dans le système de fichiers du référentiel de configuration de WebSphere à l'emplacement suivant :

<racine_configuration>/itfim/*<domaine_fim>*/etc/jks/tdi_client.jks
<racine_configuration>/itfim/*<domaine_fim>*/etc/jks/tdi_server.jks

Cet exemple de configuration utilise une valeur fim_domain pour `idp`.

L'étape suivante consiste en l'une des deux méthodes de configuration SSL côté client pour le module STS TDI :

- Utilisation de la configuration JSSE de WebSphere
- Utilisation des propriétés système Java pour la spécification de clés

Il n'est pas nécessaire d'appliquer les deux méthodes.

Utilisation de SSL côté client avec la configuration JSSE de WebSphere

Cette rubrique récapitule les informations décrites en détail aux emplacements suivants :

- Centre de documentation WebSphere. Pour WebSphere Application Server, par exemple, reportez-vous à la rubrique *Dynamic outbound selection of Secure Sockets Layer configurations*
- Article Developer Works *SSL, certificate, and key management enhancements for even stronger security in WebSphere Application Server V6.1* :

  http://www-128.ibm.com/developerworks/websphere/techjournal/0612_birk/0612_birk.html?ca=drs-

Il n'est pas possible d'utiliser les configurations SSL de noeuds finals sortants dynamiques, car elles nécessitent l'utilisation de la classe WebSphere JSSEHelper afin de paramétrer les informations de connexion spécifiques, alors que TDI utilise seulement les interfaces JSSE Java standard.

Vous devez par conséquent modifier la configuration SSL sur le serveur hébergeant le composant d'exécution de Tivoli Federated Identity Manager. Selon que vous exécutez le serveur d'applications en cluster ou autonome, vous pouvez appliquer cette modification au niveau cellule ou au niveau noeud. Notre exemple repose sur un serveur d'applications autonome et modifie les fichier de clés par défaut du noeud.

Pour notre modèle de déploiement, nous allons effectuer les opérations suivantes :

- Mise à jour de NodeDefaultKeyStore en important la clé privée et le certificat client
- Mise à jour de NodeDefaultTrustStore en important le certificat public côté serveur

Pour importer la clé privée et le certificat client dans le fichier NodeDefaultKeyStore, utilisez la console d'administration WebSphere :

1. Accédez à **Sécurité > Certificat SSL et gestion des clés > Magasins de clés et certificats > NodeDefaultKeyStore > Certificats personnels**.
2. Appuyez sur Importe afin d'importer une nouvelle clé, puis entrez les valeurs :

   Nom du fichier de clés
   /opt/IBM/WebSphere/AppServer/profiles/idp/config/itfim/idp/etc/jks/tdi_client.jks

   Type
   JKS

   Mot de passe du fichier de clés
   passw0rd

   Appuyez maintenant sur **Obtenir les alias de fichier de clés** (Get key file aliases)

   Alias de certificat à importer
   tdi_client

   Alias de certificat importé
   tdi_client
3. Une fois l'importation effectuée, la clé doit s'afficher comme suit dans la colonne Alias : tdi_client. Sauvegardez la configuration WebSphere après le chargement de la clé.

Avant de pouvoir importer le certificat public du serveur dans le fichier NodeDefaultTrustStore, nous avons besoin du certificat de serveur dans un format de fichier simple (format ASCII PEM ou binaire DER), au lieu du format JKS. Utilisez l'utilitaire IKeyman ou keytool pour exporter le certificat public du serveur depuis le fichier : *<racine_configuration>*/itfim/*<domaine_fim>*/etc/jks/tdi_server.jks

Vous pouvez par exemple exporter la clé publique via l'utilitaire IKeyman sous la forme d'un fichier PEM ASCII appelé : /root/keys/tdi_server.arm.

Pour importer le certificat public de serveur dans le fichier NodeDefaultTrustStore, utilisez la console d'administration WebSphere comme suit :

1. Accédez à **Sécurité > Certificat SSL et gestion des clés > Magasins de clés et certificats > NodeDefaultTrustStore > Certificats de signature**.
2. Cliquez sur **Ajouter** pour ajouter un certificat.

   L'écran Ajout de certificat de signataire s'affiche.

Alias
tdi_server

Nom de fichier
/root/keys/tdi_server.arm

Type de données
Données ASCII codées en base 64

3. Il convient que le certificat nommé tdi_server se trouve maintenant dans la liste des certificats. Sauvegardez la configuration WebSphere après avoir validé ce changement.
4. Redémarrez WebSphere ; le client doit normalement être configuré pour le protocole SSL.

Utilisation de SSL côté client avec les propriétés système Java

L'utilisation des propriétés système Java pour le protocole SSL côté client est décrite dans le centre de documentation de Tivoli Directory Integrator. Consultez, dans le guide de l'administrateur TDI, la rubrique *Sécurité d'accès à l'API de serveur*

Remarque : Cette option n'est pas disponible sur les installations WebSphere intégrées.

Ces propriétés système Java peuvent servir à sélectionner des fichiers de clés et des certificats pour les communications SSL :

api.client.ssl.custom.properties.on
Indique à 'API du serveur TDI d'utiliser ces propriétés personnalisées pour la configuration des fichiers de clés et des fichiers de clés sécurisées plutôt que la configuration JSSE. Exemple de valeur : true

api.client.keystore
Spécifie le fichier de clés contenant le certificat client. Exemple de valeur :
`${USER_INSTALL_ROOT}/config/itfim/idp/etc/jks/tdi_client.jks`

api.client.keystore.pass
Mot de passe du fichier spécifié dans api.client.keystore. Exemple de valeur : passw0rd

api.client.key.pass
Mot de passe de la clé réelle dans le fichier api.client.keystore.

N'indiquez pas cette valeur, car nous définirons le même mot de passe que pour le fichier de clés au moyen de l'utilitaire keytool.

api.truststore
Spécifie le fichier de clés contenant le certificat public du serveur TDI. Exemple :
`${USER_INSTALL_ROOT}/config/itfim/idp/etc/jks/tdi_server.jks`

api.truststore.pass
Mot de passe du fichier spécifié dans api.client.truststore. Exemple de valeur : passw0rd

A l'aide de la console d'administration WebSphere, mettez à jour les paramètres de démarrage JVM du serveur :

1. Cliquez sur **Serveurs > Serveurs d'applications > server1 > Gestion des processus et Java > Définition des processus > Machine virtuelle Java**.
2. Mettez à jour les propriétés :

Arguments JVM génériques :
-Dapi.client.ssl.custom.properties

3. Redémarrez WebSphere ; le client doit normalement être configuré pour le protocole SSL.

Création d'un module de mappage personnalisé

Avant de commencer

La création d'un module de mappage personnalisé est une procédure de programmation intensive impliquant l'écriture d'une classe Java et son installation dans le répertoire des plug-ins de votre domaine. Pour créer un module de mappage personnalisé, vous devez être familiarisé avec la structure des modules du service d'accréditation Tivoli Federated Identity Manager, ainsi que les procédures permettant de les créer et de les ajouter à votre environnement.

Pourquoi et quand exécuter cette tâche

Consultez des informations complémentaires sur les modules du service d'accréditation dans le document suivant :

- *Federated Identity Management et Web Services Security avec IBM Tivoli Security Solutions* (SG24-6394-01). Ce guide est disponible au format PDF (Portable Document Format) à l'adresse ../http://www.redbooks.ibm.com/redbooks/pdfs/sg246394.pdf ou au format HTML (Hypertext Markup Language) à l'adresse ../http://www.redbooks.ibm.com/redbooks/SG246394/
- Un article developerWorks intitulé *Tivoli Federated Identity Manager: Implementing and deploying custom trust modules* est disponible à l'adresse http://www-128.ibm.com/developerworks/tivoli/library/t-sts-custom/

Ajout d'un module de mappage personnalisé

Pour procéder à l'ajout d'un module de mappage personnalisé que vous avez créé, vous devez d'abord le définir en tant que nouveau type de module dans l'environnement Tivoli Federated Identity Manager.

Avant de commencer

Vous devez écrire une classe Java pour un nouveau type de module et installer la classe dans le répertoire des plug-in de votre domaine. Vous pouvez ensuite utiliser les instructions ci-dessous pour créer une entrée de type de module dans la console.

Pourquoi et quand exécuter cette tâche

Cette tâche est nécessaire uniquement lorsque le module de transformation XSL fourni avec Tivoli Federated Identity Manager n'est pas conforme à la configuration de votre déploiement.

Procédure

1. Cliquez sur **Tivoli Federated Identity Manager → Gestion de la configuration → Gestion des noeuds d'exécution**. Le panneau Gestion des noeuds d'exécution s'affiche.
2. Cliquez sur le bouton **Publier les plug-ins**.

3. Lorsque vous y êtes invité, cliquez sur **Charger les modifications de configuration dans l'environnement d'exécution de Tivoli Federated Identity Manager**. Le nouveau type de module s'affiche dans la liste des types de module.

Que faire ensuite

Poursuivez avec la tâche consistant à ajouter une instance du fichier de mappage dans «Ajout d'une instance de module de mappage personnalisé».

Ajout d'une instance de module de mappage personnalisé

Après avoir créé votre module de mappage et avoir ajouté celle-ci en tant que type de module, vous devez créer une instance de ce type de module afin de pouvoir l'utiliser dans l'environnement Tivoli Federated Identity Manager.

Avant de commencer

Assurez-vous d'avoir configuré les tâches suivantes avant de passer à ces instructions :

- «Création d'un module de mappage personnalisé», à la page 145
- «Ajout d'un module de mappage personnalisé», à la page 145

Pourquoi et quand exécuter cette tâche

La console est dotée d'un assistant qui vous guidera tout au long de l'ajout de l'instance de module.

Procédure

1. Cliquez sur**Tivoli Federated Identity Manager → Configurer le service d'accréditation → Instances de module**. Le panneau Instances de module affiche les instances de module par défaut, ainsi que toutes celles que vous avez ajoutées.
2. Cliquez sur **Créer**. Le panneau Type de jeton affiche les types de module définis. La liste comprend les types de jeton par défaut, ainsi que tous ceux que vous avez définis à votre convenance.
3. Sélectionnez un type de jeton, puis cliquez sur **Suivant**. L'assistant des instances de module affiche le panneau Nom d'instance du module.
4. Saisissez les valeurs des propriétés requises, puis cliquez sur **Terminer**. Pour obtenir une description de chaque zone, consultez l'aide en ligne.

Que faire ensuite

Le nouveau fichier de mappage est désormais disponible dans la liste des modules que vous pouvez sélectionner lors de l'établissement d'une fédération.

Chapitre 13. Fédérations SAML : présentation

Tivoli Federated Identity Manager prend en charge les spécifications de sécurité OASIS suivantes lors de l'échange d'informations dans une fédération:

- SAML 1.0 et 1.1 (également appelé 1.x)
- SAML 2.0

Le langage SAML (Security Assertion Markup Language) est un langage XML normalisé destiné à l'échange d'informations de connexion unique. Il s'appuie entre autres sur la technologie SOAP pour échanger des messages XML sur les réseaux informatiques. L'échange de messages s'effectue par le biais d'une série de requêtes et de réponses, où l'un des partenaires de la fédération envoie un message de requête à l'autre partenaire de la fédération. Le partenaire récipiendaire envoie alors immédiatement un message de réponse au partenaire ayant émis la requête.

Les spécifications SAML incluent les descripteurs suivants, qui servent à spécifier la structure et de contenu des messages, ainsi que la méthode de communication des messages entre les partenaires et les utilisateurs finals avec pour objectif de créer une fédération et d'initialiser et gérer la connexion unique :

Assertions
: Jetons au format XML utilisés pour transférer les informations d'identité des utilisateurs, telles que les données d'authentification, attributs et autorisations d'utilisation contenues dans les messages.

Protocoles
: Types de messages de requête et de réponse utilisés pour obtenir les données d'authentification et gérer les identités.

Liaisons
: Méthode de communication utilisée pour le transport des messages.

Profils
: Combinaisons des protocoles, assertions et liaisons utilisées conjointement pour créer une fédération et activer la connexion unique fédérée.

Lors de l'utilisation de Tivoli Federated Identity Manager, vous et votre partenaire devez utiliser la même spécification SAML (1.0, 1.1 ou 2.0) et convenir des protocoles, liaisons et profils à utiliser.

Les sections suivantes décrivent brièvement la manière dont les spécifications SAML 1.x et SAML 2.0 sont utilisées dans Tivoli Federated Identity Manager. Toutefois, ces descriptions n'incluent pas de manière exhaustive les détails de ces spécifications. Pour connaître ces détails, reportez-vous aux documents relatifs à la spécification OASIS sur le site http://www.oasis-open.org/specs/index.php.

SAML 1.x

Tivoli Federated Identity Manager prend en charge les spécifications SAML 1.0 et SAML 1.1. Ces spécifications sont communément référencées sur l'appellation SAML 1.x.

Si vous décidez, en accord avec partenaire, d'utiliser la norme SAML 1.x dans votre fédération, vous devez comprendre les principes du support SAML 1.x décrits à la rubrique Tivoli Federated Identity Manager.

Assertions

Les assertions créées par Tivoli Federation Identity Manager contiennent des instructions d'authentification permettant de confirmer que le principal (c'est-à-dire l'entité qui émet la demande d'accès) a été authentifié. Les assertions peuvent également comporter des attributs relatifs à l'utilisateur, que le fournisseur d'identité souhaite mettre à la disposition du fournisseur de services.

Les assertions sont généralement transmises au fournisseur de services par le fournisseur d'identité.

Le contenu des assertions créées par Tivoli Federated Identity Manager est contrôlé par la spécification (SAML 1.0 ou 1.1) que vous avez sélectionnée lors de l'établissement d'une fédération, ainsi que par les définitions employées dans la méthode de mappage d'identité de Tivoli Federated Identity Manager (soit un module de mappage personnalisé, soir un fichier de transformation XSL) que vous configurez. Le mappage d'identité définit également la manière dont les identités sont mappées entre les partenaires de la fédération.

Protocole

Dans Tivoli Federated Identity Manager, SAML 1.x gère les demandes d'authentification en s'appuyant sur un protocole simple de requêtes/réponses.

Liaison

SAML 1.x peut utiliser le protocole HTTP de base (via des redirections du navigateur) ou le protocole SOAP pour le transport des messages. Le *profil* utilisé dans la fédération spécifie plus en détails la manière dont s'effectue la communications des messages.

Profils

Deux options sont spécifiées par SAML 1.x pour les profils :

Artefact du navigateur (Browser Artifact)
L'artefact du navigateur utilise des communications SOAP (également appelées canal de retour SOAP) pour échanger un artefact au cours de l'établissement et de l'utilisation d'une session sécurisée entre un fournisseur d'identité, un fournisseur de services et un client (navigateur).

POST du navigateur (Browser POST)
Le profil POST du navigateur utilise un formulaire qui renvoie l'action à lui-même (self-posting form) pour échanger un artefact au cours de l'établissement et de l'utilisation de la session sécurisée entre un fournisseur d'identité, un fournisseur de services et un client (navigateur).

Tivoli Federated Identity Manager prend en charge l'artefact de navigateur par défaut lorsque vous sélectionnez SAML 1.0 ou SAML 1.1 en tant que profil de fédération. Toutefois, vous pouvez utiliser le POST du navigateur dans votre fédération en l'appliquant à des partenaires choisis. A titre d'exemple, si vous être un fournisseur de services, vous pouvez spécifier que votre fournisseur d'identité partenaire doit utiliser le POST du navigateur, lors de la configuration de ce partenaire. Si vous êtes un fournisseur d'identité, vous pouvez activer l'extension IBM PROTOCOL lors de la configuration d'une fédération SAML 1.x.

L'adresse URL servant à déclencher la connexion unique varie selon que le fournisseur d'identité utilise ou non cette extension. Pour plus d'informations sur les adresses URL, voir «Adresse URL initiale SAML 1.x», à la page 541.

SAML 2.0

La spécification SAML 2.0 a permis d'introduire davantage de souplesse que les spécifications SAML 1.x antérieures.

Assertions

Les assertions créées par Tivoli Federated Identity Manager contiennent des instructions d'authentification. Ces instructions d'authentification confirment que le principal (à savoir l'entité qui émet la demande d'accès) a été authentifié. Les assertions peuvent également comporter des attributs relatifs à l'utilisateur, que le fournisseur d'identité souhaite mettre à la disposition du fournisseur de services.

Les assertions sont en général transmises au fournisseur de services par le fournisseur d'identité.

Le contenu des assertions créées est contrôlé par la spécification (SAML 2.0). Vous sélectionnez ces assertions lorsque vous établissez une fédération. Vous sélectionnez également ces assertions dans les définitions utilisées dans la méthode de mappage d'identité Tivoli Federated Identity Manager que vous configurez. La méthode de mappage d'identité peut être un module de mappage personnalisé ou un fichier de transformation XSL. Le mappage d'identité définit également la manière dont les identités sont mappées entre les partenaires de la fédération.

Protocoles

La spécification SAML 2.0 définit plusieurs protocoles de requête et de réponse, qui renvoient tous à l'action communiquée dans le message. Les protocoles SAML 2.0 pris en charge par Tivoli Federated Identity Manager sont les suivants :

- Requête d'authentification
- Single logout (SLO, Déconnexion unique)
- Résolution d'artefact
- Gestion des identificateurs de nom

Liaisons

Lors de l'utilisation de SAML 2.0 dans Tivoli Federated Identity Manager, vous avez plusieurs options de liaison. Ces options spécifient la manière dont les messages peuvent être transportés :

Réacheminement HTTP
La redirection HTTP du navigateur permet la transmission de messages de protocole SAML à l'intérieur de paramètres d'URL. Les demandeurs et les répondeurs SAML peuvent ainsi communiquer à l'aide d'un agent d'utilisateur HTTP employé comme intermédiaire. Ceci peut être nécessaire si les entités de communication n'ont pas d'accès direct de communication. L'intermédiaire peut également être nécessaire si le répondeur requiert une interaction avec un agent d'utilisateur tel qu'un agent d'authentification.

La redirection HTTP est parfois appelée "redirection de navigateur" dans le cadre d'opérations de connexion unique. Ce profil est sélectionné par défaut.

HTTP POST
Le profil POST HTTP permet la transmission de messages de protocole SAML au format HTML codé en base64. Les demandeurs et les répondeurs SAML peuvent ainsi communiquer à l'aide d'un agent d'utilisateur HTTP employé comme intermédiaire. L'agent peut être nécessaire si les entités de communication n'ont pas de chemin direct de communication. L'intermédiaire peut également être nécessaire si le répondeur requiert une interaction avec un agent d'utilisateur tel qu'un agent d'authentification.

HTTP POST est parfois appelé POST du navigateur, notamment quand il est utilisé dans les opérations de connexion unique. Ce profil utilise un formulaire qui renvoie l'action à lui-même (self-posting form) pour échanger un artefact au cours de l'établissement et de l'utilisation d'une session sécurisée entre un fournisseur d'identité, un fournisseur de services et un client (navigateur).

Artefact HTTP
L'artefact HTTP est une liaison dans laquelle une requête ou une réponse SAML (ou les deux) sont transmises par référence à un identificateur unique appelé artefact. Une liaison séparée, telle qu'une liaison SOAP, est utilisée pour échanger l'artefact du message de protocole. Les demandeurs et les répondeurs SAML peuvent ainsi communiquer à l'aide d'un agent d'utilisateur HTTP employé comme intermédiaire. Ce paramètre est utilisé lorsqu'il n'est pas recommandé d'exposer le contenu du message dans l'intermédiaire.

L'artefact HTTP est parfois appelé Artefact du navigateur, notamment quand il est utilisé dans les opérations de connexion unique. L'artefact HTTP utilise un canal de retour SOAP. Le canal de retour SOAP est utilisé pour échanger un artefact au cours de l'établissement et de l'utilisation d'une session sécurisée entre un fournisseur d'identité, un fournisseur de services et un client (navigateur).

SOAP La liaison SOAP est une liaison qui utilise le protocole SOAP (Simple Object Access Protocol) pour les communications.

Le choix de la liaison dépend du profil que vous choisissez d'utiliser dans votre fédération.

Profils

Tivoli Federated Identity Manager prend en charge la configuration du profil de connexion unique de chaque partenaire pris séparément. Les profils prise en charge sont les suivants :

Connexion unique du navigateur Web

Le profil SSO du navigateur Web constitue le regroupement entre l'artefact et les profils POST du navigateur introduits dans la spécification 1.x. Grâce à ce profil, un message de requête d'authentification est envoyé à un fournisseur d'identité par un fournisseur de services. Un message de réponse contenant une assertion SAML est envoyé au fournisseur de services depuis le fournisseur d'identité. D'autres messages sont envoyés liés à la résolution d'artefact, si cette liaison est utilisée. Ce profil comprend des options concernant l'initialisation du flux de messages et le transport des messages :

Initialisation des messages

Le flux de messages peut être initialisé par le fournisseur de services ou le fournisseur d'identité.

Liaisons

Dans un environnement Tivoli Federated Identity Manager, les liaisons suivantes peuvent être utilisées dans le profil SSO du navigateur Web :

- HTTP Redirect (disponible uniquement dans une configuration de fournisseur d'identité)
- HTTP POST
- Artefact HTTP

Le choix de la liaison dépend du type de messages envoyés. Par exemple, un message de requête d'authentification peut être envoyé depuis un fournisseur de services à un fournisseur d'identité. Le message de réponse peut être envoyé par un fournisseur d'identité à un fournisseur de services via une liaison HTTP POST ou un artefact HTTP. Il n'est pas obligatoire pour un couple de partenaires au sein d'une fédération d'utiliser la même liaison.

Options

Le profil SLO du navigateur Web fourni par Tivoli Federated Identity Manager propose également l'option suivante :

Proxy client amélioré Cette option de profil permet à un client ou proxy amélioré (ECP) de communiquer avec un fournisseur d'identité et un fournisseur de services pour le compte d'un utilisateur (client). Par exemple, un utilisateur peut demander une ressource auprès d'un fournisseur de services. Celui-ci peut ignorer quel fournisseur d'identité contacter afin d'authentifier l'utilisateur. Grâce à l'option de profil ECP, le fournisseur de services peut contacter l'ECP, qui est en mesure de localiser le fournisseur d'identité approprié et d'accéder à celui-ci. Le profil d'ECP prend en charge les liaisons SOAP et les liaisons SOAP inverses (PAOS) lors du traitement des requêtes d'authentification.

Déconnexion unique (SLO)

Le profil SLO permet de mettre fin à toutes les sessions de connexion actives d'un utilisateur donné dans la fédération. Un utilisateur qui utilise

la connexion unique sur une fédération établit des sessions avec plusieurs participants. Les sessions sont gérées par une autorité de sessions, généralement un fournisseur d'identité. Lorsque l'utilisateur souhaite fermer toutes les sessions avec tous les participants de session, l'autorité de sessions peut utiliser le profil SLO pour arrêter de façon globale toutes les sessions actives.

Initialisation des messages
Le flux de messages peut être initialisé par le fournisseur de services ou le fournisseur d'identité.

Liaisons
Dans un environnement Tivoli Federated Identity Manager, les liaisons suivantes peuvent être utilisées dans le profil SLO :

- Réacheminement HTTP
- HTTP POST
- Artefact HTTP
- SOAP

Gestion des identificateurs de nom
Le profil Gestion des identificateurs de nom gère les identités utilisateur échangées entre fournisseurs d'identité et fournisseurs de services. Ce profil permet aux fournisseurs d'identité d'informer les fournisseurs de services. Les fournisseurs de services sont informés de toute modification apportée au contenu ou au format de l'identité d'un utilisateur donné (principal). Le profil permet aux fournisseurs de service de spécifier des *alias* uniques pour le principal. Les fournisseurs de service peuvent également envoyer ces alias au fournisseur d'identité à utiliser à la place du nom principal. Le profil active également le fournisseur. Le profil informe son partenaire lorsqu'il décide de ne plus émettre ni d'accepter des messages utilisant l'identité du principal.

Pour gérer les alias, Tivoli Federated Identity Manager utilise une fonction appelée *service d'alias*. Le service d'alias enregistre et extrait les alias liés à une identité fédérée. Les alias peuvent être exploités de différentes manières :

Alias persistants
Lors de l'utilisation d'alias persistants, l'identité de l'utilisateur est fédérée par le fournisseur d'identité dans l'identité de l'utilisateur au niveau du fournisseur de service. Un identificateur de nom SAML persistant est utilisé. L'utilisateur reste indéfiniment membre de la fédération, c'est-à-dire jusqu'à ce qu'une requête de suppression de la fédération soit émise.

Alias transitoires
Lorsque des alias transitoires sont utilisés, un identificateur temporaire est utilisé pour fédérer le fournisseur d'identité et le fournisseur de services.Un identificateur temporaire est utilisé uniquement pour la durée de la session de connexion unique de l'utilisateur.

Dans un environnement Tivoli Federated Identity Manager, le stockage et l'extraction d'alias s'effectue en provenance et en direction des types de référentiel suivants :

- Une base de données LDAP.
- Une base de données relationnelle avec prise en charge JDBC.

Durant la configuration de Tivoli Federated Identity Manager, vous pouvez configurer votre environnement en vue d'exploiter l'un de ces types de référentiel.

Initialisation des messages
Le flux de messages peut être initialisé par le fournisseur de services ou le fournisseur d'identité.

Liaisons
Les liaisons suivantes peuvent être utilisées dans le profil Gestion d'identificateurs de nom :

- Réacheminement HTTP
- HTTP POST
- Artefact HTTP
- SOAP

Reconnaissance du fournisseur d'identité
Le profil Reconnaissance du fournisseur d'identité est employé par les fournisseurs de services pour reconnaître le fournisseur d'identité employé par un utilisateur (principal) lors d'une connexion unique du navigateur Web. Certains déploiements possèdent plusieurs fournisseurs d'identité, et le fournisseur de services doit être en mesure de déterminer quel fournisseur d'identité est utilisé par un utilisateur principal. Le profil de reconnaissance du fournisseur d'identité utilise un cookie. Le cookie est créé dans un domaine commun aux fournisseurs d'identité et fournisseurs de service dans un déploiement donné. Le cookie, appelé *cookie de domaine commun*, contient la liste des fournisseurs d'identité.

Lors de la configuration de votre fédération au moyen de la console Tivoli Federated Identity Manager, vous disposez des options de profil suivantes :

Basique : Connexion unique de navigateur Web, déconnexion unique
Ce paramètre active les profils et liaisons suivants :

- Connexion unique de navigateur Web avec liaisons HTTP POST et HTTP Artifact.
- Déconnexion SLO avec liaisons HTTP POST et HTTP Artifact.

Typique : Connexion unique de navigateur Web, déconnexion unique et identificateurs de nom
Ce paramètre active les profils et liaisons suivants :

- Connexion unique de navigateur Web avec liaisons HTTP POST et HTTP Artifact.
- Déconnexion SLO avec liaisons HTTP POST et HTTP Artifact.
- Client ou proxy évolué
- Gestion des identificateurs de nom avec liaisons HTTP POST et HTTP Artifact.

Activer tous les profils et toutes les liaisons
Ce paramètre active tous les profils et liaisons disponibles :

- Connexion unique de navigateur Web avec liaisons HTTP POST, HTTP Artifact et HTTP Redirect.

  Remarque : La liaison HTTP Redirect est disponible uniquement dans une configuration de fournisseur d'identité.
- Client ou proxy amélioré

- Déconnexion SLO avec liaisons HTTP Redirect, HTTP POST et HTTP Artifact.
- Gestion des identificateurs de nom avec liaisons HTTP Redirect, HTTP POST, HTTP Artifact et SOAP
- Reconnaissance du fournisseur d'identité

Manuel : Choisissez des profils et des liaisons individuels
L'ensemble des profils pris en charge et des liaisons disponibles est présenté de manière à ce que vous puissiez choisir les options souhaitées.

Liaison de compte

Dans SAML 2.0, la liaison de compte permet à un utilisateur de relier un compte de fournisseur d'identité à un fournisseur de service. La liaison survient lors de l'initiation de la connexion unique sur le fournisseur d'identité et le fournisseur de service. Dans les deux cas, la liaison de compte requiert l'authentification de l'utilisateur au niveau du fournisseur de service et du fournisseur d'identité.

Un administrateur peut activer cette fonction dans le panneau de configuration du partenaire. Si cette fonction est activée, l'utilisateur doit s'authentifier dans le fournisseur de service à la réception d'un alias persistant. L'alias ne peut pas avoir été lié précédemment à un compte dans le fournisseur de service pour que l'authentification fonctionne.

Une fois que l'utilisateur est authentifié, l'implémentation SAML 2.0 stocke l'alias au niveau du fournisseur de service et service d'alias et établit une liaison de compte.

Gestion d'un alias inconnu

SAML 2.0 prend en charge les alias pour communiquer les identités d'utilisateur entre les partenaires.

Un administrateur peut configurer les paramètres de partenaire SAML 2.0 de sorte à gérer un alias inconnu d'une des manières suivantes :

- La page d'authentification affiche une page d'erreur lorsque le fournisseur de service ne connaît pas l'alias reçu du fournisseur d'identité. Ce paramètre représente la valeur par défaut lorsque vous
  - Ne sélectionnez pas **Imposez l'authentification pour procéder à la liaison des comptes**.
  - Ne sélectionnez pas **Mapper les identificateurs de nom inconnu au nom d'utilisateur anonyme**.
- L'implémentation SAML 2.0 mappe l'identité de l'utilisateur sur le compte utilisateur par défaut. Un compte invité établit la session de connexion unique. Ce paramètre nécessite que vous
  - Ne sélectionniez pas **Imposez l'authentification pour procéder à la liaison des comptes**.
  - Sélectionniez **Mapper les identificateurs de nom inconnu au nom d'utilisateur anonyme**.

- L'utilisateur doit s'authentifier au niveau du fournisseur de service, ce qui active la liaison de comptes. Ce paramètre nécessite que vous
  - Sélectionniez **Imposez l'authentification pour procéder à la liaison des comptes**.
  - Ne sélectionnez pas **Mapper les identificateurs de nom inconnu au nom d'utilisateur anonyme**.

Chapitre 14. Noeuds finals SAML et adresses URL

Les communications échangées au sein d'une fédération sont établies entre des noeuds finals sur les serveurs des fournisseurs d'identité et fournisseurs de services partenaires. Dans un environnement Tivoli Federated Identity Manager, les noeuds finals appartiennent à deux catégories :

- Noeuds finals définis par la spécification de la fédération (par exemple SAML 1.x ou SAML 2.0) et utilisés pour les communications inter-partenaires.
- Noeuds finals auxquels les utilisateurs peuvent accéder pour initier une activité de connexion unique.

Tous les noeuds finals sont accessibles via des adresses URL. La syntaxe des URL dépend spécifiquement du motif de l'accès, ainsi que l'auteur de cet accès (partenaire ou utilisateur final).

Adresses URL de communication entre les partenaires

Les adresses URL employées pour les communications inter-partenaires, par exemple lors de l'échange de requêtes, sont définies collectivement dans les fédérations SAML 1.x et SAML 2.0 par la notion d'*URL de noeud final*, ou individuellement par le nom du protocole, ainsi que la liaison ou le service dont elles dépendent. Les administrateurs responsables de l'installation, de la configuration et de la gestion de l'environnement Tivoli Federated Identity Manager, ainsi que des communications inter-partenaires au sein de cet environnement, peuvent visualiser des références à ces URL de noeud final, ce qui peut les aider à comprendre leur utilité. Voir «Noeuds finals et adresses URL SAML 1.x», à la page 158 ou «Noeuds finals SAML et adresses URL SAML 2.0», à la page 161.

Adresses URL pour l'accès utilisateur

Alors que les spécifications SAML définissent les noeuds finals pour les communications inter-partenaires, elles ne contiennent pas ou peu d'informations sur les noeuds finals ou les méthodes que l'utilisateur final doit employer pour initier des actions de connexion unique. Tivoli Federated Identity Manager prend en charge des URL spécifiques pour l'initiation d'actions de connexion unique par les utilisateurs finals.

Dans une fédération SAML 1.x, le processus de connexion unique est toujours initié au niveau du *service de transfert inter-sites*. La méthode selon laquelle la requête parvient à ce noeud final n'est pas précisée dans la spécification SAML. La syntaxe d'URL du service de transfert inter-sites dans un environnement Tivoli Federated Identity Manager est décrite à la rubrique «Adresse URL initiale SAML 1.x», à la page 541.

Dans une fédération SAML 2.0, les actions de connexion unique peuvent être initiées au niveau du site du fournisseur d'identité, ou celui du fournisseur de services. Les adresses URL auxquelles les utilisateurs peuvent se connecter pour déclencher une action de connexion unique dépendent spécifiquement de cette action (par exemple, l'établissement d'une connexion unique fédérée, d'une déconnexion unique ou d'une liaison de compte), ainsi que du site d'origine de l'action (fournisseur d'identité ou fournisseur de services). Dans un environnement Tivoli Federated Identity Manager, les adresses URL pouvant servir au

déclenchement d'actions de connexion unique sont référencées comme *adresse URL initiales de profil*. Les architectes et développeurs d'applications, qui conçoivent et mettent en oeuvre l'interaction des utilisateurs avec le processus de connexion unique, doivent pouvoir cerner le concept des URL initiales de profil. Voir «Adresses URL initiales de profil SAML 2.0», à la page 543.

Noeuds finals et adresses URL SAML 1.x

Plusieurs noeuds finals sont configurés sur votre serveur point de contact afin de permettre l'échange de communications entre vous et votre partenaire. La configuration de ces noeuds finals a lieu en même temps que celle de votre fédération dans Tivoli Federated Identity Manager. Les noeuds finals sont accessibles via des URL et sont utilisés par les partenaires au sein de la fédération. Si vous êtes responsable de l'installation, de la configuration ou de la gestion d'une fédération dans Tivoli Federated Identity Manager, il peut être utile de vous familiariser avec ces noeuds finals et adresses URL.

Les noeuds finals suivants sont utilisés dans une fédération SAML 1.x.

Serveur point de contact
Noeud final du serveur point de contact sur lequel les communications ont lieu. La syntaxe de l'URL du serveur point de contact est la suivante :

`https://`*`nom_hôte:numéro_port`*

Où :

https HTTPS peut être HTTP si le protocole SSL n'est pas activé sur le serveur.

nom d'hôte
Nom d'hôte du serveur point de contact.

numéro_port
Numéro de port où les communications prennent effet sur le serveur. Le numéro de port par défaut est le 9443 sur WebSphere Application Server si le protocole SSL est activé, ou le 9080 dans le cas contraire.

Vous serez invité à indiquer l'URL de votre serveur point de contact lors de la configuration de votre fédération. Une fois la configuration terminée, l'URL de votre serveur point de contact comporte le suffixe `/sps`, de sorte que la syntaxe de l'URL configurée pour le serveur point de contact est la suivante :

`https://`*`nom_hôte:numéro_port`*`/sps`

Le suffixe `/sps` indique que l'URL est définie pour les services de connexion unique.

Service de transfert inter-sites
Noeud final du serveur point de contact du fournisseur d'identité sur lequel démarre le processus de demande de connexion. Il s'agit de l'emplacement auquel sont envoyées les demandes de connexion unique des utilisateurs. SAML n'indique pas comment les demandes arrivent sur ce noeud final. Si vous êtes un fournisseur d'identité utilisant Tivoli Federated Identity Manager, la méthode utilisée est fonction de la procédure de connexion des utilisateurs et de l'emplacement dans lequel les utilisateurs ouvrent une session. Par exemple, si les utilisateurs ouvrent une session sur le site Web du fournisseur de services partenaire, votre fournisseur de services partenaire a besoin de l'URL de votre service de

transfert inter-sites et doit ensuite configurer un certain type de réacheminement permettant aux utilisateurs d'accéder à partir de leur site à votre page de connexion.

L'adresse URL repose sur celle que vous avez spécifiée pour votre serveur point de contact. La syntaxe est la suivante :

`https://nom_hôte:numéro_port/sps/nom_fédération/samlxx/login`

Où :

https HTTPS peut être HTTP si le protocole SSL n'est pas activé sur le serveur.

nom d'hôte
Nom d'hôte du serveur point de contact.

numéro_port
Le numéro de port où les communications prennent effet sur le serveur.

sps Racine de contexte de l'application de connexion unique sur WebSphere Application Server. Cette partie de l'URL ne peut pas être modifiée.

nom_fédération
Nom donné à la fédération lors de la configuration.

saml*xx*
Version de SAML configurée pour la fédération. Les valeurs peuvent être les suivantes :

- saml (pour SAML 1.0)
- saml11 (pour SAML 1.1)

login Désignation du type de noeud final qui utilise le port. Le type **login** est utilisé pour le service de transfert inter-sites dans les fédérations SAML 1.x.

Ce noeud final est utilisé uniquement dans les configurations de fournisseur d'identité et est défini automatiquement à votre place lors de la configuration de votre fédération.

Service de résolution des artefacts
Noeud final du serveur point de contact du fournisseur d'identité sur lequel des artefacts sont échangés pour les assertions. Ce noeud final est l'emplacement dans lequel les partenaires de la fédération communiquent. Il est parfois désigné par le terme de noeud final *noeud final SOAP* sur le serveur point de contact du fournisseur d'identité.

Remarque : Il se peut aussi que vous connaissiez ce noeud final sous le nom de *service répondeur*.

L'adresse URL repose sur celle que vous avez spécifiée pour votre serveur point de contact. La syntaxe est la suivante :

`https://nom_hôte:numéro_port/sps/nom_fédération/samlxx/soap`

Où :

https HTTPS peut être HTTP si le protocole SSL n'est pas activé sur le serveur.

nom d'hôte
Nom d'hôte du serveur point de contact.

numéro_port
Numéro de port où les communications prennent effet sur le serveur. Le numéro de port par défaut est 9444.

sps Racine de contexte de l'application de connexion unique sur WebSphere Application Server. Cette partie de l'URL ne peut pas être modifiée.

nom_fédération
Nom donné à la fédération lors de la configuration.

saml*xx*
Version de SAML configurée pour la fédération. Les valeurs peuvent être les suivantes :

- saml (pour SAML 1.0)
- saml11 (pour SAML 1.1)

soap Désignation du type de noeud final qui utilise le port. Le type **soap** est utilisé pour le service de résolution des artefacts dans les fédérations SAML 1.x.

Ce noeud final est utilisé uniquement dans les configurations de fournisseur d'identité et est défini automatiquement à votre place lors de la configuration de votre fédération.

Service d'assertion client
Noeud final du serveur point de contact du fournisseur de services qui reçoit des assertions ou des artefacts. Ce noeud final est l'emplacement dans lequel les partenaires de la fédération communiquent. Ce noeud final est parfois désigné par le terme de noeud final *SOAP* sur le serveur point de contact du fournisseur de services.

Remarque : Si vous utilisez le profil Artefact du navigateur, vous connaissez peut-être ce noeud final sous le nom de *service client d'artefacts* ou *service de réception d'artefacts*.

L'adresse URL repose sur celle que vous avez spécifiée pour votre serveur point de contact. La syntaxe est la suivante :

`https://`*`nom_hôte:numéro_port`*`/sps/`*`nom_fédération`*`/saml`*`xx`*`/login`

Où :

https HTTPS peut être HTTP si le protocole SSL n'est pas activé sur le serveur.

nom d'hôte
Nom d'hôte du serveur point de contact.

numéro_port
Numéro de port où les communications prennent effet sur le serveur. Le numéro de port par défaut est le 9443 sur WebSphere Application Server.

sps Racine de contexte de l'application de connexion unique sur WebSphere Application Server. Cette partie de l'URL ne peut pas être modifiée.

nom_fédération
Nom donné à la fédération lors de la configuration.

saml*xx*

Version de SAML configurée pour la fédération. Les valeurs peuvent être les suivantes :

- saml (pour SAML 1.0)
- saml11 (pour SAML 1.1)

login Désignation du type de noeud final qui utilise le port. Le type **login** est utilisé pour le service d'assertion client.

Ce noeud final est utilisé uniquement dans les configurations de fournisseur de services des fédérations SAML 1.x et est défini automatiquement à votre place lors de la configuration de votre fédération.

Noeuds finals SAML et adresses URL SAML 2.0

Plusieurs noeuds finals sont configurés sur votre serveur point de contact afin de permettre l'échange de communications entre vous et votre partenaire. La configuration de ces noeuds finals a lieu en même temps que celle de votre fédération dans Tivoli Federated Identity Manager. Les noeuds finals sont accessibles via des URL et sont utilisés par les partenaires au sein de la fédération. Si vous êtes responsable de l'installation, de la configuration ou de la gestion d'une fédération dans Tivoli Federated Identity Manager, il peut être utile de vous familiariser avec ces noeuds finals et adresses URL.

Les noeuds finals suivants sont utilisés dans une fédération SAML 2.0.

Serveur point de contact

Noeud final du serveur point de contact sur lequel les communications ont lieu. L'URL du serveur point de contact est également utilisée en tant qu'ID de fournisseur. La syntaxe de l'URL du serveur point de contact est la suivante :

`https://`*`nom_hôte:numéro_port`*

Où :

https HTTPS peut être HTTP si le protocole SSL n'est pas activé sur le serveur.

nom d'hôte

Nom d'hôte du serveur point de contact.

numéro_port

Numéro de port où les communications prennent effet sur le serveur. Numéro de port où les communications prennent effet sur le serveur. Le numéro de port par défaut est le 9443 sur WebSphere Application Server si le protocole SSL est activé, ou le 9080 dans le cas contraire.

Vous serez invité à indiquer l'URL de votre serveur point de contact lors de la configuration de votre fédération. Une fois la configuration terminée, l'URL de votre serveur point de contact comporte le suffixe `/sps`, de sorte que la syntaxe de l'URL configurée pour le serveur point de contact est la suivante :

`https://`*`nom_hôte:numéro_port`*`/sps`

Le suffixe `/sps` indique que l'URL est définie pour les services de connexion unique.

Service de résolution des artefacts (ou noeud final SOAP)

Noeud final du serveur point de contact du fournisseur d'identité ou de

services sur lequel des artefacts sont échangés pour les messages SAML. Ce noeud final est l'emplacement dans lequel les partenaires de la fédération communiquent. Il est parfois désigné par le terme de noeud final *noeud final SOAP*.

Remarque : Il se peut aussi que vous connaissiez ce noeud final sous le nom de *service répondeur*.

L'adresse URL repose sur celle que vous avez spécifiée pour le serveur point de contact. La syntaxe est la suivante :

`https://nom_hôte:numéro_port/sps/nom_fédération/saml20/soap`

Où :

https HTTPS peut être HTTP si le protocole SSL n'est pas activé sur le serveur.

nom d'hôte
Nom d'hôte du serveur point de contact.

numéro_port
Numéro de port où les communications prennent effet sur le serveur. Le numéro de port par défaut est 9444.

sps Racine de contexte de l'application de connexion unique sur WebSphere Application Server. Cette partie de l'URL ne peut pas être modifiée.

nom_fédération
Nom donné à la fédération lors de la configuration.

saml20
Désignation du protocole SAML que vous choisissez d'utiliser dans votre fédération.

soap Désignation du type de noeud final qui utilise le port. Le type **soap** est utilisé pour le service de résolution des artefacts dans les fédérations SAML 2.0.

Ce noeud est défini automatiquement à votre place lors de la configuration de votre fédération.

Service d'assertion client
Noeud final du serveur point de contact du fournisseur de services qui reçoit des assertions ou des artefacts. Ce noeud final est l'emplacement dans lequel les partenaires de la fédération communiquent.

L'adresse URL repose sur celle que vous avez spécifiée pour le serveur point de contact. La syntaxe est la suivante :

`https://nom_hôte:numéro_port/sps/nom_fédération/saml20/login`

Où :

https HTTPS peut être HTTP si le protocole SSL n'est pas activé sur le serveur.

nom d'hôte
Nom d'hôte du serveur point de contact.

numéro_port
Numéro de port où les communications prennent effet sur le

serveur. Le numéro de port par défaut est le 9443 sur WebSphere Application Server si le protocole SSL est activé, ou le 9080 dans le cas contraire.

sps Racine de contexte de l'application de connexion unique sur WebSphere Application Server. Cette partie de l'URL ne peut pas être modifiée.

nom_fédération
Nom donné à la fédération lors de la configuration.

saml20
Désignation du protocole SAML que vous choisissez d'utiliser dans votre fédération.

login Désignation du type de noeud final qui utilise le port. Le type **login** est utilisé pour le service d'assertion client dans les fédérations SAML 2.0.

Ce noeud final est utilisé uniquement dans les configurations de fournisseur de services des fédérations SAML 2.0 et est défini automatiquement à votre place lors de la configuration de votre fédération.

Service de connexion unique
Noeud final du serveur point de contact du fournisseur d'identité qui reçoit les requêtes d'authentification.

L'adresse URL repose sur celle que vous avez spécifiée pour le serveur point de contact. La syntaxe est la suivante :

`https://`*`nom_hôte:numéro_port`*`/sps/`*`nom_fédération`*`/saml20/login`

Où :

https HTTPS peut être HTTP si le protocole SSL n'est pas activé sur le serveur.

nom d'hôte
Nom d'hôte du serveur point de contact.

numéro_port
Numéro de port où les communications prennent effet sur le serveur. Le numéro de port par défaut est le 9443 sur WebSphere Application Server si le protocole SSL est activé, ou le 9080 dans le cas contraire.

sps Racine de contexte de l'application de connexion unique sur WebSphere Application Server. Cette partie de l'URL ne peut pas être modifiée.

nom_fédération
Nom donné à la fédération lors de la configuration.

saml20
Désignation du protocole SAML que vous choisissez d'utiliser dans votre fédération.

login Désignation du type de noeud final qui utilise le port. Le type **login** est utilisé pour le service d'assertion client dans les fédérations SAML 2.0.

Ce noeud final est utilisé uniquement dans les configurations de fournisseur d'identité des fédérations SAML 2.0 et est défini automatiquement à votre place lors de la configuration de votre fédération.

Service SLO (Single Logout)
Noeud final du serveur point de contact du fournisseur d'identité ou de services qui reçoit les requêtes de déconnexion.

L'adresse URL repose sur celle que vous avez spécifiée pour le serveur point de contact. La syntaxe est la suivante :

```
https://nom_hôte:numéro_port/sps/nom_fédération/saml20/slo
```

Où :

https HTTPS peut être HTTP si le protocole SSL n'est pas activé sur le serveur.

nom d'hôte
Nom d'hôte du serveur point de contact.

numéro_port
Numéro de port où les communications prennent effet sur le serveur. Le numéro de port par défaut est le 9443 sur WebSphere Application Server si le protocole SSL est activé, ou le 9080 dans le cas contraire.

La valeur par défaut est attribuée à ce port, sauf si celui-ci est indisponible lors de l'installation de Tivoli Federated Identity Manager. Si le port par défaut est indisponible, le programme d'installation ajoute une valeur de 1 au numéro de port jusqu'à ce qu'il trouve un port disponible portant ce numéro.

sps Racine de contexte de l'application de connexion unique sur WebSphere Application Server. Cette partie de l'URL ne peut pas être modifiée.

nom_fédération
Nom donné à la fédération lors de la configuration.

saml20
Désignation du protocole SAML que vous choisissez d'utiliser dans votre fédération.

slo Désignation du type de noeud final qui utilise le port. Le type **slo** est utilisé pour le service de déconnexion SLO dans les fédérations SAML 2.0.

Service de gestion des identificateurs de nom
Noeud final du serveur point de contact du fournisseur d'identité ou de services qui reçoit les messages liées à la gestion des noms. L'adresse URL repose sur celle que vous avez spécifiée pour le serveur point de contact, ainsi que la liaison utilisée.

La syntaxe des adresses de redirection HTTP, POST HTTP et d'artefact HTTP est la suivante :

```
https://nom_hôte:numéro_port/sps/nom_fédération/saml20/mnids
```

La syntaxe pour SOAP est la suivante :

```
https://nom_hôte:numéro_port/sps/nom_fédération/saml20/soap
```

Où :

https HTTPS peut être HTTP si le protocole SSL n'est pas activé sur le serveur.

nom d'hôte
Nom d'hôte du serveur point de contact.

numéro_port
Numéro de port où les communications prennent effet sur le serveur. Le numéro de port dépend de la liaison utilisée. Les ports par défaut sont les suivants :

HTTP SOAP : 9444

POST HTTP, Artefact HTTP, Redirection HTTP : 9443

sps Racine de contexte de l'application de connexion unique sur WebSphere Application Server. Cette partie de l'URL ne peut pas être modifiée.

nom_fédération
Nom donné à la fédération lors de la configuration.

saml20
Désignation du protocole SAML que vous choisissez d'utiliser dans votre fédération.

mnids ou soap
Désignation du type de noeud final qui utilise le port. Le type **mnids** est employé pour le service de gestion des identificateurs de nom dans les fédérations SAML 2.0 utilisant les entités de redirection HTTP, POST HTTP ou artefact HTTP. Le type **soap** est utilisé lorsque le type de liaison SOAP est configuré.

URL du service Common Domain Cookie utilisée par le service de reconnaissance de fournisseur d'identité (Identity Provider Discovery service)
Par défaut, Tivoli Federated Identity Manager permet la mise en oeuvre d'un service de domaine commun qui permet à un fournisseur d'identité d'informer un fournisseur de services qu'un utilisateur spécifique est prêt à utiliser une fédération. L'adresse URL par défaut est utilisée en interne pour indiquer si le service de cookies du domaine commun doit accéder en lecture ou en écriture ('get' ou 'set') aux valeurs, en rattachant le suffixe cdcwriter (fournisseur d'identité) ou cdcreader (fournisseur de services) à la fin de l'URL. La syntaxe par défaut de l'URL est la suivante :

```
https://nom_domaine_commun/sps/nom_fédération/saml20/[cdcreader|cdcwriter}
```

Où :

https HTTPS peut être HTTP si le protocole SSL n'est pas activé sur le serveur.

nom_domaine_commun
Nom de domaine commun partagé.

sps Racine de contexte de l'application de connexion unique sur WebSphere Application Server. Cette partie de l'URL ne peut pas être modifiée.

nom_fédération
Nom donné à la fédération lors de la configuration.

saml20
Désignation du protocole SAML que vous choisissez d'utiliser dans votre fédération.

cdcwriter *ou* **cdcreader**
Désignation du type d'action (read/get ou write/set) utilisé.

Remarque : Tivoli Federated Identity Manager prend également en charge l'utilisation d'un service de reconnaissance tierce partie ou personnalisé.

Chapitre 15. Exemples de règles de mappage d'identité pour les fédérations SAML

Les rubriques suivantes indiquent les règles de mappage d'identité fournies pour les fédérations SAML. Si vous avez décidé d'utiliser des règles de mappage d'identité pour votre fédération, vous pouvez consulter les règles XSLT.

Pour des généralités sur le mappage d'identité, ainsi qu'une descriptions des options de mappage d'identité qui n'utilisent pas les fichiers de règles de mappage XSLT, voir PlanningIdentityMapping.dita

- «Mappage d'une identité d'utilisateur local vers un jeton SAML 1.x»
- «Mappage d'un jeton SAML 1.x vers une identité d'utilisateur local», à la page 168
- «Mappage d'une identité locale vers un jeton SAML 2.0 à l'aide d'un alias», à la page 169
- «Mappe un jeton SAML 2.0 avec une identité locale», à la page 171

Mappage d'une identité d'utilisateur local vers un jeton SAML 1.x

Ce scénario se produit lors de l'échange de messages entre des partenaires d'une fédération de connexion unique SAML 1.0 ou SAML 1.1. Lorsqu'une demande d'utilisateur est reçue (par exemple, pour accéder à une ressource distante), Tivoli Federated Identity Manager prend contact avec le serveur point de contact (par exemple, WebSphere Application Server) et obtient une identité d'utilisateur local.

Le serveur Tivoli Federated Identity Manager place les informations relatives à l'identité d'utilisateur local dans un document XML qui est conforme au schéma STSUUSER (utilisateur universel STS (Security Token Service)). Le serveur consulte ensuite son entrée de configuration correspondant au partenaire de la fédération (par exemple, la destination qui héberge une ressource demandée). La configuration indique le type de jeton à créer. Dans ce cas, le type de jeton est SAML.

Le module de mappage d'identité modifie ensuite le document XML de sorte que ce dernier contienne les informations requises pour la génération d'un jeton SAML.

Tableau 19. Entrées STSUUSER servant à générer un jeton SAML

Elément STSUUSER	Informations de jeton SAML	Obligatoire/Facultatif
Principal Attr: Name	AuthenticationStatement/Subject/NameIdentifier	Obligatoire
Liste des attributs	Attributs personnalisés supplémentaires	Facultatif

Le module de mappage est responsable des deux tâches suivantes :

1. Mappage de l'élément Principal Attr Name vers une entrée Principal Name.

   Le type doit être valide pour SAML. Par exemple :

   ```
   urn:oasis:names:tc:SAML:1.0:assertion#emailAddress
   ```

   La figure 10, à la page 168 présente une partie du fichier de règles de mappage par défaut, ip_saml_1x.xsl.

```
<!--
  Ce modèle remplace l'intégralité de l'élément Principal par un élément qui ne
  contient que le nom d'utilisateur iv.
 -->
 <xsl:template match="//stsuuser:Principal">
  <stsuuser:Principal>
   <stsuuser:Attribute name="name" type="urn:oasis:names:tc:SAML:1.0:assertion#emailAddress">
    <stsuuser:Value>
     <xsl:value-of select="//stsuuser:Principal/stsuuser:Attribute[@name='name']
     [@type='urn:ibm:names:ITFIM:5.1:accessmanager']/stsuuser:Value" />
    </stsuuser:Value>
   </stsuuser:Attribute>
  </stsuuser:Principal>
 </xsl:template>
```

Figure 10. Exemple de code XSL présentant le mappage d'une identité d'utilisateur local vers un nom de Principal pour un jeton SAML

Dans cet exemple, l'identité d'utilisateur local est désignée par le *nom d'utilisateur iv*.

```
<stsuuser:Value>
     <xsl:value-of select="//stsuuser:Principal/stsuuser:Attribute[@name='name']
     [@type='urn:ibm:names:ITFIM:5.1:accessmanager']/stsuuser:Value" />
```

2. Paramétrage de la méthode d'authentification sur le mécanisme `password`. Cette action est requise par la norme SAML.

   Voir la figure 11.

```
<xsl:template match="//stsuuser:AttributeList">
     <stsuuser:AttributeList>
         <!-- Tout d'abord l'attribut de la méthode d'authentification -->
         <stsuuser:Attribute name="AuthenticationMethod"
              type="urn:oasis:names:tc:SAML:1.0:assertion">
            <stsuuser:Value>urn:oasis:names:tc:SAML:1.0:am:password</stsuuser:Value>
         </stsuuser:Attribute>
     </stsuuser:AttributeList>
</xsl:template>
```

Figure 11. Exemple de code XSL présentant l'affectation d'une méthode d'authentification sous forme d'attribut pour un jeton SAML

Mappage d'un jeton SAML 1.x vers une identité d'utilisateur local

Le fournisseur de services reçoit un jeton SAML 1.0 ou SAML 1.1. Tivoli Federated Identity Manager convertit le contenu du jeton en un fichier XML conforme au schéma d'utilisateur universel STS (Security Token Service).

Tableau 20. Informations de jeton SAML converties en document d'utilisateur universel STS

Informations de jeton SAML	Elément STSUUSER
AuthenticationStatement/Subject/NameIdentifier	Principal Attr: Name

Tivoli Federated Identity Manager convertit cette information en identité d'utilisateur local.

- L'élément NameIdentifier sert à remplir l'attribut `name` de l'élément Principal.

  La figure 12, à la page 169 présente l'affectation d'une valeur définie pour le nom Principal. Cet exemple de code est issu du fichier de mappage par défaut, sp_saml_1x.xsl.

```
<!--
  Ce modèle remplace le nom de principal par le nom local de l'utilisateur.
 -->
 <xsl:template match="//stsuuser:Principal/stsuuser:Attribute[@name='name']">
  <stsuuser:Attribute name="name" type="urn:ibm:names:ITFIM:5.1:accessmanager">
            <stsuuser:Value><xsl:value-of
select="//stsuuser:Principal/stsuuser:Attribute[@name='name']/stsuuser:Value" />
           </stsuuser:Value>
            </stsuuser:Attribute>
 </xsl:template>
```

Figure 12. Exemple de code XSL présentant l'affectation d'une valeur pour le nom Principal d'un jeton SAML

Autre exemple de fichier de mappage entre un jeton SAML 1.x et une identité locale : sp_saml_1x_ext.xsl. ce fichier effectue le mappage comme décrit, mais ajoute une section chargée de vérifier que le fournisseur d'identité a utilisé un niveau d'authentification approprié. Dans cet exemple de fichier, une exception est générée su le fournisseur d'identité a utilisé une authentification par mot de passe.

```
<xsl:param name="message">Detected an unacceptable authentication method.
  A higher level of authentication is required.</xsl:param>
 <xsl:template match="//stsuuser:AttributeList">
 <xsl:variable name="result" select="//stsuuser:AttributeList/
  stsuuser:Attribute[@name='AuthenticationMethod']/stsuuser:Value"/>
 <xsl:if test="(contains($result,'password')) = 'true'">
  <xsl:value-of select="mapping-ext:throwSTSException($message)" />
 </xsl:if>
 </xsl:template>
```

Figure 13. Exemple de code XSL illustrant la vérification d'une valeur de AuthenticationMethod

Mappage d'une identité locale vers un jeton SAML 2.0 à l'aide d'un alias

Ce scénario se produit lors de l'échange de messages entre des partenaires dans une fédération de connexion unique SAML 2.0. Lorsqu'une demande d'utilisateur est reçue (par exemple, pour accéder à une ressource distante), Tivoli Federated Identity Manager prend contact avec le serveur point de contact (par exemple, WebSphere Application Server) et obtient une identité d'utilisateur local. Le scénario décrit ici utilise l'exemple de fichier de mappage ip_saml_20.xsl contenant un alias pour l'identité.

Le serveur Tivoli Federated Identity Manager place les informations relatives à l'identité d'utilisateur local dans un document XML qui est conforme au schéma STSUUSER (utilisateur universel STS (Security Token Service)). Le serveur consulte ensuite son entrée de configuration correspondant au partenaire de la fédération (par exemple, la destination qui héberge une ressource demandée). La configuration indique le type de jeton à créer. Dans ce cas, le type de jeton est SAML.

Le module de mappage d'identité modifie ensuite le document XML de sorte que ce dernier contienne les informations requises pour la génération d'un jeton SAML 2.0.

Tableau 21. Entrées STSUUSER servant à générer un jeton SAML (à l'aide d'un alias)

Elément STSUUSER	Informations de jeton SAML	Obligatoire/Facultatif
Attribut : AuthContextClassRef	Référence à la classe du contexte d'authentification. Il est à noter que cet élément est toujours paramétré sur "password" (nom d'utilisateur/mot de passe), quelle que soit la méthode d'authentification définie dans les droits d'accès.	Obligatoire
Liste des attributs	Attributs personnalisés supplémentaires	Facultatif

Le module de mappage est responsable des tâches suivantes :

1. Mappage de l'élément Principal Attr Name vers une entrée Principal Name.

   Il est à noter que lorsque le module de jeton génère le jeton, ce nom de Principal n'est pas utilisé directement. En revanche, la valeur de la zone Name est envoyée en entrée du service d'alias du service Tivoli Federated Identity Manager. Le service d'alias obtient le nom d'alias (identificateur de nom) pour le principal et place l'alias renvoyé dans le module de jeton généré.

   Le type doit être valide pour SAML. Par exemple :

   ```
   urn:oasis:names:tc:
   SAML:2.0:assertion
   ```

2. Paramétrage de la méthode d'authentification sur le mécanisme `password`. Cette action est requise par la norme SAML.

   L'exemple de code suivant présente une partie du fichier de règles de mappage par défaut, ip_saml_20.xsl.

```
<!--
Remarque : aucun modèle principal n'est requis pour le fournisseur d'identité sous SAML 2.0 car les
identificateurs de noms sont fournis dans l'élément 'Subject' de l'assertion.
-->

 <xsl:template match="//stsuuser:AttributeList">
 <stsuuser:AttributeList>
                      <!-- Tout d'abord l'attribut de la classe de référence du contexte
d'authentification -->
  <stsuuser:Attribute name="AuthnContextClassRef" type="urn:oasis:names:tc:SAML:2.0:assertion">
   <stsuuser:Value>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</stsuuser:Value>
   </stsuuser:Attribute>
  </stsuuser:AttributeList>
 </xsl:template>
```

Figure 14. Exemple de code XSL présentant le mappage d'une identité d'utilisateur local avec un jeton SAML (à l'aide d'un alias)

3. Remplissage de l'instruction d'attribut de la vérification à l'aide des attributs de l'élément AttributeList dans In-STSUU. Ces informations deviennent des informations personnalisées du jeton.

   Des attributs personnalisés peuvent être requis par les applications qui utilisent les informations à transmettre entre les partenaires d'une fédération.

Mappe un jeton SAML 2.0 avec une identité locale

Le fournisseur de services reçoit un jeton SAML 2.0. Tivoli Federated Identity Manager convertit le contenu du jeton en un document STSUU conforme au schéma d'utilisateur universel STS (Security Token Service).

Tableau 22. Informations de jeton SAML converties en document d'utilisateur universel STS

Informations de jeton SAML	**Elément STSUUSER**
AuthenticationStatement/Subject/NameIdentifier	Principal Attr: Name
Attributs personnalisés supplémentaires	AttributeList (facultatif)

Le module de jeton lit le jeton et extrait l'élément NameIdentifier. Le module de jeton transmet l'élément NameIdentifier (alias) au service d'alias. Le service d'alias convertit l'alias reçu en identité locale. Le module de jeton place l'identité locale dans l'élément Principal du document STSUU.

- L'alias NameIdentifier renvoyé sert à spécifier l'attribut `name` de l'élément Principal, qui est l'ID utilisateur local.

  L'exemple de code suivant présente l'affectation d'une valeur définie pour le nom Principal. Cet exemple de code est issu du fichier de mappage par défaut, sp_saml_20.xsl.

```
<!--
  Ce modèle remplace le nom de principal par le nom local de l'utilisateur.
 -->
 <xsl:template match="//stsuuser:Principal/stsuuser:Attribute[@name='name']">
  <stsuuser:Attribute name="name" type="urn:ibm:names:ITFIM:5.1:accessmanager">
   <stsuuser:Value>
    <xsl:value-of select="//stsuuser:Principal/stsuuser:Attribute[@name='name']/stsuuser:Value"/>
   </stsuuser:Value>
  </stsuuser:Attribute>
 </xsl:template>
```

Figure 15. Exemple de code XSL présentant l'affectation d'une valeur pour le nom Principal d'un jeton SAML 2.0.

- D'autres informations issues du jeton servent à remplir la zone Attributes de l'élément AttributeList.

  L'exemple de code suivant présente l'affectation facultative de valeurs supplémentaires aux attributs. Cet exemple de code est issu du fichier de mappage par défaut, sp_saml_20.xsl.

```
<xsl:variable name="department">
<xsl:value-of select="//stsuuser:AttributeList/stsuuser:Attribute[@name='Department']/stsuuser:Value"/>
 </xsl:variable>

<xsl:template match="//stsuuser:AttributeList">
 <stsuuser:AttributeList>
  <stsuuser:Attribute type="urn:ibm:names:ITFIM:5.1:accessmanager">
   <xsl:attribute name="Department">
    <stsuuser:Value>
  <xsl:value-of select="//stsuuser:AttributeList/stsuuser:Attribute[@name='Department']
  /stsuuser:Value"/>
    </stsuuser:Value>
   </stsuuser:Attribute>
 </stsuuser:AttributeList>
</xsl:template>
```

Figure 16. Exemple de code XSL présentant l'élément AttributeList pour un jeton SAML 2.0.

Chapitre 16. Requête d'attribut SAML 2.0

La fonction de requête d'attribut SAML 2.0 étend la fonction du protocole SAML 2.0. La fonction SAML 2.0 traditionnel nécessite que le fournisseur d'identité envoie le partenaire de fédération *tous* les attributs utilisateur requis. Les attributs sont inclus dans le cadre de l'assertion générée durant le flux de connexion unique.

La fonction de requête d'attribut SAML 2.0 supprime cette limitation. Les administrateurs pour les fournisseurs d'identité peuvent seulement inclure au flux de connexion unique les attributs utilisés par la plupart des applications cibles. Les applications peuvent utiliser un flux de requête d'attribut SAML 2.0 pour obtenir des conditions requises d'attribut ou des valeurs spécialisées.

La prise en charge de requête d'attribut fournit un ensemble d'attributs de base à l'établissement du contexte d'authentification initial. Vous pouvez demander des informations utilisateur selon nécessaire durant l'opération d'exécution de l'application. Différentes applications requièrent des informations utilisateur différentes. Par exemple, les applications nécessitant une autorisation à grains fins. requièrent des droits utilisateur spécifiques pour pendre les décisions d'autorisation.

La requête d'attribut prend en charge les modes suivants :

Mode direct
: L'application de la requête émet un appel direct au fournisseur d'identité pour obtenir les attributs requis.

Mode pour le compte
: L'application de requête contacte le fournisseur de service, qui transfère la requête d'attribut au fournisseur d'identité.

Mode direct

En mode direct, l'application de requête envoie une requête AttributeQuery au noeud final SOAP de fédération SAML 2.0 au niveau du fournisseur d'identité. Le protocole délégué SOAP termine les actions de protocole nécessaires et émet une assertion SAML. La fonction de requête d'attribut SAML utilise le module STS de requête d'attribut pour émettre l'assertion.

le mode direct nécessite que l'application (demandeur d'attribut) soit connue du fournisseur d'identité. Pour qu'une application soit connue au niveau du fournisseur d'identité, vous devez importer les métadonnées de requête à l'aide de la commande d'interface de ligne de commande `manageItfimPartner`.

La flux de connexion unique pour le mode direct est :

1. L'utilisateur nécessite l'accès à une ressource ou application et lance le flux de connexion unique fédérée.
2. Le fournisseur d'identité authentifie l'utilisateur et émet une assertion SAML avec un sous-ensemble d'attributs requis par la plupart des applications ou ressources.
3. L'application ou la ressource détermine si d'autres attributs sont requis. Si c'est le cas, l'application émet une requête `AttributeQuery` au fournisseur d'identité.

4. Le fournisseur d'identité renvoie une assertion SAML avec les attributs requis.
5. L'application ou la ressource obtient les attributs renvoyés par le fournisseur d'identité dans le message de réponse SAML de requête d'attribut.

Mode pour le compte

Le mode on behalf (pour le compte) exige que les applications envoient des demandes de requêtes au fournisseur de service, qui les transmet alors au fournisseur d'identité. Le fournisseur d'identité fournit les attributs requis. Le mode on behalf (pour le compte) prend en charge deux différents types de requêtes :

- Requêtes SAML 2.0 *<AttributeQuery>*

  L'application doit envoyer des messages AttributeQuery au noeud final SOAP de fournisseur de service. Si un message de requête AttributeQuery est utilisé, le fournisseur de service renvoie un message de réponse SAML avec l'assertion correspondante.
- Messages de jeton de sécurité de requête WS-Trust.

  Pour ce protocole, l'application doit envoyer des messages WS-Trust au noeud final de service de confiance. Si l'application de requête envoie un message WS-Trust, le message de réponse est un jeton d'utilisateur universel

  Remarque : Si votre application est un client WS-Trust, vous pouvez utiliser cette option plutôt qu'utiliser le protocole SAML.

Le mode on behalf (pour le compte) limite la configuration requise au niveau du fournisseur d'identité pour un grand nombre d'applications de fournisseur de service dans les attributs utilisateur de requête. Avec ce mode, le fournisseur de service représente la seule entité connue au niveau du fournisseur d'identité.

Le flux de connexion unique pour le mode on behalf (pour le compte) est le suivant :

1. L'utilisateur nécessite l'accès à une ressource ou application au niveau du fournisseur de service et lance le flux de connexion unique fédérée.
2. Le fournisseur d'identité authentifie l'utilisateur et émet une assertion SAML avec un sous-ensemble d'attributs requis par la plupart des applications ou ressources.
3. Le fournisseur de service sélectionne les attributs à rendre disponibles pour la ressource ou l'application. Le fournisseur de service crée alors la session authentifiée pour l'utilisateur.
4. L'application ou la ressource détermine si d'autres attributs sont requis. Si c'est le cas, l'application émet une valeur `AttributeQuery` ou `RequestSecurityToken` WS-Trust pour les obtenir. L'application envoie la requête au fournisseur de service. Le fournisseur de service transmet la requête au fournisseur d'identité.
5. Le fournisseur d'identité renvoie une assertion SAML avec les attributs requis.
6. L'application ou la ressource obtient les attributs renvoyés par le fournisseur d'identité dans le message de réponse SAML de requête d'attribut.Si une requête WS-Trust est utilisée, les attributs sont renvoyés à l'application client à l'aide d'un jeton d'utilisateur universel. Si la requête est une requête AttributeQuery SAML, les attributs sont renvoyés dans une réponse SAMLResponse générée par le fournisseur de service.

Partenaire de demande de requête d'attribut

La fonction de requête d'attribut définit un nouveau type de rôle. Les partenaires d'application d'une fédération SAML 2.0 peuvent maintenant agir avec un rôle de *demandeur de requête d'attribut*. Ce rôle est différent du rôle de partenaire de fournisseur de service ou d'identité.

Un demandeur de requête d'attribut représente une entité qui effectue les appels de requête `<AttributeQuery>` basés sur SOAP pour obtenir les attributs utilisateur.

Si vous comptez configurer un *partenaire de demandeur de requête d'attribut*, vous devez générer un fichier de métadonnées tel que spécifié dans la spécification SAML 2.0. Tivoli Federated Identity Manager utilise ce fichier de métadonnées pour créer le partenaire de requête d'attribut. Vous devez utiliser la commande `manageItfimPartner` pour créer le partenaire. Cette commande utilise un fichier de réponse, qui contient un paramètre qui spécifie l'emplacement du fichier de métadonnées.

Développement d'un module STS de requête d'attribut

La fonction de requête d'attribut utilise un module de jeton STS appelé *module de requête d'attribut*. Vous devez configurer le module pour la chaîne d'accréditation pour la fédération SAML 2.0.

Avant de configurer la requête d'attribut, vous devez :

1. Déterminer l'attribut souhaité par votre ressource ou application pour faire la demande à partir du fournisseur d'identité.
2. Développer un script ou module demandant les attributs. Cette requête peut être effectuée par un fichier XSLT ou JavaScript, une chaîne d'assemblage Tivoli Directory Integrator, ou un module de mappage STS personnalisé.

Limitation liée à la migration d'une version précédente de Tivoli Federated Identity Manager

Tivoli Federated Identity Manager prend en charge la migration des fédérations SAML 2.0 depuis une version précédente vers la version actuelle. La fonction de requête d'attribut n'était pas disponible dans les versions précédentes. Cela signifie que lors de la migration des fédérations SAML 2.0 depuis des versions précédentes, la requête d'attribut n'est pas automatiquement activée dans la nouvelle version.

Pour activer la requête d'attribut pour la fédération, procédez comme suit après la migration de la fédération :

- Cochez la case située sur la page de propriétés de la fédération pour activer la requête d'attribut.
- Utilisez l'interface utilisateur graphique de la page de propriétés de fédération pour configurer un module de requête d'attribut.
- Utilisez l'assistant Ajouter un partenaire pour ajouter tous les partenaires qui existaient précédemment pour la fédération.

Configuration de requête d'attribut

Vous pouvez configurer les fédérations et partenaires SAML 2.0 pour prendre en charge la fonction de requête d'attribut.

Les étapes de configuration de requête d'attribut varient selon le scénario de déploiement. Le déploiement inclut la création d'une fédération et l'addition d'un partenaire à la fédération.

Lorsque vous configurez les fédérations, les partenaires de fournisseur d'identité et de service, vous pouvez utiliser une interface utilisateur graphique qui vous demande des paramètres de requête d'attribut. La section fournit des descriptions détaillées de ces paramètres.

Certains paramètres de requête d'attribut utilisent des valeurs existantes pour les fédérations SAML 2.0. Pour ces paramètres, aucune configuration supplémentaire n'est demandée pour la requête d'attribut.

Par exemple, les fournisseurs signent ou valident des assertions selon les paramètres de configuration établis pour la fédération ou le partenaire SAML 2.0. Ce dernier signe ou valide les assertions de requête d'attribut tel que requis par le partenaire de fédération. Vous n'avez pas à spécifier d'autres paramètres pour appliquer la signature ou validation.

Si vous installez SAML 2.0 avec des profils standard ou tous les profils, la signature et la validation sont automatiquement activées. Si vous sélectionnez une installation manuelle des profils, l'assistant vous invite à spécifier s'il faut signer et valider les messages. L'assistant nécessite ces paramètres, que la fonction de requête d'attribut soit activée ou pas.

Pour configurer votre fédération et partenaire en mode direct, procédez comme suit :

- «Création d'une fédération en droit d'attribut»
- «Création d'un partenaire de demande de requête d'attribut», à la page 181

Pour configurer votre fédération et partenaire en mode on behalf (pour le compte), procédez comme suit :

- «Création d'une fédération en droit d'attribut»
- «Création d'un partenaire de fournisseur d'identité ou de service pour une fédération d'autorité d'attribut», à la page 178
- «Création d'un partenaire de demande de requête d'attribut», à la page 181

Création d'une fédération en droit d'attribut

Vous pouvez utiliser la console d'administration ou l'interface de ligne de commande pour créer une fédération SAML 2.0 en droit d'autorité.

Choisissez l'une des méthodes suivantes :

- «Utilisation de la console d'administration pour créer une fédération en autorité d'attribut»
- «Utilisation de l'interface de ligne de commande pour créer une fédération en droit d'attribut», à la page 177

Utilisation de la console d'administration pour créer une fédération en autorité d'attribut

Vous pouvez utiliser la console d'administration pour créer une fédération SAML 2.0 en autorité d'attribut.

Pourquoi et quand exécuter cette tâche

La configuration pour la requête d'attribut utilise le même assistant que celui de toutes les fédérations SAML. Lorsque vous utilisez l'assistant, vous activez la requête d'attribut et êtes invité à fournir des paramètres de configuration.

Les paramètres pour la requête d'attribut sont décrits dans les feuilles de travail pour la configuration de fédération. Voir la rubrique concernant votre type de partenaire :

- «Formulaire de fournisseur d'identité SAML 2.0», à la page 196.
- «Formulaire de fournisseur de services SAML 2.0», à la page 190.

Remarque : Combinez les informations de la procédure suivante avec les instructions de configuration pas à pas des fédérations SAML 2.0 dans le Chapitre 17, «Etablissement d'une fédération SAML», à la page 185.

Procédure

1. Dans le panneau Profils de l'assistant, sélectionnez **Tous** ou **Manuel**.
2. Dans le panneau Détails du profil, accédez à Requête d'attribut et sélectionnez **Activé**. Si vous cochez cette case, de nouveaux panneaux s'affichent.
3. Dans le panneau Assertions de SAML, indiquez la durée de validité d'une assertion avant sa date d'émission. Indiquez également la durée de validité de l'assertion après émission.

   Remarque : Lorsque vous utilisez une fédération de *fournisseur de service* pour une requête d'attribut, la fédération doit émettre des assertions. Cette condition signifie que vous avez activé une requête d'attribut pour une fédération de fournisseur de service, le panneau Assertions de SAML s'affiche, et vous devez indiquer des valeurs. Lorsque vous configurez une fédération de fournisseur de service sans requête d'attribut, vous n'avez pas à définir de valeurs pour les assertions SAML.

   Le panneau Assertions de SAML s'affiche pour la création de fédération de *fournisseur d'identité* que la requête d'attribut soit sélectionné ou non. Dans ce type de fédération, les assertions SAML sont émises pour plusieurs fins.
4. Dans le panneau Sélection de module d'attribut, sélectionnez un des choix suivants :
   - Transformation XSLT ou JavaScript
   - Module Tivoli Directory Integrator
   - Module de mappage personnalisé.

   Basez votre sélection sur la méthode identifiée pour votre déploiement lorsque vous avez planifié la configuration.

Utilisation de l'interface de ligne de commande pour créer une fédération en droit d'attribut

Vous pouvez utiliser l'interface de ligne de commande pour créer une fédération SAML 2.0 en droit d'attribut.

Pourquoi et quand exécuter cette tâche

Lors de l'utilisation de l'interface de ligne de commande pour créer une fédération SAML 2, vous devez d'abord créer et renseigner un fichier de réponses de

fédération SAML 2. Pour établir la fédération SAML 2 en droit d'attribut, vous devez définir les valeurs dans le fichier de réponses pour les paramètres suivants :

- `AttributeQueryMappingRule`
- `AttributeQueryMappingRuleFileName`
- `AttributeAuthorityEnabled`
- `SignAttributeQueryRequest`
- `SignAttributeQueryResponse`

Pour des descriptions des paramètres nécessaires, voir «Paramètres de fichier de réponses de fédération de requête d'attribut SAML 2.0», à la page 182

Pour plus d'informations sur l'utilisation de l'interface de ligne de commande pour créer une fédération SAML 2 et un fichier de réponses, voir le document *IBM Tivoli Federated Identity Manager - Guide d'administration*.

Procédure

1. Créez un fichier de réponses SAML 2.

   Par exemple, pour créer un fichier de réponses SAML 2 basé sur une fédération existante :

   ```
   $AdminTask manageItfimFederation {-operation createResponseFile
   -fimDomainName domain1 -federationName idpsaml2
   -fileId c:\temp\saml2idp.rsp}
   ```

2. Editez le fichier de réponses SAML 2 pour définir les paramètres de requête d'attribut.

   Dans l'exemple, le fichier de réponses est `c:\temp\saml2idp.rsp`

3. Créez la fédération SAML 2 en droit d'attribut.

   Pour créer une fédération de fournisseur d'identité ou de fournisseur de service activé pour la requête d'attribut, utilisez la syntaxe standard. Aucune autre option n'est à spécifier.

   Par exemple, si le fichier de réponses est `c:\temp\saml2idp.rsp`:

   ```
   $AdminTask manageItfimFederation { -operation create -fimDomainName domain1
   -fileId c:\temp\saml2idp.rsp}
   ```

Création d'un partenaire de fournisseur d'identité ou de service pour une fédération d'autorité d'attribut

Vous pouvez créer un partenaire de fournisseur d'identité ou de service pour une fédération SAML 2.0 configurée en autorité d'attribut.

Lorsqu'une fédération a été configurée sur une autorité d'attribut, vous pouvez ajouter des partenaires des types suivants :

- Partenaire de fournisseur de service

  Ajoutez un partenaire de fournisseur de service à une fédération de fournisseur d'identité. Vous pouvez configurer ce partenaire pour échanger des requêtes-réponses de demandes d'attributs avec le fournisseur de fédération.

- Partenaire de fournisseur d'identité

  Ajoutez un partenaire de fournisseur d'identité dans une fédération de fournisseurs de service.Vous pouvez configurer ce partenaire pour échanger des requêtes-réponses de demandes d'attributs avec le fournisseur de fédération.

- Partenaire de demande de requête d'attribut

  Ce type de partenaire représente un cas spécial à utiliser lorsque la ressource ou l'application de requête ne dispose pas de Tivoli Federated Identity Manager.

  Remarque : Les instructions de cette rubrique ne concernant pas les partenaires de requête de demande d'attribut. Voir «Création d'un partenaire de demande de requête d'attribut», à la page 181.

Pour ajouter un partenaire de fournisseur d'identité ou de service, voir :

- «Utilisation de la console d'administration pour créer un partenaire de fournisseur d'identité ou fournisseur de service»
- «Utilisation de l'interface de ligne de commande pour créer un partenaire de fournisseur d'identité ou fournisseur de service», à la page 180

Utilisation de la console d'administration pour créer un partenaire de fournisseur d'identité ou fournisseur de service

Vous pouvez utiliser la console d'administration pour créer un partenaire de fournisseur d'identité ou fournisseur de service.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser l'assistant Ajouter un partenaire pour ajouter un partenaire de fournisseur de service ou d'identité à une fédération. Cet assistant est également utilisé pour ajouter des partenaires SAML 2.0 sans requête d'attribut.

Lorsque vous utilisez l'assistant pour ajouter un partenaire à une fédération, le programme de configuration détermine si la fédération est configurée en tant qu'autorité de requête d'attribut. Si la fédération est une autorité de requête d'attribut, d'autres panneaux vous invitent à entrer davantage d'informations.

Les panneaux de configuration sont légèrement différents pour les partenaires de fournisseur d'identité ou de service. Voir la table suivante.

Panneau de configuration	**Type de partenaire**	**Description**
Assertions SAML	Partenaire de fournisseur d'identité pour une fédération de fournisseur de service *uniquement*	Le panneau de configuration d'assertions SAML vous permet de spécifier les attributs à inclure à l'assertion. La valeur par défaut est d'inclure tous les attributs. Vous pouvez utiliser ce paramètre pour spécifier un ensemble de base d'attributs. Le panneau d'assertions SAML vous permet également de spécifier les attributs à chiffrer et les algorithmes de chiffrage à utiliser.

Panneau de configuration	Type de partenaire	Description
Sélection de module d'attribut	Partenaire de fournisseur d'identité pour une fédération de fournisseur de service et partenaire de fournisseur de service pour une fédération de partenaire d'identité	Dans le panneau Sélection de module d'attribut, vous devez sélectionner un des éléments suivants : • Transformation XSLT ou JavaScript • Module Tivoli Directory Integrator • Module de mappage personnalisé. Basez votre sélection sur la méthode identifiée pour votre déploiement lorsque vous avez planifié la configuration.

Les paramètres pour la configuration de partenaire pour la requête d'attribut sont décrits dans la feuille de travail pour la configuration de partenaire SAML 2.0. Voir la rubrique pour votre type de partenaire :

- «Formulaire de fournisseur d'identité partenaire SAML 2.0», à la page 226
- «Formulaire de fournisseur de services partenaire SAML 2.0», à la page 220

L'assistant d'interface utilisateur graphique pour l'ajout de partenaires SAML 2.0 inclut les panneaux pour la configuration de requête d'attribut. Pour configurer le partenaire de fournisseur d'identité ou de service, voir les instructions SAML 2.0 : «Ajout à votre partenaire», à la page 234

Utilisation de l'interface de ligne de commande pour créer un partenaire de fournisseur d'identité ou fournisseur de service

Vous pouvez créer un partenaire de fournisseur d'identité ou de service pour une fédération SAML 2.0 configurée en autorité d'attribut.

Pourquoi et quand exécuter cette tâche

Lors de l'utilisation de l'interface de ligne de commande pour créer un partenaire, vous devez d'abord créer et renseigner un fichier de réponses de partenaire SAML 2. Pour configurer les partenaires afin d'utilisateur la fonction de requête d'attribut, vous devez définir les valeurs pour les paramètres suivants dans le fichier de réponses :

- `AttributeQueryMappingRule`
- `AttributeQueryMappingRuleFileName`
- `ValidateAttributeQueryRequest`
- `ValidateAttributeQueryResponse`

Pour plus d'informations sur l'utilisation de l'interface de ligne de commande pour créer un partenaire SAML 2 et un fichier de réponses de partenaire, voir le document *IBM Tivoli Federated Identity Manager - Guide d'administration*.

Procédure

1. Créez un fichier de réponses de partenaire SAML 2.

Par exemple, pour créer un fichier de réponses de partenaire SAML 2 basé sur un partenaire existant :

```
$AdminTask manageItfimPartner {-operation createResponseFile
-fimDomainName domain1  -federationName fed1
-partnerName idppartner -fileId c:\temp\saml2idp.rsp }
```

2. Editez le fichier de réponses de partenaire SAML 2 pour définir les paramètres de requête d'attribut.

   Dans l'exemple, le fichier de réponses est `c:\temp\saml2idp.rsp`

   Pour des descriptions des paramètres de fichier de réponses de requête, voir «Paramètres de fichier de réponses de partenaire de requête d'attribut SAML 2.0», à la page 183

3. Pour créer un partenaire de fournisseur d'identité configuré pour une requête d'attribut, utilisez la syntaxe standard.

   Vous pouvez éventuellement spécifier le rôle de partenaire dans la ligne de commande. Vous n'avez pas à spécifier le rôle partenaire. Lorsque le rôle n'est pas spécifié, le programme définit automatiquement le rôle du partenaire basé sur le rôle de la fédération.

   Par exemple, si le fichier de réponses est `c:\temp\saml2idp.rsp` :

   ```
   $AdminTask manageItfimPartner { -operation create -fimDomainName domain1
   -federationName idpsaml2 -partnerName idpartner
   -fileId c:\temp\saml2idp.rsp
   -signingKeystorePwd testonly -encryptionKeystorePwd testonly }
   ```

   Si vous souhaitez spécifier le rôle du partenaire dans la ligne de commande, ajoutez l'option `-partnerRole`, et indiquez `sp` ou `idp`. Par exemple, pour spécifier un partenaire de fournisseur de service :

   ```
   $AdminTask manageItfimPartner { -operation create -fimDomainName domain1
   -federationName idpsaml2 -partnerName idpartner
   -partnerRole sp
   -fileId c:\temp\saml2sp.rsp
   -signingKeystorePwd testonly -encryptionKeystorePwd testonly }
   ```

Création d'un partenaire de demande de requête d'attribut

Utilisez l'interface de ligne de commande pour créer un partenaire de demande de requête d'attribut.

Pourquoi et quand exécuter cette tâche

Vous devez utiliser l'interface de ligne de commande pour ajouter un partenaire de demande de requête d'attribut à une fédération. L'interface utilisateur graphique d'administration ne fournit pas d'assistant pour cette tâche.

Utilisez la commande `manageItfimPartner` pour créer le partenaire. Cette commande prend en charge un paramètre de rôle de partenaire `qr` qui indique qu'un partenaire de demande de requête va être créé.

Procédure

1. Créez un fichier de réponses de partenaire SAML 2.

   Par exemple, pour créer un fichier de réponses de partenaire de demande de requête d'attribut SAML 2 basé sur un partenaire existant :

   ```
   $AdminTask manageItfimPartner { -operation createResponseFile
   -fimDomainName fimipdomain  -federationName saml20ip
   -partnerRole qr -fileId /downloads/qr.out }
   ```

2. Editez le fichier de réponses de sorte à afficher l'emplacement du fichier de métadonnées à partir du partenaire de demande de requête d'attribut. Ce nom de fichier est un paramètre du fichier de réponses. Vous devez également ajouter des informations spécifiques au partenaire.

   Pour plus d'informations sur l'utilisation de l'interface de ligne de commande pour créer un partenaire SAML 2 et un fichier de réponses de partenaire, voir le document *IBM Tivoli Federated Identity Manager - Guide d'administration*.

3. Créez un partenaire de demande de requête d'attribut :

```
$AdminTask manageItfimPartner { -operation create
-fimDomainName fimipdomain
-federationName saml20ip -partnerName samlqr
-partnerRole qr -fileId /downloads/qr.out
-signingKeystorePwd testonly
-encryptionKeystorePwd testonly}
```

Paramètres de fichier de réponses de fédération de requête d'attribut SAML 2.0

Le fichier de réponses de fédération SAML 2.0 contient des paramètres utilisés par la requête d'attribut.

Tableau 23. Paramètres de requête d'attribut pour le fichier de réponse de fédération

Paramètre	Valeur	Description
AttributeQueryMappingRule	*contenu du fichier de règle de mappage*	Contient le contenu de la règle de mappage (XSL) nécessaire au formatage correct de la règle, afin que cette dernière puisse être incluse dans un fichier de réponses XML. Utilisez cette propriété pour spécifier une règle de mappage sans utiliser de fichier sur le système de fichiers. Utilisez également cette propriété si vous modifiez une fédération. Si vous souhaitez éditer la règle XSLT en fichier normal, indiquez-le dans le fichier de réponses à l'aide de la propriété **AttributeQueryMappingRuleFileName**. Cette règle est utilisée pour les opérations de requête d'attribut.
AttributeQueryMappingRuleFileName	*chemin et nom de fichier*	Indique le nom du chemin d'accès vers un fichier XSLT utilisé en règle de mappage. S'il est défini, il a la priorité sur la priorité **AttributeQueryMappingRule**. Cette règle est utilisée pour les opérations de requête d'attribut.
AttributeAuthorityEnabled	*true ou false*	Indique si la fonction de requête d'attribut est configurée dans la fédération. La valeur `true` active la requête d'attribut. La valeur `false` désactive la requête d'attribut. Par défaut : false
SignAttributeQueryResponse	*true ou false*	Indique si les réponses de requête d'attribut sont signées.
SignAttributeQueryRequest	*true ou false*	Indique si les requêtes d'analyse d'attributs sont signées.

Paramètres de fichier de réponses de partenaire de requête d'attribut SAML 2.0

Le fichier de réponses de partenaire SAML 2.0 contient des paramètres utilisés par la requête d'attribut.

Tableau 24. Paramètres de requête d'attribut pour le fichier de réponse de partenaire

Paramètre	Valeur	Description
AttributeQueryMappingRule	*contenu du fichier de règle de mappage*	Contient le contenu de la règle de mappage (XSL) nécessaire au formatage correct de la règle, afin que cette dernière puisse être incluse dans un fichier de réponses XML. Utilisez cette propriété si vous souhaitez spécifier une règle de mappage sans utiliser de fichier sur le système de fichiers. Utilisez également cette propriété si vous modifiez une fédération. Si vous souhaitez éditer la règle XSLT en fichier normal, indiquez-le dans le fichier de réponses à l'aide de la propriété **AttributeQueryMappingRuleFileName**. Cette règle est utilisée pour les opérations de requête d'attribut.
AttributeQueryMappingRuleFileName	*chemin et nom de fichier*	Indique le nom du chemin d'accès vers un fichier XSLT utilisé en règle de mappage. S'il est défini, il a la priorité sur la priorité **AttributeQueryMappingRule**. Cette règle est utilisée pour les opérations de requête d'attribut.
ValidateAttributeQueryResponse	*true ou false*	Indique que la validation des signatures de partenaire a lieu sur les réponses de requête d'attribut reçues. Une erreur se produit si le message n'est pas signé.
ValidateAttributeQueryRequest	*true ou false*	Indique qu'une demande d'analyse d'attributs reçue de la signature du partenaire est validée. Une erreur se produit si le message n'est pas signé.

Chapitre 17. Etablissement d'une fédération SAML

Pour configurer votre fédération, procédez comme suit :

1. «Rassemblement des informations relatives à la configuration de votre fédération».
2. «Création de votre rôle dans la fédération», à la page 202.
3. «Délivrance d'instructions à votre partenaire», à la page 204.
4. «Obtention des données de configuration de fédération de la part de votre partenaire», à la page 207.
5. «Ajout à votre partenaire», à la page 234.
6. «Transmission des propriétés de la fédération au partenaire», à la page 236.

Rassemblement des informations relatives à la configuration de votre fédération

L'assistant Fédération vous invite à indiquer les informations utilisées dans votre fédération. Avant de démarrer l'assistant, préparez le processus de configuration en réunissant les informations correspondantes dans le formulaire approprié.

Pourquoi et quand exécuter cette tâche

Sélectionnez un formulaire en fonction de la norme SAML que vous souhaitez utiliser dans la fédération, ainsi que le rôle que vous tenez dans cette dernière.

- «Formulaire de fournisseur de services IDP SAML 1.x»
- «Formulaire de fournisseur d'identité SAML 1.x», à la page 187
- «Formulaire de fournisseur de services SAML 2.0», à la page 190
- «Formulaire de fournisseur d'identité SAML 2.0», à la page 196

Formulaire de fournisseur de services IDP SAML 1.x

Si vous devez être le fournisseur de services d'une fédération SAML 1.0 ou SAML 1.1, enregistrez vos informations de configuration dans les tables suivantes.

Tableau 25. Informations générales pour le fournisseur de services dans la fédération SAML 1.x

Informations générales	Description	Votre valeur
Nom de la fédération	Nom unique attribué à la fédération.	
Rôle	Votre rôle dans la fédération. (Dans les présentes instructions, vous êtes le fournisseur de services.)	Fournisseur de services

Tableau 26. Informations de contact pour le fournisseur de services dans la fédération SAML 1.x

Personne à contacter	Description	Votre valeur
Nom de l'entreprise, adresse URL et nom de contact de l'entreprise.	Nom de votre entreprise ainsi que, le cas échéant, d'autres informations relatives au contact associé avec votre rôle dans la fédération.	

Tableau 27. Protocole de fédération pour le fournisseur de services dans la fédération SAML 1.x

Protocole de fédération	Description	Votre valeur
Protocole	Protocole SAML utilisé par votre partenaire et vous-même dans la fédération.	Vous pouvez choisir une des options suivantes : • SAML 1.0 • SAML 1.1

Tableau 28. Informations du serveur point de contact pour le fournisseur de services dans la fédération SAML 1.x

Serveur point de contact	Description	Votre valeur
URL du serveur point de contact	Adresse URL donnant accès aux noeuds finals sur le serveur point de contact.	

Tableau 29. Informations de signature pour le fournisseur de services dans la fédération SAML 1.x

Signatures	Description	Votre valeur
Signer les requêtes de résolution d'artefact	Case à cocher indiquant que vous signerez les messages de requête. Valeur par défaut : Aucune signature. La case n'est pas cochée.	Vous pouvez choisir une des options suivantes : • Signer les messages de requête (cochez la case). • Ne pas signer les messages de requête (ne pas cocher la case).
Sélectionner la clé de signature • Fichier de clés du service de clés Tivoli Federated Identity Manager, dans lequel la clé est stockée • Mot de passe du fichier de clés • Clé privée utilisée pour la signature des messages de requête	Si vous cochez cette case, vous devez indiquer la clé de signature à utiliser pour signer les requêtes. **Remarque :** Avant d'effectuer cette tâche, veillez à créer la clé et à l'importer dans le fichier de clés approprié du service de clés Tivoli Federated Identity Manager. Pour plus d'informations, voir Chapitre 6, «Configuration de la sécurité des messages», à la page 29.	Nom de fichiers de clés : Mot de passe du fichier de clés : Nom d'alias de clé :

Tableau 30. Informations de mappage d'identité pour le fournisseur de services dans la fédération SAML 1.x

Mappage d'identité	Description	Votre valeur
Options de mappage d'identité Vous pouvez choisir une des options suivantes : • Fichier de transformation XSL (XSLT) contenant les règles de mappage • Module de mappage personnalisé	Type de mappage d'identité utilisé. Vous devez savoir si vous allez utiliser un fichier XSLT pour le mappage d'identité ou un module de mappage personnalisé. Le mappage personnalisé est une option avancée. Si vous souhaitez utiliser cette option, vous devez créer votre module de mappage et l'ajouter à l'environnement en tant que module type et module d'instance *avant* de pouvoir l'utiliser dans votre configuration. Si vous choisissez d'utiliser un fichier XSLT, vous devez préparer le fichier pour la fédération. .	L'une des valeurs suivantes : • Fichier XSLT (chemin et nom): • Nom de l'instance de module de mappage personnalisée :

Une fois que vous avez complété les tables, poursuivez avec les instructions de la rubrique «Création de votre rôle dans la fédération», à la page 202.

Formulaire de fournisseur d'identité SAML 1.x

Si vous devez être le fournisseur d'identité d'une fédération SAML 1.0 ou SAML 1.1, enregistrez vos informations de configuration dans les tables suivantes.

Tableau 31. Informations générales pour le fournisseur d'identité dans la fédération SAML 1.x

Informations générales	Description	Votre valeur
Nom de la fédération	Nom unique attribué à la fédération.	
Rôle	Votre rôle dans la fédération. (Dans les présentes instructions, vous êtes le fournisseur d'identité.)	Fournisseur d'identité

Tableau 32. Informations de contact pour le fournisseur d'identité dans la fédération SAML 1.x

Personne à contacter	Description	Vos valeurs
Nom de l'entreprise, adresse URL et nom de contact de l'entreprise.	Nom de l'entreprise et, le cas échéant, autres informations relatives au contact associé à la fédération.	Nom de l'entreprise :

Tableau 33. Informations sur le protocole de fédération pour le fournisseur d'identité dans la fédération SAML 1.x

Protocole de fédération	Description	Votre valeur
Protocole	Protocole SAML utilisé par votre partenaire et vous-même dans la fédération.	Vous pouvez choisir une des options suivantes : • SAML 1.0 • SAML 1.1

Tableau 34. Serveur point de contact pour le fournisseur de services dans la fédération SAML 1.x

Serveur point de contact	Description	Votre valeur
URL du serveur point de contact	Adresse URL donnant accès aux noeuds finals sur le serveur point de contact.	

Tableau 35. Informations de signature pour le fournisseur d'identité dans la fédération SAML 1.x

Signatures	Description	Votre valeur
Options de signature : • **Les messages SAML pour le profil POST du navigateur sont signés** (obligatoire) • **Signer les messages SAML du profil d'artefact** (facultatif)	• Lorsque le POST du navigateur est utilisé en tant que profil, les messages SAML doivent être signés. Cette option est donc présélectionnée et ne peut pas être désélectionnée. • Il est possible de signer également les messages SAML lorsque l'artefact du navigateur est utilisé.	Vous pouvez choisir une des options suivantes : • Signer les messages d'artefact du navigateur (cochez la case). • Ne pas signer les messages d'artefact du navigateur (ne pas cocher la case).
Sélectionner la clé de signature • Fichier de clés du service de clés Tivoli Federated Identity Manager, dans lequel la clé est stockée • Mot de passe du fichier de clés • Clé privée utilisée pour la signature	Etant donné que les messages POST du navigateur doivent être signés, vous êtes tenu de fournir une clé de signature. Si vous choisissez de signer également les messages lorsque l'artefact du navigateur est utilisé, cette signature s'effectue au moyen de la même clé. **Remarque :** Avant d'effectuer cette tâche, veillez à créer la clé et à l'importer dans le fichier de clés approprié du service de clés Tivoli Federated Identity Manager. Pour plus d'informations, voir Chapitre 6, «Configuration de la sécurité des messages», à la page 29.	Nom de fichiers de clés : Mot de passe du fichier de clés : Nom d'alias de clé :

Tableau 36. Informations sur les paramètres de message SAML pour le fournisseur d'identité dans la fédération SAML 1.x

Paramètres des messages SAML	Description	Votre valeur
URL du service de résolution des artefacts	Adresse URL de votre noeud final de résolution d'artefacts. **Remarque :** La valeur de cette zone est renseignée automatiquement à l'aide de l'URL du serveur point de contact que vous avez définie précédemment.	
Durée de mise en cache d'artefact (en secondes)	Durée de mise en cache d'artefact en secondes. Valeur par défaut : 30 secondes.	
Autoriser l'extension IBM Protocol	Vous devez indiquer si vous autorisez l'utilisation de l'extension IBM PROTOCOL. Cette extension autorise un paramètre de chaîne de requête qui indique si l'artefact du navigateur (Browser Artifact) ou le profil POST du navigateur (Browser POST) doivent être utilisés. Pour plus d'informations, voir «SAML 1.x», à la page 147.	Vous pouvez choisir une des options suivantes : • Autoriser l'extension IBM Protocol (cochez la case). • Ne pas autoriser l'extension Protocol (ne pas cocher la case).

Tableau 37. Informations sur les paramètres de jetons pour le fournisseur d'identité dans la fédération SAML 1.x

Configuration des paramètres de jeton	Description	Votre valeur
Durée de validité (en secondes) d'une assertion avant sa date d'émission	Durée en secondes pendant laquelle une assertion est considérée comme valide avant sa date de création. Valeur par défaut : 60	
Durée de validité de l'assertion après émission	Durée en secondes pendant laquelle une assertion est considérée comme valide après sa date de création. Valeur par défaut : 60	

Tableau 38. Informations de mappage d'identité pour le fournisseur d'identité dans la fédération SAML 1.x

Mappage d'identité	Description	Votre valeur
Options de mappage d'identité Vous pouvez choisir une des options suivantes : • Fichier de transformation XSL (XSLT) contenant les règles de mappage • Module de mappage personnalisé	Type de mappage d'identité utilisé. Vous devez savoir si vous allez utiliser un fichier XSLT pour le mappage d'identité ou un module de mappage personnalisé. Le mappage personnalisé est une option avancée. Si vous souhaitez utiliser cette option, vous devez créer votre module de mappage et l'ajouter à l'environnement en tant que module type et module d'instance *avant* de pouvoir l'utiliser dans votre configuration. Si vous choisissez d'utiliser un fichier XSLT, vous devez préparer le fichier pour la fédération.	L'une des valeurs suivantes : • Fichier XSLT (chemin et nom): • Nom de l'instance de module de mappage personnalisée :

Une fois que vous avez complété les tables, poursuivez avec les instructions de la rubrique «Création de votre rôle dans la fédération», à la page 202.

Formulaire de fournisseur de services SAML 2.0

Si vous devez être le fournisseur de services d'une fédération SAML 2.0, enregistrez vos informations de configuration dans les tables suivantes.

Tableau 39. Informations générales pour le fournisseur de services dans la fédération SAML 2.0

Informations générales	Description	Votre valeur
Nom de la fédération	Nom unique attribué à la fédération.	
Rôle	Votre rôle dans la fédération. (Dans les présentes instructions, vous êtes le fournisseur de services.)	Fournisseur de services

Tableau 40. Informations de contact pour le fournisseur de services dans la fédération SAML 2.0

Personne à contacter	Description	Votre valeur
Nom de l'entreprise, adresse URL et nom de contact de l'entreprise.	Nom de votre entreprise ainsi que, le cas échéant, d'autres informations relatives au contact associé avec votre rôle dans la fédération.	

Tableau 41. Protocole de fédération pour le fournisseur de services dans la fédération SAML 2.0

Protocole de fédération	Description	Votre valeur
Protocole	Protocole SAML utilisé par votre partenaire et vous-même dans la fédération.	SAML 2.0

Tableau 42. Informations du serveur point de contact pour le fournisseur de services dans la fédération SAML 2.0

Serveur point de contact	Description	Votre valeur
URL du serveur point de contact	Adresse URL donnant accès aux noeuds finals sur le serveur point de contact.	

Tableau 43. Sélection de profil et informations de configuration pour le fournisseur de services dans la fédération SAML 2.0

Sélection de profil	Description	Votre valeur
Options de profil SAML 2.0 : Choisissez l'une des options de profil suivantes :	Profil de votre fédération. Pour plus d'informations sur les profils, voir «SAML 2.0», à la page 149.	Vous pouvez choisir une des options suivantes : • Basique • Typique • Tous • Manuel
Basique : Connexion unique de navigateur Web, déconnexion unique	Ce paramètre active les profils suivants avec toutes les liaisons prises en charge : • Liaison SSO de navigateur Web • Déconnexion unique (SLO)	(aucune valeur supplémentaire requise)
Typique : Connexion unique de navigateur Web, déconnexion unique et Gestion des identificateurs de nom	Ce paramètre active les profils suivants avec toutes les liaisons prises en charge : • Liaison SSO de navigateur Web • Déconnexion unique (SLO) • Client ou proxy évolué • Gestion des identificateurs de nom	(aucune valeur supplémentaire requise)

Tableau 43. Sélection de profil et informations de configuration pour le fournisseur de services dans la fédération SAML 2.0 (suite)

Sélection de profil	Description	Votre valeur
Activer tous les profils et toutes les liaisons	Si vous sélectionnez l'option **Activer tous les profils et toutes les liaisons**, vous devez être prêt à fournir les informations suivantes dans les panneaux successifs : **Paramètres de reconnaissance du fournisseur d'identité :** • Nom de domaine commun • URL du service de cookie de domaine commun **Panneau Proxy client amélioré :** • En-têtes HTTP	**Paramètres de reconnaissance du fournisseur d'identité** • Nom de domaine commun : • URL du service de cookie de domaine commun : **Proxy client amélioré** En-têtes HTTP :
Manuel : Choisissez des profils et des liaisons individuels	Si vous choisissez l'option **Manuel**, vous devez être prêt à sélectionner des profils individuels et des liaisons prises en charge.	Profils et liaisons :

Tableau 44. Informations de signature pour le fournisseur de services dans la fédération SAML 2.0

Signatures	Description	Votre valeur
Demander une signature sur les messages et assertions entrants	Case à cocher indiquant que votre partenaire devra utiliser sa clé privée pour signer le message et l'assertion. Par défaut, la case est cochée.	Vous pouvez choisir une des options suivantes : • Le partenaire signe (la case est cochée). • Le partenaire ne signe pas (la case n'est pas cochée).
Sélectionner les messages et assertions sortants qui nécessitent une signature	Boutons indiquant quels messages sortants doivent être signés par vos soins. Lorsque le paramètre par défaut est sélectionné, l'ensemble des messages et assertions SAML sortants classiques (à l'exception des objets ArtifactResponse et AuthnResponse) doivent être signés.	Vous pouvez choisir une des options suivantes : • Les ensembles de messages SAML sortants classiques sont signés. • Toutes les assertions et tous les messages SAML sortants sont signés. • Aucune assertion ni aucun message SAML sortant ne sont signés.

Tableau 44. Informations de signature pour le fournisseur de services dans la fédération SAML 2.0 (suite)

Signatures	Description	Votre valeur
Sélectionner la clé de signature • Fichier de clés du service de clés Tivoli Federated Identity Manager, dans lequel la clé est stockée • Mot de passe du fichier de clés • Clé privée utilisée pour la signature des messages	Si vous devez signer les messages et assertions, vous devez indiquer la clé à utiliser pour les signer. **Remarque :** Avant d'effectuer cette tâche, veillez à créer la clé et à l'importer dans le fichier de clés approprié du service de clés Tivoli Federated Identity Manager. Pour plus d'informations, voir Chapitre 6, «Configuration de la sécurité des messages», à la page 29.	Nom de fichiers de clés : Mot de passe du fichier de clés : Nom d'alias de clé :

Tableau 45. Informations de chiffrement pour le fournisseur de services dans la fédération SAML 2.0

Chiffrement	Description	Votre valeur
Clé de chiffrement: • Fichier de clés du service de clés Tivoli Federated Identity Manager, dans lequel la clé est stockée • Mot de passe du fichier de clés • Biclé publique/privée utilisée pour les données reçues en provenance de votre partenaire.	Biclé publique/privée utilisée pour le chiffrement. Votre partenaire utilisera la clé publique pour chiffrer les données à votre intention. Vous utiliserez la clé privée pour déchiffrer les données qui vous sont envoyées par votre partenaire. Vous devez indiquer la paire de clés utilisée. **Remarque :** Avant d'effectuer cette tâche, veillez à créer la clé et à l'importer dans le fichier de clés approprié du service de clés Tivoli Federated Identity Manager. .	Nom de fichiers de clés : Mot de passe du fichier de clés : Nom d'alias de clé :

Tableau 46. Paramètres des messages SAML pour le fournisseur de services dans la fédération SAML 2.0

Paramètres des messages	Description	Votre valeur
Options des messages : • Durée de vie du message (en secondes) • Durée de vie de l'artefact (en secondes) • Délai d'expiration de session	Intervalle de temps, spécifié en secondes, pendant lequel les messages, artefacts et sessions sont valides. Les valeurs par défaut sont les suivantes : • Durée de vie des messages : 300 • Durée de vue des artefacts : 120 • Délai d'expiration de session : 7200	Durée de vie du message (en secondes) : Durée de vie de l'artefact (en secondes) : Délai d'expiration de session :
Options de connexion unique • Le fournisseur d'identité est autorisé avec l'utilisateur • La connexion unique est passive • Forcer le fournisseur d'identité à authentifier l'utilisateur	Spécifie la manière dont le fournisseur d'identité interagit avec les utilisateurs.	Vous pouvez choisir une des options suivantes : • Le fournisseur d'identité est autorisé avec l'utilisateur • La connexion unique est passive • Forcer le fournisseur d'identité à authentifier l'utilisateur
Noeud final SOAP	URL du point d'extrémité SOAP. Valeur par défaut : la valeur contenue dans cette zone dépend de l'URL du serveur point de contact que vous avez fournie précédemment. **Remarque :** Si aucune liaison SOAP n'est utilisée dans le profil que vous avez sélectionné, l'affichage de cette zone n'a pas lieu.	

Tableau 47. Informations de requête d'attribut pour le fournisseur de service

Requête d'attribut	Description	Votre valeur
Activé	Indique si le fournisseur est autorisé à agir en tant qu'autorité d'attribut. Si cette option est sélectionnée, le profil de requête d'attribut est activé.	
Durée d'assertion avant sa date d'émission.	Durée en secondes pendant laquelle une assertion est considérée valide avant sa date de création. Valeur par défaut : 60	

Tableau 47. Informations de requête d'attribut pour le fournisseur de service (suite)

Requête d'attribut	Description	Votre valeur
Durée de validité de l'assertion après émission	Durée en secondes pendant laquelle une assertion est considérée valide après sa date de création. Valeur par défaut : 60	

Tableau 48. Informations de mappage de requête d'attribut pour le fournisseur de services dans la fédération SAML 2.0

Mappage de requête d'attribut	Description	Votre valeur
Options de mappage de requête d'attribut Vous pouvez choisir une des options suivantes : • Fichier de transformation XSL ou JavaScript contenant les règles de mappage • Module de mappage Tivoli Directory Integrator • Module de mappage personnalisé	Type de mappage de requête d'attribut utilisé. Vous devez sélectionner un fichier XSLT, un module de mappage Tivoli Directory Integrator ou un module de mappage personnalisé. Si vous utilisez un fichier XSLT, ce dernier doit avoir été créé avant la configuration de la fédération. Le module de mappage Tivoli Directory Integrator est un module STS. Le mappage personnalisé est une option avancée. Si vous utilisez cette option, vous devez créer et ajouter un nouveau type et instance de module *avant* de pouvoir l'utiliser dans votre configuration.	L'une des valeurs suivantes : • Chemin de fichier XSLT • Module de mappage Tivoli Directory Integrator • Nom de l'instance de module de mappage personnalisée

Tableau 49. Informations de mappage d'identité pour le fournisseur de services dans la fédération SAML 2.0

Mappage d'identité	Description	Votre valeur
Options de mappage d'identité Vous pouvez choisir une des options suivantes : • Fichier de transformation XSL contenant les règles de mappage • Module de mappage personnalisé	Type de mappage d'identité utilisé. Vous devez savoir si vous allez utiliser un fichier XSLT pour le mappage d'identité ou un module de mappage personnalisé. Le mappage personnalisé est une option avancée. Si vous souhaitez utiliser cette option, vous devez créer votre module de mappage et l'ajouter à l'environnement en tant que module type et module d'instance *avant* de pouvoir l'utiliser dans votre configuration. Si vous choisissez d'utiliser un fichier XSLT, vous devez préparer le fichier pour la fédération.	L'une des valeurs suivantes : • Fichier XSLT (chemin et nom): • Nom de l'instance de module de mappage personnalisée :

Une fois que vous avez complété les tables, poursuivez avec les instructions de la rubrique «Création de votre rôle dans la fédération», à la page 202.

Formulaire de fournisseur d'identité SAML 2.0

Si vous devez être le fournisseur d'identité d'une fédération SAML 2.0, enregistrez vos informations de configuration dans les tables suivantes.

Tableau 50. Informations générales pour le fournisseur d'identité dans la fédération SAML 2.0

Informations générales	Description	Votre valeur
Nom de la fédération	Nom unique attribué à la fédération.	
Rôle	Votre rôle dans la fédération. (Dans les présentes instructions, vous êtes le fournisseur d'identité.)	Fournisseur d'identité

Tableau 51. Informations de contact pour le fournisseur d'identité dans la fédération SAML 2.0

Personne à contacter	Description	Votre valeur
Nom de l'entreprise, adresse URL et nom de contact de l'entreprise.	Nom de votre entreprise ainsi que, le cas échéant, d'autres informations relatives au contact associé avec votre rôle dans la fédération.	

Tableau 52. Protocole de fédération pour le fournisseur d'identité dans la fédération SAML 2.0

Protocole de fédération	Description	Votre valeur
Protocole	Protocole SAML utilisé par votre partenaire et vous-même dans la fédération.	SAML 2.0

Tableau 53. Informations du serveur point de contact pour le fournisseur d'identité dans la fédération SAML 2.0

Serveur point de contact	Description	Votre valeur
URL du serveur point de contact	Adresse URL donnant accès aux noeuds finals sur le serveur point de contact.	

Tableau 54. Sélection de profil et informations de configuration pour le fournisseur d'identité dans la fédération SAML 2.0

Sélection de profil	Description	Votre valeur
Options de profil SAML 2.0 : Choisissez l'une des options de profil suivantes :	Profil de votre fédération. Pour plus d'informations sur les profils, voir «SAML 2.0», à la page 149.	Vous pouvez choisir une des options suivantes : • Basique • Typique • Tous • Manuel
Basique : Connexion unique de navigateur Web, déconnexion unique	Ce paramètre active les profils suivants avec toutes les liaisons prises en charge : • Liaison SSO de navigateur Web • Déconnexion unique (SLO)	(aucune valeur supplémentaire requise)
Typique : Connexion unique de navigateur Web, déconnexion unique et Gestion des identificateurs de nom	Ce paramètre active les profils suivants avec toutes les liaisons prises en charge : • Liaison SSO de navigateur Web • Déconnexion unique (SLO) • Client ou proxy évolué • Gestion des identificateurs de nom	(aucune valeur supplémentaire requise)

Tableau 54. Sélection de profil et informations de configuration pour le fournisseur d'identité dans la fédération SAML 2.0 (suite)

Sélection de profil	Description	Votre valeur
Activer tous les profils et toutes les liaisons	Si vous sélectionnez l'option **Activer tous les profils et toutes les liaisons**, vous devez être prêt à fournir les informations suivantes dans les panneaux successifs : **Panneau Reconnaissance du fournisseur d'identité** • Nom de domaine commun • URL du service de cookie de domaine commun • Durée de vie du cookie de domaine commun, en secondes. Valeur par défaut : 1 **Panneau Proxy client amélioré** • En-têtes HTTP	**Panneau Reconnaissance du fournisseur d'identité** • Nom de domaine commun • URL du service de cookie de domaine commun • Durée de vie du cookie de domaine commun, en secondes. Valeur par défaut : 1 **Panneau Proxy client amélioré** • En-têtes HTTP
Manuel : Choisissez des profils et des liaisons individuels	Si vous choisissez l'option **Manuel**, vous devez être prêt à sélectionner des profils individuels et des liaisons prises en charge.	Profils et liaisons :

Tableau 55. Informations de signature pour le fournisseur d'identité dans la fédération SAML 2.0

Signatures	Description	Votre valeur
Demander une signature sur les messages et assertions entrants	Case à cocher indiquant que votre partenaire devra utiliser sa clé privée pour signer le message et l'assertion. Par défaut, la case est cochée.	Vous pouvez choisir une des options suivantes : • Le partenaire signe (la case est cochée). • Le partenaire ne signe pas (la case n'est pas cochée).
Sélectionner les messages et assertions sortants qui nécessitent une signature	Boutons indiquant quels messages sortants doivent être signés par vos soins. Lorsque le paramètre par défaut est sélectionné, l'ensemble des messages et assertions SAML sortants classiques (à l'exception des objets ArtifactResponse et AuthnResponse) doivent être signés.	Vous pouvez choisir une des options suivantes : • Les ensembles de messages SAML sortants classiques sont signés. • Toutes les assertions et tous les messages SAML sortants sont signés. • Aucune assertion ni aucun message SAML sortant ne sont signés.

Tableau 55. Informations de signature pour le fournisseur d'identité dans la fédération SAML 2.0 (suite)

Signatures	Description	Votre valeur
Sélectionner la clé de signature • Fichier de clés du service de clés Tivoli Federated Identity Manager, dans lequel la clé est stockée • Mot de passe du fichier de clés • Clé privée utilisée pour la signature des messages	Si vous devez signer les messages et assertions, vous devez indiquer la clé à utiliser pour les signer. **Remarque :** Avant d'effectuer cette tâche, veillez à créer la clé et à l'importer dans le fichier de clés approprié du service de clés Tivoli Federated Identity Manager.	Nom de fichiers de clés : Mot de passe du fichier de clés : Nom d'alias de clé :

Tableau 56. Informations de chiffrement pour le fournisseur d'identité dans la fédération SAML 2.0

Chiffrement	Description	Votre valeur
Clé de chiffrement: • Fichier de clés du service de clés Tivoli Federated Identity Manager, dans lequel la clé est stockée • Mot de passe du fichier de clés • Biclé publique/privée utilisée pour les données reçues en provenance de votre partenaire.	Biclé publique/privée utilisée pour le chiffrement. Votre partenaire utilisera la clé publique pour chiffrer les données à votre intention. Vous utiliserez la clé privée pour déchiffrer les données qui vous sont envoyées par votre partenaire. Vous devez indiquer la paire de clés utilisée. **Remarque :** Avant d'effectuer cette tâche, veillez à créer la clé et à l'importer dans le fichier de clés approprié du service de clés Tivoli Federated Identity Manager. Pour plus d'informations, voir Chapitre 6, «Configuration de la sécurité des messages», à la page 29.	Nom de fichiers de clés : Mot de passe du fichier de clés : Nom d'alias de clé :

Tableau 57. Paramètres des messages SAML pour le fournisseur d'identité dans la fédération SAML 2.0

Paramètres des messages	Description	Votre valeur
Options des messages : • Durée de vie du message (en secondes) • Durée de vie de l'artefact (en secondes) • Délai d'expiration de session	Intervalle de temps, spécifié en secondes, pendant lequel les messages, artefacts et sessions sont valides. Les valeurs par défaut sont les suivantes : • Durée de vie des messages : 300 • Durée de vue des artefacts : 120 • Délai d'expiration de session : 7200	Durée de vie du message (en secondes) : Durée de vie de l'artefact (en secondes) : Délai d'expiration de session :
Nécessite un accord pour fédérer	Si vous cochez cette case, vous devez présenter une page à l'utilisateur afin de vérifier que celui-ci a émis une requête de fédération. Valeur par défaut : un accord de fédération est requis.	Vous pouvez choisir une des options suivantes : • Nécessite un accord pour fédérer (la case est cochée). • Ne pas demander d'accord pour fédérer (la case n'est pas cochée).
Noeud final SOAP	URL du point d'extrémité SOAP. Valeur par défaut : la valeur contenue dans cette zone dépend de l'URL du serveur point de contact que vous avez fournie précédemment. **Remarque :** Si aucune liaison SOAP n'est utilisée dans le profil que vous avez sélectionné, l'affichage de cette zone n'a pas lieu.	

Tableau 58. Informations relatives aux paramètres de jeton pour le fournisseur d'identité dans la fédération SAML 2.0

Configuration des paramètres de jeton	Description	Votre valeur
Durée de validité (en secondes) d'une assertion avant sa date d'émission	Durée en secondes pendant laquelle une assertion est considérée comme valide avant sa date de création. Valeur par défaut : 60	
Durée de validité de l'assertion après émission	Durée en secondes pendant laquelle une assertion est considérée comme valide après sa date de création. Valeur par défaut : 60	

Tableau 59. Informations de requête d'attribut pour le fournisseur d'identité

Requête d'attribut	Description	Votre valeur
Activé	Indique si le fournisseur est autorisé à agir en tant qu'autorité d'attribut. Si cette option est sélectionnée, le profil de requête d'attribut est activé.	

Tableau 60. Informations de mappage requête d'attribut pour le fournisseur d'identité

Mappage de requête d'attribut	Description	Votre valeur
Options de mappage de requête d'attribut Vous pouvez choisir une des options suivantes : • Fichier de transformation XSL ou JavaScript contenant les règles de mappage • Module de mappage Tivoli Directory Integrator • Module de mappage personnalisé	Type de mappage de requête d'attribut utilisé. Vous devez sélectionner un fichier XSLT, un module de mappage Tivoli Directory Integrator ou un module de mappage personnalisé. Si vous utilisez un fichier XSLT, ce dernier doit avoir été créé avant la configuration de la fédération. Le module de mappage Tivoli Directory Integrator est un module STS. Le mappage personnalisé est une option avancée. Si vous utilisez cette option, vous devez créer et ajouter un nouveau type et instance de module *avant* de pouvoir l'utiliser dans votre configuration.	L'une des valeurs suivantes : • Chemin de fichier XSLT • Module de mappage Tivoli Directory Integrator • Nom de l'instance de module de mappage personnalisée

Tableau 61. Informations de mappage d'identité pour le fournisseur d'identité dans la fédération SAML 2.0

Mappage d'identité	Description	Votre valeur
Options de mappage d'identité Vous pouvez choisir une des options suivantes : • Fichier de transformation XSL contenant les règles de mappage • Module de mappage personnalisé	Type de mappage d'identité utilisé. Vous devez savoir si vous allez utiliser un fichier XSLT pour le mappage d'identité ou un module de mappage personnalisé. Le mappage personnalisé est une option avancée. Si vous souhaitez utiliser cette option, vous devez créer votre module de mappage et l'ajouter à l'environnement en tant que module type et module d'instance *avant* de pouvoir l'utiliser dans votre configuration. Si vous choisissez d'utiliser un fichier XSLT, vous devez préparer le fichier pour la fédération.	L'une des valeurs suivantes : • Fichier XSLT (chemin et nom): • Nom de l'instance de module de mappage personnalisée :

Une fois que vous avez complété les tables, poursuivez avec les instructions de la rubrique «Création de votre rôle dans la fédération».

Création de votre rôle dans la fédération

Utilisez la console pour créer une fédération. Pour commencer, l'assistant Fédération vous invite à renseigner les informations relatives à votre rôle dans la fédération. Pour obtenir la description des zones que l'assistant vous invite à renseigner, consultez l'aide en ligne.

Avant de commencer

Avant de commencer cette procédure, complétez la formulaire standard SAML approprié, en indiquant le rôle que vous tenez dans la fédération :

- «Formulaire de fournisseur de services IDP SAML 1.x», à la page 185
- «Formulaire de fournisseur d'identité SAML 1.x», à la page 187
- «Formulaire de fournisseur de services SAML 2.0», à la page 190
- «Formulaire de fournisseur d'identité SAML 2.0», à la page 196

Pourquoi et quand exécuter cette tâche

Remarque : Pendant la configuration, il se peut que vous soyez invité à redémarrer WebSphere Application Server. Avant de poursuivre la tâche, assurez-vous que le serveur a redémarré entièrement.

Pour créer une fédération, procédez comme suit :

Procédure

1. Connectez-vous à la console, puis cliquez sur **Tivoli Federated Identity Manager → Configurer la connexion unique fédérée → Fédérations**. Le portlet Fédérations affiche plusieurs boutons d'action.
2. Cliquez sur **Créer**. L'assistant de fédération démarre. Le panneau Informations générales s'affiche.
3. A l'aide de votre formulaire, complétez les panneaux affichés par l'assistant Fédération. Utilisez le formulaire complété comme guide pour renseigner les zones affichées. Si vous avez besoin de revenir à un panneau précédent, cliquez sur **Précédent**. Si vous souhaitez mettre fin à la configuration, cliquez sur **Annuler**. Sinon, cliquez sur **Suivant** après avoir complété chaque panneau.
4. Lorsque vous avez complété tous les écrans de configuration, le panneau Récapitulatif s'affiche. Vérifiez que les paramètres de configuration sont corrects, puis cliquez sur **Terminer**. Le portlet Création de fédération terminée s'affiche.
5. Vous pouvez ajouter votre partenaire maintenant ou ultérieurement. Choisissez-en un :
   - Cliquez sur **Ajouter un partenaire** pour lancer l'assistant Partenaire et ajouter la configuration de votre partenaire en suivant les étapes décrites à la section :
     a. «Obtention des données de configuration de fédération de la part de votre partenaire», à la page 207, et complétez le formulaire approprié en fonction du rôle de votre partenaire dans la fédération.
     b. «Ajout à votre partenaire», à la page 234.
   - Pour ajouter votre partenaire ultérieurement, cliquez sur **Terminé**. Vous serez redirigé vers l'écran des fédérations.

Configuration d'un serveur point de contact WebSEAL pour la fédération SAML

Si vous envisagez d'utiliser WebSEAL en tant que serveur point de contact, vous devez le configurer pour la fédération SAML.

Avant de commencer

L'assistant de fédération comporte un bouton qui vous permet d'obtenir un utilitaire de configuration.

Pourquoi et quand exécuter cette tâche

Vous devez obtenir l'utilitaire, puis l'exécuter. Procédez comme suit :

Procédure

1. Cliquez sur **Télécharger l'outil de configuration Tivoli Access Manager**.
2. Enregistrez l'outil de configuration sur le système de fichiers de l'ordinateur hébergeant le serveur WebSEAL.
3. Revenez à la console de gestion et cliquez sur **Terminé** pour revenir au panneau Fédérations.

   Remarque : La console de gestion vous offre la possibilité d'ajouter immédiatement un partenaire, mais pour cette configuration initiale de la fédération, nous commencerons par exécuter d'abord les autres tâches.

4. Démarrez l'outil de configuration depuis une ligne de commande. La syntaxe est la suivante :

   ```
   java -jar /rép_téléchargement/tfimcfg.jar -cfgfile webseald-nom_instance.conf
    -action tamconfig
   ```

   Vous aurez besoin de l'ID (par défaut : sec_master) et du mot de passe de l'utilisateur d'administration Tivoli Access Manager. L'utilitaire configure les noeuds finals sur le serveur WebSEAL, crée une jonction WebSEAL, relie les listes de contrôle d'accès adaptées et active les méthodes d'authentification adéquates.

Exemple

Par exemple, lorsque vous avez mis le fichier tfimcfg.jar dans le répertoire `/tmp` et que le nom de l'instance WebSEAL est `default`, la commande est la suivante :

```
java -jar /tmp/tfimcfg.jar -cfgfile webseald-default -action tamconfig
```

Pour plus d'informations, accédez à l'adresse suivante :

- Annexe A, «Référence de tfimcfg», à la page 533

Configuration de WebSphere en tant que serveur point de contact

Tivoli Federated Identity Manager est configuré par défaut pour utiliser Tivoli Access Manager WebSEAL en tant que serveur point de contact. Pour configurer WebSphere en tant que serveur point de contact, vous devez procéder à une modification de la configuration.

Procédure

1. Connectez-vous à la console d'administration.
2. Cliquez sur Tivoli Federated Identity Manager > Gestion de la configuration > Point de contact
3. Sélectionnez **WebSphere**
4. Cliquez sur **Activer**.

Résultats

Le serveur WebSphere est désormais configuré en tant que point de contact.

Délivrance d'instructions à votre partenaire

Lorsque vous travaillez en collaboration avec des partenaires en vue d'établir une fédération, vous devez leur fournir des informations et en recueillir également de leur part.

Suivant le rôle que vous exercez au sein de vos fédérations, vous pouvez être amené à envisager la délivrance de conseils ou d'une assistance à votre partenaire, en complément des informations de configuration qui leurs sont destinées. L'expérience de votre partenaire peut vous aider à déterminer le meilleur moyen de lui porter assistance. Les partenaires ayant une expérience des connexions uniques sauront probablement besoin d'une aide limitée, par exemple via une assistance téléphonique ou par courriel. En revanche, les partenaires inexpérimentés en matière de connexion unique peuvent avoir besoin d'une réelle orientation, telle qu'un tutoriel ou une description écrite.

Le moment propice pour fournir ces instructions est laissé à votre discrétion. Il peut être souhaitable de les délivrer en même temps que vous sollicitez des informations de la part de votre partenaire. Sinon, vous pouvez choisir de partager des informations de présentation dès les premières étapes de votre relation fédérée, avant que les procédures de configuration ne soient mises en place.

Le plan indiqué ci-après a pour but de vous aider à élaborer une instruction documentée à l'attention de votre partenaire. Ce plan suppose que vous êtes le partenaire responsable de la délivrance des instructions. En revanche, si vous êtes celui qui a besoin d'aide, envisagez de transmettre les instructions à votre partenaire, ou de faire évoluer le plan au profit d'un questionnaire que vous pourrez utiliser pour solliciter des informations de sa part.

Plan du guide d'intégration

1. Introduction

a. Expliquez en quoi consiste une connexion unique, ainsi que l'usage de Tivoli Federated Identity Manager.

b. Définissez les termes tels que fédération, fournisseur d'identité, fournisseur de services ainsi que, le cas échéant, protocole, profil et liaison.

c. Identifiez le rôle que vous souhaitez jouer, ainsi que celui de votre partenaire dans la fédération.

d. Décrivez le mode d'interaction entre les utilisateurs finals de votre site, ainsi que celui de votre partenaire. Par exemple : identifiez le service auquel les utilisateurs finals tentent d'accéder. Evaluez la possibilité d'inclure un graphique qui identifie le flux d'activités établi parmi les participants, tels que l'utilisateur final qui se connecte, le fournisseur d'identité qui authentifie l'utilisateur, le fournisseur de services qui délivre l'accès et l'utilisateur final qui accède au service.

2. Spécifications techniques

a. Définissez les exigences ou options relatives aux protocoles, aux liaisons et aux profils. Vous avez peut-être besoin, par exemple, que votre partenaire utilise le protocole SAML 1.1 avec un artefact de navigateur. Ou bien, vous avez besoin que votre partenaire utilise le protocole 1.1, mais en laissant au partenaire le choix du type de profil.

b. Expliquez les exigences ou options relatives aux assertions. Vous pouvez par exemple souhaiter que le partenaire inclue des zones spécifiques dans l'assertion, telles qu'une clé de mappage de groupe d'utilisateurs avec un identificateur individuel. Vous pouvez également expliquer que la spécification de certaines options d'assertion est nécessaire, par exemple pour la durée de vie de l'assertion ou de l'artefact (en cas d'utilisation de l'artefact de navigateur), ou encore les informations de signature.

c. Présentez les limitations quant aux types de périphériques que vous pouvez utiliser dans le cadre d'une fonction de connexion unique. Il se peut, par exemple, que la fédération prenne uniquement en charge l'interaction des utilisateurs finals avec le navigateur Web.

d. Décrivez les exigences relatives à l'audit et à la consignation. Pour plus d'informations, voir la rubrique *IBM Tivoli Federated Identity Manager - Guide d'audit*.

e. Expliquez de quelle manière les utilisateurs seront amenés à voir s'afficher des messages d'événement lors des interactions avec la fédération. A titre d'exemple, si vous êtes un fournisseur de services, vous pouvez proposer à votre partenaire des options de personnalisation, relatives aux circonstances

dans lesquelles les utilisateurs doivent se déconnecter ou recevoir des messages de dépassement de délai d'attente, ou d'autres événements en provenance du système. Si vous êtes un fournisseur d'identité, vous pouvez proposer à votre partenaire des options de personnalisation relatives à la manière dont les utilisateurs doivent se connecter.

f. Convenez, avec votre partenaire, du mode de synchronisation entre les horloges système.

III. Sécurité

a. Définissez les exigences relatives à SSL.

b. Demandez des informations de certificat (telles que le nom de l'autorité de certification ayant émis le certificat du partenaire, ou une copie du certificat du partenaire).

c. Expliquez les exigences ou options relatives à la signature.

IV. Echange de données

Etablissez le mode d'échange des données dans la fédération, y compris les clés (dans les fédérations SAML 1.x, l'échange de données peut s'effectuer manuellement ou par le biais d'un fichier de métadonnées. Dans SAML 2.0, l'usage d'un fichier de métadonnées est obligatoire). Si une méthode manuelle est utilisée, indiquez la liste des informations demandées à votre partenaire. Pour cela, basez-vous sur les formulaires contenus dans les rubriques «Obtention des données de configuration de fédération de la part de votre partenaire», à la page 207 et «Transmission des propriétés de la fédération au partenaire», à la page 236.

V. Test

Décrivez votre aptitude à effectuer les tests de la fédération et mentionnez les exigences éventuelles auxquelles votre partenaire doit se conformer avant d'utiliser la fédération dans un environnement de production. Evaluez la possibilité d'inclure les URL nécessaires à votre partenaire aux fins de test. A titre d'exemple, si vous êtes le fournisseur de services d'une fédération SAML 1.x, il se peut que vous deviez fournir à votre partenaire une URL cible et une URL d'assertion de client.

VI. Production

Décrivez les conditions à remplir pour que la fédération soit prête pour la production. Vous pouvez inclure des URL de production ou expliquer comment vous les produirez ultérieurement.

VII. Support

Expliquez la manière dont la prise en charge au niveau utilisateur ou au niveau administrateur sera gérée dans la fédération.

VIII. Formulaire de partenaire

Il se peut qu'à différents stades au cours des sections précédentes, vous ayez demandé des informations à votre partenaire, ou que vous lui ayez expliqué les raisons de cette demande d'informations. A la fin de votre document, envisagez d'ajouter un formulaire sur lequel votre partenaire aura la possibilité d'inscrire les informations demandées. Ce formulaire peut par exemple contenir les zones suivantes :

- Adresses URL de noeuds finals aux fins de test

- Adresses URL de noeuds finals pour la production
- Personne à contacter
- Informations relatives aux certificats SSL (nom de l'autorité de certification, etc.)
- Informations de signature (nature des informations signées ou validées, etc.)
- Méthode d'échange de données (manuelle ou métadonnées). Si une méthode manuelle est utilisée, il se peut que vous deviez ajouter votre formulaire d'autres zones relatives aux informations demandées.

Obtention des données de configuration de fédération de la part de votre partenaire

Vous devez obtenir des informations de configuration de la part de votre partenaire avant d'ajouter ce partenaire à une fédération.

Le partenaire peut exporter la configuration de la fédération dans un fichier de métadonnées ou, si ce partenaire utilise SAML 1.x, il peut vous la communiquer manuellement (la configuration manuelle par les partenaires n'est pas prise en charge dans les fédérations SAML 2.0).

Pour rassembler plus facilement les informations appropriées en provenance de votre partenaire, complétez la formulaire relatif à la norme SAML que vous utiliserez dans la fédération, ainsi que pour le rôle attribué à votre partenaire dans cette fédération :

- *Si vous êtes le fournisseur d'identité*, ajoutez un partenaire fournisseur de services. Utilisez le formulaire destiné au partenaire fournisseur de services en fonction de la norme SAML que vous utilisez dans votre fédération :
  - «Formulaire pour fournisseur de services partenaire SAML 1.x»
  - «Formulaire de fournisseur de services partenaire SAML 2.0», à la page 220
- *Si vous êtes le fournisseur de services*, ajoutez un partenaire fournisseur d'identité. Utilisez le formulaire destiné au partenaire fournisseur d'identité en fonction de la norme SAML que vous utilisez dans votre fédération :
  - «Formulaire pour fournisseur d'identité partenaire SAML 1.x», à la page 213
  - «Formulaire de fournisseur d'identité partenaire SAML 2.0», à la page 226

Lorsque vous avez rassemblé les informations de configuration du partenaire, vous pouvez utiliser l'assistant de partenaire, dans la console d'administration, pour ajouter les propriétés de sa fédération. Voir «Ajout à votre partenaire», à la page 234.

Formulaire pour fournisseur de services partenaire SAML 1.x

Si vous êtes un fournisseur d'identité SAML 1.x, vous devez ajouter un fournisseur de services partenaire dans votre fédération. Certaines informations peuvent vous êtres fournies sous la forme d'un fichier de métadonnées, ou toutes les informations peuvent vous être fournies manuellement.

Utilisez le formulaire suivant pour rassembler les informations nécessaires en provenance de votre partenaire. Il peut être souhaitable de modifier ce formulaire afin qu'il reflète les informations spécifiques que vous avez besoin d'obtenir de la part de vous partenaire, et de demander à ce dernier de compléter le formulaire modifié.

Tableau 62. Options relatives aux métadonnées pour l'ajout d'un fournisseur de services partenaire dans une fédération SAML 1.x

Options de métadonnées	Description	Vos valeurs
Spécifiez manuellement les paramètres SAML **Importez le fichier de métadonnées**	Indique la méthode employée pour saisir les données relatives au partenaire. Vous pouvez soit recevoir un fichier de métadonnées de la part de votre partenaire, soit saisir manuellement les informations qui le concernent. Si vous optez pour l'importation d'un fichier de métadonnées, vous devez connaître son nom et son emplacement.	choisissez l'une des options suivantes : • Spécifiez manuellement les paramètres SAML • Importez le fichier de métadonnées et spécifiez le nom et le chemin d'accès du fichier :

Tableau 63. Informations de contact pour le fournisseur de services partenaire dans la fédération SAML 1.x

Personne à contacter	Description	Votre valeur
Remarque : Ce panneau s'affiche uniquement en cas de saisie manuelle des informations relatives au partenaire.		
Nom de l'entreprise du fournisseur d'identité, adresse URL et personne à contacter.	Nom de l'entreprise et, le cas échéant, autres informations relatives au contact associé à la fédération.	Nom de l'entreprise :

Tableau 64. Paramètres des messages SAML pour le fournisseur de services partenaire dans une fédération SAML 1.x

Paramètres des messages SAML	Description	Votre valeur
Remarque : Ce panneau s'affiche uniquement en cas de saisie manuelle des informations relatives au partenaire.		
ID fournisseur	Adresse URL du serveur point de contact du fournisseur de services, également utilisée en tant qu'ID de fournisseur.	ID fournisseur :
URL du service d'assertion client	Adresse URL du noeud final du service d'assertion client sur le site du fournisseur de services.	URL du service d'assertion client :
Le partenaire utilise le profil POST du navigateur pour la connexion unique	Case à cocher indiquant que le fournisseur de services partenaire utilise le POST du navigateur.	Vous pouvez choisir une des options suivantes : • Le partenaire utilise le profil POST du navigateur (cochez la case). • Le partenaire n'utilise pas le profil POST du navigateur (ne pas cocher la case).

Tableau 65. Informations relatives à la validation de signature pour le fournisseur de services partenaire dans une fédération SAML 1.x

Signatures	Description	Votre valeur
Valider les signatures sur les requêtes d'artefact	Il est possible de valider les signatures de message SAML lorsque l'artefact du navigateur est utilisé. Pour utiliser cette option, cochez la case Validation de signatures.	Vous pouvez choisir une des options suivantes : • Valider les signatures pour l'artefact (cochez la case). • Ne pas valider les signatures pour l'artefact (ne pas cocher la case).
Sélectionner le fichier de clés certifiées ou la clé de validation • Fichier de clés certifiées de Tivoli Federated Identity Manager, dans lequel la clé est stockée • Mot de passe du fichier de clés certifiées • Clé publique utilisée pour effectuer la validation	Si vous choisissez de valider les messages lorsque l'artefact du navigateur est utilisé, vous devez indiquer une clé pour cette validation. Il doit s'agir de la clé publique correspondant à la clé privée que votre partenaire utilise pour signer les messages. **Remarque :** Si vous effectuez l'importation des données de votre partenaire, la clé est fournie dans le fichier de métadonnées. Vous serez invité à sélectionner un fichier de clés. Avant d'effectuer cette tâche, assurez-vous que le fichier de clés a été créé. Si vous procédez à la saisie manuelle des données de votre partenaire, assurez-vous de vous être procuré la clé et de l'avoir importée dans le fichier de clés approprié du service de clés de Tivoli Federated Identity Manager, avant de d'effectuer cette tâche. Pour plus d'informations, voir Chapitre 6, «Configuration de la sécurité des messages», à la page 29.	**Méthode utilisant les métadonnées :** • Nom du fichier de clés certifiées : • Mot de passe du fichier de clés certifiées : • Libellé de la clé : **Méthode manuelle :** • Nom du fichier de clés certifiées : • Mot de passe du fichier de clés certifiées : • nom d'alias de clé :

Tableau 66. Informations relatives aux paramètres jetons de sécurité pour le fournisseur de services partenaire dans une fédération SAML 1.x

Configuration du jeton de sécurité	Description	Votre valeur
Signer les assertions SAML	Vous avez la possibilité de signer les assertions SAML.	Vous pouvez choisir une des options suivantes : • Activer les signatures SAML (cochez la case). • Ne pas activer les signatures (ne pas cocher la case).
Sélectionner la clé de signature • Fichier de clés du service de clés Tivoli Federated Identity Manager, dans lequel la clé est stockée • Mot de passe du fichier de clés • Clé privée utilisée pour la signature de l'assertion.	Si vous choisissez de signer les assertions, vous devez sélectionner un fichier de clés et une clé. **Remarque :** avant d'effectuer cette tâche, créez le fichier de clés, ainsi que la clé. Pour plus d'informations, voir Chapitre 6, «Configuration de la sécurité des messages», à la page 29.	• Nom de fichiers de clés : • Mot de passe du fichier de clés : • nom d'alias de clé :
Inclure les données de certificat X509	Si vous optez pour la signature de l'assertion SAML, indiquez si vous souhaitez que les données de certificat codées en base 64 soient incluses dans votre signature. L'action par défaut consiste à inclure les données de certificat X.509 (**Oui**). Vous pouvez également choisir d'exclure les données de certificat X.509 (**Non**).	
Inclure les détails de l'émetteur de sujet X509	Si vous optez pour la signature de l'assertion SAML, indiquez si vous souhaitez que le nom de l'émetteur et le numéro de série du certificat soient inclus dans votre signature. L'action par défaut consiste à exclure (**Non**) les détails relatifs à l'émetteur de sujet X.509. Vous pouvez également choisir d'inclure les détails relatifs à l'émetteur de sujet X.509 (**Oui**).	

Tableau 66. Informations relatives aux paramètres jetons de sécurité pour le fournisseur de services partenaire dans une fédération SAML 1.x (suite)

Configuration du jeton de sécurité	Description	Votre valeur
Inclure le nom de sujet X509	Si vous optez pour la signature de l'assertion SAML, indiquez si vous souhaitez que le nom de sujet soit inclus dans votre signature. L'action par défaut consiste à exclure le nom de sujet X.509 (**Non**). Vous pouvez également choisir d'inclure le nom de sujet X.509 (**Oui**).	
Inclure l'identificateur de clé de sujet X509	Si vous optez pour la signature de l'assertion SAML, indiquez si vous souhaitez que l'identificateur de clé de sujet soit inclus dans votre signature. L'action par défaut consiste à exclure l'identificateur de clé de sujet (**Non**). Vous pouvez également choisir d'inclure l'identificateur de clé de sujet X.509 (**Oui**).	
Inclure la clé publique	Si vous optez pour la signature de l'assertion SAML, indiquez si vous souhaitez que la clé publique soit incluse dans votre signature. L'action par défaut consiste à exclure la clé publique (**Non**). Vous pouvez également choisir d'inclure la clé publique (**Oui**).	
Inclure l'élément InclusiveNamespaces	Si vous optez pour la signature de l'assertion SAML, vous pouvez sélectionner cette option afin d'inclure l'élément InclusiveNamespaces à la canonicalisation de l'assertion lors de la création de la signature. Par défaut, cette option est désélectionnée.	

Tableau 66. Informations relatives aux paramètres jetons de sécurité pour le fournisseur de services partenaire dans une fédération SAML 1.x (suite)

Configuration du jeton de sécurité	Description	Votre valeur
Inclure les types d'attributs suivants	Cochez la case pour indiquer les types d'attributs à inclure dans l'assertion. L'astérisque (*), qui est le paramètre par défaut, indique que tous les types d'attributs spécifiés dans le fichier de mappage personnalisé ou par le module de mappage personnalisé seront inclus dans l'assertion. Pour spécifier un ou plusieurs types d'attributs individuellement, tapez chaque type d'attribut dans la case. Par exemple, si vous souhaitez inclure uniquement des attributs de type `urn:oasis:names:tc:SAML:2.0:assertion` entrez cette valeur dans la zone. Utilisez && pour séparer plusieurs types d'attributs.	

Tableau 67. Informations de mappage d'identité pour le fournisseur de services partenaire dans la fédération SAML 1.x

Mappage d'identité	Description	Votre valeur
Options de mappage d'identité Vous pouvez choisir une des options suivantes : • Module de mappage personnalisé • Fichier de transformation XSL contenant les règles de mappage • Ne sélectionnez aucune option si vous souhaitez appliquer l'option de mappage d'identité actuellement définie pour la fédération.	Type de mappage d'identité utilisé avec ce partenaire. Vous pouvez ne sélectionner aucune de ces options si vous souhaitez que ce partenaire choisisse l'option de mappage d'identité déjà configurée pour la fédération. Sinon, vous pouvez choisir une option de mappage spécifique et l'appliquer à ce partenaire. Pour choisir une option de mappage, vous devez savoir si vous allez utiliser un fichier XSLT pour le mappage d'identité ou un module de mappage personnalisé. Le mappage personnalisé est une option avancée. Si vous souhaitez utiliser cette option, vous devez créer votre module de mappage et l'ajouter à l'environnement en tant que module type et module d'instance *avant* de pouvoir l'utiliser dans votre configuration. Si vous choisissez d'utiliser un fichier XSLT, vous devez préparer le fichier pour la fédération.	Ne sélectionnez aucune option pour utiliser la configuration de mappage existante. Sinon, utilisez l'une des valeurs suivantes : • Fichier XSLT (chemin et nom): • Nom de l'instance de module de mappage personnalisée :

Une fois que vous avez complété ce formulaire, poursuivez avec les étapes de la rubrique «Ajout à votre partenaire», à la page 234.

Formulaire pour fournisseur d'identité partenaire SAML 1.x

Si vous êtes un fournisseur de services SAML 1.x, vous devez ajouter un fournisseur d'identité partenaire dans votre fédération. Certaines informations peuvent vous êtres fournies sous la forme d'un fichier de métadonnées, ou toutes les informations peuvent vous être fournies manuellement.

Utilisez le formulaire suivant pour rassembler les informations nécessaires en provenance de votre partenaire. Il peut être souhaitable de modifier ce formulaire afin qu'il reflète les informations spécifiques que vous avez besoin d'obtenir de la part de vous partenaire, et de demander à ce dernier de compléter le formulaire modifié.

Tableau 68. Options relatives aux métadonnées pour l'ajout d'un fournisseur d'identité partenaire dans une fédération SAML 1.x

Options de métadonnées	Description	Vos valeurs
Spécifiez manuellement les paramètres SAML **Importez le fichier de métadonnées**	Indique la méthode employée pour saisir les données relatives au partenaire. Vous pouvez soit recevoir un fichier de métadonnées de la part de votre partenaire, soit saisir manuellement les informations qui le concernent. Si vous optez pour l'importation d'un fichier de métadonnées, vous devez connaître son nom et son emplacement.	choisissez l'une des options suivantes : • Spécifiez manuellement les paramètres SAML • Importez le fichier de métadonnées et spécifiez le nom et le chemin d'accès du fichier :

Tableau 69. Informations de contact pour le fournisseur d'identité partenaire dans une fédération SAML 1.x

Personne à contacter	Description	Votre valeur
Remarque : Ce panneau s'affiche uniquement en cas de saisie manuelle des informations relatives au partenaire.		
Nom de l'entreprise, adresse URL et personne à contacter	Nom de l'entreprise et, le cas échéant, autres informations relatives au contact associé à la fédération.	Nom de l'entreprise :

Tableau 70. Paramètres des messages SAML pour le fournisseur d'identité partenaire dans une fédération SAML 1.x

Paramètres des messages SAML	Description	Votre valeur
Remarque : Ce panneau s'affiche uniquement en cas de saisie manuelle des informations relatives au partenaire.		
ID fournisseur	Adresse URL du serveur point de contact du fournisseur de services, également utilisée en tant qu'ID de fournisseur.	ID fournisseur :
ID source • Générer l'ID source automatiquement • Indiquez une valeur explicite pour l'ID source	Vous avez la possibilité de générer un ID source pour le partenaire, ou d'en indiquer un.	ID source :
Noeuds finals • URL du service de transfert inter-sites • URL du service de résolution des artefacts	Adresses URL renvoyant aux noeuds finals du service de transfert inter-sites et du service de résolution d'artefacts.	URL du service de transfert inter-sites : URL du service de résolution des artefacts :

Tableau 71. Informations relatives à la validation de signature pour le fournisseur d'identité partenaire dans une fédération SAML 1.x

Validation des signatures	Description	Votre valeur
Les messages SAML pour le profil POST du navigateur sont signés et doivent être validés (obligatoire) **Valider les signatures sur les messages SAML pour le profil d'artefact** (facultatif)	• Lorsque le POST du navigateur est utilisé en tant que profil, les messages SAML doivent être signés et validés. Cette option est donc présélectionnée et ne peut pas être désélectionnée. • Il est également possible de valider les signatures de message SAML lorsque l'artefact du navigateur est utilisé.	Vous pouvez choisir une des options suivantes : • Valider les signatures pour l'artefact (cochez la case). • Ne pas valider les signatures pour l'artefact (ne pas cocher la case).

Tableau 71. Informations relatives à la validation de signature pour le fournisseur d'identité partenaire dans une fédération SAML 1.x (suite)

Validation des signatures	Description	Votre valeur
Sélectionner le fichier de clés certifiées ou la clé de validation • Fichier de clés certifiées de Tivoli Federated Identity Manager, dans lequel la clé est stockée • Mot de passe du fichier de clés certifiées • Clé publique utilisée pour valider la signature de votre partenaire	Etant donné que les messages POST du navigateur doivent être signés et validés, vous êtes tenu de spécifier une clé permettant de valider la signature. Si vous choisissez de valider également les messages lorsque l'artefact du navigateur est utilisé, cette validation s'effectue au moyen de la même clé. La clé publique que vous utilisez correspond à la clé privée que votre partenaire utilise pour signer les messages. **Remarque :** Si vous effectuez l'importation des données de votre partenaire, la clé est fournie dans le fichier de métadonnées. Vous serez invité à sélectionner un fichier de clés. Avant d'effectuer cette tâche, assurez-vous que le fichier de clés a été créé. Si vous procédez à la saisie manuelle des données de votre partenaire, assurez-vous de vous être procuré la clé auprès de votre partenaire et d'avoir importé celle-ci dans le fichier de clés approprié du service de clés de Tivoli Federated Identity Manager, avant de d'effectuer cette tâche. Pour plus d'informations, voir Chapitre 6, «Configuration de la sécurité des messages», à la page 29.	**Méthode utilisant les métadonnées :** • Nom du fichier de clés certifiées : • Mot de passe du fichier de clés certifiées : • Libellé de la clé : **Méthode manuelle :** • Nom du fichier de clés certifiées : • Mot de passe du fichier de clés certifiées : • nom d'alias de clé :

Tableau 72. Validation de certificat serveur pour votre fournisseur d'identité partenaire dans une fédération SAML 1.x

Validation de certificat serveur pour SOAP	Description	Votre valeur
Sélectionner le certificat de validation du serveur	Clé publique du certificat affichée durant les communications SSL avec votre partenaire. Il convient que vous ayez discuté, avec votre partenaire, du certificat à utiliser. Vous devez avoir déjà obtenu le certificat, ainsi que le fichier de clés de celui-ci. Voir «Réception certificat serveur de votre partenaire», à la page 61.	Nom du fichier de clés certifiées : Mot de passe du fichier de clés certifiées : Nom du certificat :

Tableau 73. Authentification du client SOAP pour votre fournisseur d'identité partenaire dans une fédération SAML 1.x

Authentification client pour SOAP	Description	Votre valeur
Informations d'authentification client L'une des options suivantes : • **Authentification de base** – Username – Mot de passe • **Authentification par certificat client** – Certificat à présenter au serveur du fournisseur d'identité. Il s'agit du certificat que vous allez présenter, comme convenu d'un commun accord entre vous et votre fournisseur d'identité partenaire. – Fichier de clés du service de clés Tivoli Federated Identity Manager, dans lequel la clé est stockée – Mot de passe du fichier de clés	Si l'authentification réciproque est exigée par votre partenaire, vous devez en connaître le type. S'il s'agit de l'authentification de base, vous avez besoin d'un nom d'utilisateur et d'un mot de passe. S'il s'agit de l'authentification par certificat client, vous avez besoin du certificat que vous et votre partenaire avez accepté d'utiliser. **Remarque :** Si vous avez besoin d'un certificat, assurez-vous, avant d'effectuer cette tâche, que vous avez convenu avec votre partenaire de sa provenance et que vous l'avez obtenu et importé vers le fichier de clés approprié du service de clés Tivoli Federated Identity Manager. Voir «Obtention de votre certificat client», à la page 62.	Vous pouvez choisir une des options suivantes : • Informations d'authentification de base : – Nom d'utilisateur : – Mot de passe : • Informations relatives à l'authentification par certificat client – Nom de fichiers de clés : – Mot de passe du fichier de clés : – Alias de clé :

Tableau 74. Informations relatives aux paramètres jetons de sécurité pour le fournisseur d'identité partenaire dans une fédération SAML 1.x

Configuration du jeton de sécurité	Description	Votre valeur
Activer la validation des signatures	Si votre partenaire signe les assertions, vous pouvez choisir de valider ces signatures. Dans certains cas, la validation des signatures par vos soins sera exigée par votre partenaire.	Vous pouvez choisir une des options suivantes : • Activer les signatures de validation (cochez la case). • Ne pas valider les signatures (ne pas cocher la case).
Sélectionner la clé de validation	Spécifiez le type de validation de signature à utiliser.	Vous pouvez choisir une des options suivantes : • Utilisez le KeyInfo de la signature XML afin de trouver un certificat X.509 pour la validation des signatures. • Utiliser l'alias du fichier de clés pour trouver une clé publique pour la validation des signatures (action par défaut). • Spécifier l'expression DN du sujet pour les certificats X.509 autorisés.
Sélectionner la clé et le fichier de clés certifiées • Fichier de clés certifiées de Tivoli Federated Identity Manager, dans lequel la clé est stockée • Mot de passe du fichier de clés certifiées • Clé que vous utiliserez pour valider la signature	Si vous choisissez de valider les signatures des assertions, ou que cette validation est exigée par votre partenaire, vous devez sélectionner un fichier de clés et une clé. **Remarque :** La clé publique que vous devez utiliser correspond à la clé privée que votre partenaire utilise pour signer les assertions. Avant d'effectuer cette tâche, assurez-vous que vous avez obtenu cette clé et créé le fichier de clés. Chapitre 6, «Configuration de la sécurité des messages», à la page 29.	• Nom du fichier de clés certifiées : • Mot de passe du fichier de clés certifiées : • nom d'alias de clé :

Tableau 74. Informations relatives aux paramètres jetons de sécurité pour le fournisseur d'identité partenaire dans une fédération SAML 1.x (suite)

Configuration du jeton de sécurité	Description	Votre valeur
Créer plusieurs instructions d'attribut dans Universal User.	Sélectionnez cette option pour conserver plusieurs instructions d'attribut dans les groupes dans lesquels elles ont été reçues. Cette option peut se révéler nécessaire si vos règles de mappage d'identité personnalisées sont écrites de manière à s'appliquer à un ou plusieurs groupes d'instructions d'attribut spécifiques. Si cette case n'est pas activée, plusieurs instructions d'attribut sont organisées dans un seul groupe (AttributeList) dans le document STSUniversalUser. Par défaut, cette option est désélectionnée, ce qui convient à la plupart des configurations.	

Tableau 75. Informations de mappage d'identité pour le fournisseur d'identité partenaire dans la fédération SAML 1.x

Mappage d'identité	Description	Votre valeur
Options de mappage d'identité Vous pouvez choisir une des options suivantes : • Module de mappage personnalisé • Fichier de transformation XSL contenant les règles de mappage • Ne sélectionnez aucune option si vous souhaitez appliquer l'option de mappage d'identité actuellement définie.	Type de mappage d'identité utilisé avec ce partenaire. Vous pouvez ne sélectionner aucune de ces options si vous souhaitez que ce partenaire choisisse l'option de mappage d'identité déjà configurée pour la fédération. Sinon, vous pouvez choisir une option de mappage spécifique et l'appliquer à ce partenaire. Pour choisir une option de mappage, vous devez savoir si vous allez utiliser un fichier XSLT pour le mappage d'identité ou un module de mappage personnalisé. Le mappage personnalisé est une option avancée. Si vous souhaitez utiliser cette option, vous devez créer votre module de mappage et l'ajouter à l'environnement en tant que module type et module d'instance *avant* de pouvoir l'utiliser dans votre configuration. Si vous choisissez d'utiliser un fichier XSLT, vous devez préparer le fichier pour la fédération.	Ne sélectionnez aucune option pour utiliser la configuration de mappage existante. Sinon, sélectionnez l'une des valeurs suivantes : • Fichier XSLT (chemin et nom): • Nom de l'instance de module de mappage personnalisée :

Une fois que vous avez complété ce formulaire, poursuivez avec les étapes de la rubrique «Ajout à votre partenaire», à la page 234.

Formulaire de fournisseur de services partenaire SAML 2.0

Si vous êtes un fournisseur d'identité SAML 2.0, vous devez ajouter un fournisseur de services partenaire dans votre fédération.

Utilisez le formulaire suivant pour rassembler les informations nécessaires en provenance de votre partenaire. Il peut être souhaitable de modifier ce formulaire afin qu'il reflète les informations spécifiques que vous avez besoin d'obtenir de la part de vous partenaire, et de demander à ce dernier de compléter le formulaire modifié.

Tableau 76. Fédération à laquelle vous ajoutez un fournisseur de services partenaire dans une fédération SAML 2.0

Sélection de fédération	Description	Votre valeur
Nom de la fédération	Nom de la fédération à laquelle vous ajoutez le partenaire.	

Tableau 77. Fichier de métadonnées délivré par votre fournisseur de services partenaire dans une fédération SAML 2.0

Importer les métadonnées	Description	Votre valeur
Fichier de métadonnées	Nom et chemin d'accès du fichier obtenu auprès de votre partenaire et qui contient les informations de configuration de votre partenaire.	

Tableau 78. Validation de signature de votre fournisseur de services partenaire dans une fédération SAML 2.0

Validation des signatures	Description	Votre valeur
Sélectionner les assertions et les messages SAML entrants qui nécessitent une signature	Boutons indiquant quels messages entrants doivent être signés par votre partenaire. Lorsque le paramètre par défaut est sélectionné, l'ensemble des messages et assertions SAML entrants classiques (à l'exception des objets ArtifactResponse et AuthnResponse) doivent être signés.	Vous pouvez choisir une des options suivantes : • Les ensembles d'assertions et de messages SAML entrants classiques sont signés. • Toutes les assertions et tous les messages SAML entrants sont signés. • Aucune assertion ni aucun message SAML entrant ne sont signés.
Fichier de clés	Si votre partenaire doit signer les messages et les assertions, il s'agit du fichier de clés certifiées dans lequel vous stockerez la clé fournie par votre partenaire pour valider sa signature dans les messages. Le fichier de clés doit avoir été déjà créé pour cette clé. «Préparation des fichiers de clés», à la page 29.	Nom du fichier de clés certifiées : Mot de passe du fichier de clés certifiées : Libellé de la clé :

Tableau 79. Fichier de clés destiné au stockage de la clé de chiffrement délivrée par votre fournisseur de services partenaire dans une fédération SAML 2.0

Chiffrement	Description	Votre valeur
Fichier de clés	Fichier de clés certifiées dans lequel vous allez stocker la clé destinée au chiffrement des messages adressés à votre partenaire. Cette option s'affiche, car votre partenaire a inclus une clé publique dans les métadonnées que vous utiliserez pour effectuer le chiffrement. Le fichier de clés doit avoir été déjà créé pour cette clé. «Préparation des fichiers de clés», à la page 29.	Nom du fichier de clés certifiées : Mot de passe du fichier de clés certifiées : Libellé de la clé :

Tableau 80. Validation du certificat serveur pour votre fournisseur de services partenaire dans une fédération SAML 2.0

Authentification SSL serveur pour la résolution d'artefact	Description	Votre valeur
Sélectionner le certificat de validation du serveur	Clé publique du certificat affichée durant les communications SSL avec votre partenaire. Il convient que vous ayez discuté, avec votre partenaire, du certificat à utiliser. Vous devez avoir déjà obtenu le certificat et l'avoir ajouté dans le fichier de clés certifiées. Voir «Réception certificat serveur de votre partenaire», à la page 61.	Nom du fichier de clés certifiées : Mot de passe du fichier de clés certifiées : Nom du certificat :

Tableau 81. Authentification client pour votre fournisseur de services partenaire dans une fédération SAML 2.0

Authentification SSL client pour la résolution d'artefact	Description	Votre valeur
Informations d'authentification client L'une des options suivantes : • **Authentification de base** – Username – Mot de passe • **Authentification par certificat client** – Certificat à présenter au serveur du fournisseur d'identité. Il s'agit du certificat que vous allez présenter, comme convenu d'un commun accord entre vous et votre fournisseur d'identité partenaire. – Fichier de clés du service de clés Tivoli Federated Identity Manager, dans lequel la clé est stockée – Mot de passe du fichier de clés	Si l'authentification réciproque est exigée par votre partenaire, vous devez en connaître le type. S'il s'agit de l'authentification de base, vous avez besoin d'un nom d'utilisateur et d'un mot de passe. S'il s'agit de l'authentification par certificat client, vous avez besoin du certificat que vous et votre partenaire avez accepté d'utiliser. **Remarque :** Si vous avez besoin d'un certificat, assurez-vous, avant d'effectuer cette tâche, que vous avez convenu avec votre partenaire de sa provenance et que vous l'avez obtenu et importé vers le fichier de clés approprié du service de clés Tivoli Federated Identity Manager. Voir «Obtention de votre certificat client», à la page 62.	Vous pouvez choisir une des options suivantes : • Informations d'authentification de base : – Nom d'utilisateur : – Mot de passe : • Informations relatives à l'authentification par certificat client – Nom de fichiers de clés : – Mot de passe du fichier de clés : – Alias de clé :

Tableau 82. Paramètres de votre fournisseur de services partenaire dans une fédération SAML 2.0

Paramètres des partenaires	Description	Votre valeur
Délai d'expiration de session (secondes)	Durée en secondes pendant laquelle une session reste valide, jusqu'à ce qu'il n'y ait plus aucune activité. Valeur par défaut : 3600 secondes.	Délai d'expiration de session :
Durée de vie de la requête de fermeture de session (secondes)	Spécifie la durée maximum, en secondes, pendant laquelle la requête de déconnexion reste valide. La valeur par défaut est 120 secondes.	Délai de déconnexion :

Tableau 83. Paramètres d'assertion SAML pour votre fournisseur de services partenaire dans une fédération SAML 2.0

Paramètres d'assertion SAML	Description	Votre valeur
Inclure les types d'attributs suivants	Cochez la case pour indiquer les types d'attributs à inclure dans l'assertion. L'astérisque (*), qui est le paramètre par défaut, indique que tous les types d'attributs spécifiés dans le fichier de mappage personnalisé ou par le module de mappage personnalisé seront inclus dans l'assertion. Pour spécifier un ou plusieurs types d'attributs individuellement, tapez chaque type d'attribut dans la case. Par exemple, si vous souhaitez inclure uniquement des attributs conformes au type suivant, entrez cette valeur dans la case : `urn:oasis:names:tc:SAML:2.0:assertion` Utilisez && pour séparer plusieurs types d'attributs.	
Options de chiffrement : • Chiffrer les identificateurs de nom • Chiffrer les assertions • Chiffrer tous les attributs de vérification	Cochez les cases qui spécifient les parties de l'assertion à chiffrer. Si vous n'effectuez aucune sélection et laissez les cases vides, aucune portion des assertions ne sera chiffrée dans vos messages.	Laissez les cases vides ou sélectionnez l'une ou plusieurs des options suivantes : • Chiffrer les identificateurs de nom • Chiffrer les assertions • Chiffrer tous les attributs de vérification
Algorithme de chiffrement : • AES-128 • AES-256 • AES-192 • Triple DES	Type d'algorithme de chiffrement appliqué aux données de chiffrement destinées à votre partenaire. Si vous ne sélectionnez aucun algorithme, la norme DES triple est appliquée.	Sélectionnez l'une des options suivantes si vous avez choisi une option de chiffrement : • AES-128 • AES-256 • AES-192 • Triple DES

Tableau 84. Informations de mappage requête d'attribut pour votre partenaire de fournisseur de service

Mappage de requête d'attribut	Description	Votre valeur
Options de mappage de requête d'attribut Vous pouvez choisir une des options suivantes : • Fichier de transformation XSL ou JavaScript contenant les règles de mappage • Module de mappage Tivoli Directory Integrator • Module de mappage personnalisé	Type de mappage de requête d'attribut utilisé. Vous devez sélectionner un fichier XSLT, un module de mappage Tivoli Directory Integrator ou un module de mappage personnalisé. Si vous utilisez un fichier XSLT, vous créez ce dernier avant de configurer la fédération. Le module de mappage Tivoli Directory Integrator est un module STS. Le mappage personnalisé est une option avancée. Si vous utilisez cette option, vous devez créer et ajouter un nouveau type et instance de module *avant* de pouvoir l'utiliser dans votre configuration.	L'une des valeurs suivantes : • Chemin de fichier XSLT • Module de mappage Tivoli Directory Integrator • Nom de l'instance de module de mappage personnalisée

Tableau 85. Options de mappage d'identité pour votre fournisseur de services partenaire dans une fédération SAML 2.0

Options de mappage d'identité	Description	Votre valeur
Options de mappage d'identité Vous pouvez choisir une des options suivantes : • Fichier de transformation XSL contenant les règles de mappage • Module de mappage personnalisé • Ne sélectionnez aucune option si vous souhaitez appliquer l'option de mappage d'identité actuellement définie.	Type de mappage d'identité utilisé avec ce partenaire. Vous pouvez ne sélectionner aucune de ces options si vous souhaitez que ce partenaire choisisse l'option de mappage d'identité déjà configurée pour la fédération. Sinon, vous pouvez choisir une option de mappage spécifique et l'appliquer à ce partenaire. Pour choisir une option de mappage, vous devez savoir si vous allez utiliser un fichier XSLT pour le mappage d'identité ou un module de mappage personnalisé. Le mappage personnalisé est une option avancée. Si vous souhaitez utiliser cette option, vous devez créer votre module de mappage et l'ajouter à l'environnement en tant que module type et module d'instance *avant* de pouvoir l'utiliser dans votre configuration. Si vous choisissez d'utiliser un fichier XSLT, vous devez préparer le fichier pour la fédération.	Ne sélectionnez aucune option pour utiliser la configuration de mappage existante. L'une des valeurs suivantes : • Fichier XSLT (chemin et nom): • Nom de l'instance de module de mappage personnalisée :

Une fois que vous avez complété ce formulaire, poursuivez avec les étapes de la rubrique «Ajout à votre partenaire», à la page 234.

Formulaire de fournisseur d'identité partenaire SAML 2.0

Si vous êtes un fournisseur de services SAML 2.0, vous devez ajouter un fournisseur d'identité partenaire dans votre fédération.

Utilisez le formulaire suivant pour rassembler les informations nécessaires en provenance de votre partenaire. Il peut être souhaitable de modifier ce formulaire afin qu'il reflète les informations spécifiques que vous avez besoin d'obtenir de la part de vous partenaire, et de demander à ce dernier de compléter le formulaire modifié.

Tableau 86. Fédération à laquelle vous ajoutez un fournisseur d'identité partenaire dans une fédération SAML 2.0

Sélection de fédération	Description	Votre valeur
Nom de la fédération	Nom de la fédération à laquelle vous ajoutez le partenaire.	

Tableau 87. Fichier de métadonnées délivré par votre fournisseur d'identité partenaire dans une fédération SAML 2.0

Importer les métadonnées	Description	Votre valeur
Fichier de métadonnées	Nom et chemin d'accès du fichier obtenu auprès de votre partenaire et qui contient les informations de configuration de votre partenaire.	

Tableau 88. Validation de signature de votre fournisseur d'identité partenaire dans une fédération SAML 2.0

Validation des signatures	Description	Votre valeur
Sélectionner les assertions et les messages SAML entrants qui nécessitent une signature	Boutons indiquant quels messages entrants doivent être signés par votre partenaire. Lorsque le paramètre par défaut est sélectionné, l'ensemble des messages et assertions SAML entrants classiques (à l'exception des objets ArtifactResponse et AuthnResponse) doivent être signés.	Vous pouvez choisir une des options suivantes : • Les ensembles d'assertions et de messages SAML entrants classiques sont signés. • Toutes les assertions et tous les messages SAML entrants sont signés. • Aucune assertion ni aucun message SAML entrant ne sont signés.
Fichier de clés	Si votre partenaire doit signer les messages et les assertions, il s'agit du fichier de clés certifiées dans lequel vous stockerez la clé fournie par votre partenaire pour valider sa signature dans les messages. Le fichier de clés doit avoir été déjà créé pour cette clé. «Préparation des fichiers de clés», à la page 29.	Nom du fichier de clés certifiées : Mot de passe du fichier de clés certifiées : Libellé de la clé :

Tableau 89. Fichier de clés destiné au stockage de la clé de chiffrement délivrée par votre fournisseur d'identité partenaire dans une fédération SAML 2.0

Chiffrement	Description	Votre valeur
Fichier de clés	Fichier de clés certifiées dans lequel vous allez stocker la clé destinée au chiffrement des messages adressés à votre partenaire. Cette option s'affiche, car votre partenaire a inclus une clé publique dans les métadonnées que vous utiliserez pour effectuer le chiffrement. Vous devez avoir déjà obtenu le certificat et l'avoir importé dans le fichier de clés de celui-ci. Chapitre 6, «Configuration de la sécurité des messages», à la page 29	Nom du fichier de clés certifiées : Mot de passe du fichier de clés certifiées : Libellé de la clé :

Tableau 90. Validation du certificat serveur pour votre fournisseur d'identité partenaire dans une fédération SAML 2.0

Authentification SSL serveur pour la résolution d'artefact	Description	Votre valeur
Sélectionner le certificat de validation du serveur	Clé publique du certificat affichée durant les communications SSL avec votre partenaire. Il convient que vous ayez discuté, avec votre partenaire, du certificat à utiliser. Vous devez avoir déjà obtenu le certificat et l'avoir ajouté dans le fichier de clés certifiées. Voir «Réception certificat serveur de votre partenaire», à la page 61.	Nom du fichier de clés certifiées : Mot de passe du fichier de clés certifiées : Nom du certificat :

Tableau 91. Authentification client pour votre fournisseur d'identité partenaire dans une fédération SAML 2.0

Authentification SSL client pour la résolution d'artefact	Description	Votre valeur
Informations d'authentification client L'une des options suivantes : • **Authentification de base** – Username – Mot de passe • **Authentification par certificat client** – Certificat à présenter au serveur du fournisseur d'identité. Il s'agit du certificat que vous allez présenter, comme convenu d'un commun accord entre vous et votre fournisseur d'identité partenaire. – Fichier de clés du service de clés Tivoli Federated Identity Manager, dans lequel la clé est stockée – Mot de passe du fichier de clés	Si l'authentification réciproque est exigée par votre partenaire, vous devez en connaître le type. S'il s'agit de l'authentification de base, vous avez besoin d'un nom d'utilisateur et d'un mot de passe. S'il s'agit de l'authentification par certificat client, vous avez besoin du certificat que vous et votre partenaire avez accepté d'utiliser. **Remarque :** Si vous avez besoin d'un certificat, assurez-vous, avant d'effectuer cette tâche, que vous avez convenu avec votre partenaire de sa provenance et que vous l'avez obtenu et importé vers le fichier de clés approprié du service de clés Tivoli Federated Identity Manager. Voir «Obtention de votre certificat client», à la page 62.	Vous pouvez choisir une des options suivantes : • Informations d'authentification de base : – Nom d'utilisateur : – Mot de passe : • Informations relatives à l'authentification par certificat client – Nom de fichiers de clés : – Mot de passe du fichier de clés : – Alias de clé :

Tableau 92. Paramètres de votre fournisseur d'identité partenaire dans une fédération SAML 2.0

Paramètres des partenaires	Description	Votre valeur
URL cible de post-authentification par défaut	Emplacement vers lequel il convient que le navigateur de l'utilisateur soit redirigé si le fournisseur de service ne fournit pas d'URL cible lors de la requête initiale. Cette URL doit être valide, mais ne doit pas nécessairement être active.	

Tableau 93. Paramètres d'assertion SAML pour votre fournisseur d'identité partenaire dans une fédération SAML 2.0

Paramètres d'assertion SAML	Description	Votre valeur
Nom d'utilisateur à employer pour les utilisateurs anonymes	Identificateur de nom permettant à un utilisateur d'accéder à un service via une identité anonyme. Le nom d'utilisateur que vous indiquez ici sera reconnu en tant qu'identifiant à usage unique d'un utilisateur légitime dans le registre d'utilisateurs local. Cette fonction permet aux utilisateurs d'accéder à une ressource du fournisseur de services sans devoir établir une identité fédérée. Cette fonctionnalité est utile dans les cas où le fournisseur n'a pas besoin de connaître l'identité du compte utilisateur mais uniquement de savoir que le fournisseur d'identité a authentifié l'utilisateur (et s'en porte garant).	
Mapper les identificateurs de nom inconnu au nom d'utilisateur anonyme.	Indique que le fournisseur de services peut mapper un alias d'identificateur de nom inconnu persistant à un compte d'utilisateur anonyme. Cette option est désactivée par défaut.	

Tableau 93. Paramètres d'assertion SAML pour votre fournisseur d'identité partenaire dans une fédération SAML 2.0 (suite)

Paramètres d'assertion SAML	Description	Votre valeur
Créer plusieurs instructions d'attribut dans l'utilisateur universel	Sélectionnez cette option pour conserver plusieurs instructions d'attribut dans les groupes dans lesquels elles ont été reçues. Cette option peut se révéler nécessaire si vos règles de mappage d'identité personnalisées sont écrites de manière à s'appliquer à un ou plusieurs groupes d'instructions d'attribut spécifiques. Si cette case n'est pas activée, plusieurs instructions d'attribut sont organisées dans un seul groupe (AttributeList) dans le document STSUniversalUser, ainsi que dans l'assertion. Par défaut, cette option est désélectionnée, ce qui convient à la plupart des configurations.	
Options de chiffrement : • Chiffrer les identificateurs de nom	Case à cocher déterminant si les identificateurs de noms contenus dans les assertions doivent être chiffrés.	Cochez ou non la case.

Tableau 94. Informations de requête d'attribut pour le partenaire de fournisseur d'identité

Requête d'attribut	Description	Votre valeur
Inclure les types d'attributs suivants	Cochez la case pour indiquer les types d'attributs à inclure dans l'assertion. L'astérisque (*), qui est le paramètre par défaut, indique que tous les types d'attributs spécifiés dans le fichier de mappage personnalisé ou par le module de mappage personnalisé seront inclus dans l'assertion. Pour spécifier un ou plusieurs types d'attributs individuellement, tapez chaque type d'attribut dans la case. Par exemple, si vous souhaitez inclure uniquement des attributs conformes au type suivant, entrez cette valeur dans la case : `urn:oasis:names:tc:SAML:2.0:assertion` Utilisez && pour séparer plusieurs types d'attributs.	
Options de chiffrement : • Chiffrer les identificateurs de nom • Chiffrer les assertions • Chiffrer tous les attributs de vérification	Cochez les cases qui spécifient les parties de l'assertion à chiffrer. Si vous n'effectuez aucune sélection et laissez les cases vides, aucune portion des assertions n'est chiffrée dans vos messages. L'option de **chiffrage de tous les attributs d'assertion** indique que tous les attributs de l'assertion sont chiffrés. Si l'option n'est pas sélectionnée, (définie sur false), vous pouvez gérer le chiffrage d'attributs spécifiques via une règle de mappage de jeton XSLT SAML.	Laissez les cases vides ou sélectionnez l'une ou plusieurs des options suivantes : • Chiffrer les identificateurs de nom • Chiffrer les assertions • Chiffrer tous les attributs de vérification
Algorithme de chiffrement : • AES-128 • AES-256 • AES-192 • Triple DES	Type d'algorithme de chiffrement appliqué aux données de chiffrement destinées à votre partenaire. Si vous ne sélectionnez aucun algorithme, la norme DES triple est appliquée.	Sélectionnez l'une des options suivantes si vous avez choisi une option de chiffrement : • AES-128 • AES-256 • AES-192 • Triple DES

Tableau 95. Informations de mappage requête d'attribut pour le partenaire de fournisseur d'identité

Mappage de requête d'attribut	Description	Votre valeur
Options de mappage de requête d'attribut Vous pouvez choisir une des options suivantes : • Fichier de transformation XSL ou JavaScript contenant les règles de mappage • Module de mappage Tivoli Directory Integrator • Module de mappage personnalisé	Type de mappage de requête d'attribut utilisé. Vous devez sélectionner un fichier XSLT, un module de mappage Tivoli Directory Integrator ou un module de mappage personnalisé. Si vous utilisez un fichier XSLT, vous créez ce dernier avant de configurer la fédération. Le module de mappage Tivoli Directory Integrator est un module STS. Le mappage personnalisé est une option avancée. Si vous utilisez cette option, vous devez créer et ajouter un nouveau type et instance de module *avant* de pouvoir l'utiliser dans votre configuration.	L'une des valeurs suivantes : • Fichier XSLT (chemin et nom) • Module de mappage Tivoli Directory Integrator • Nom de l'instance de module de mappage personnalisée

Tableau 96. Options de mappage d'identité pour votre fournisseur d'identité partenaire dans une fédération SAML 2.0

Options de mappage d'identité	Description	Votre valeur
Options de mappage d'identité Vous pouvez choisir une des options suivantes : • Fichier de transformation XSL contenant les règles de mappage • Module de mappage personnalisé • Ne sélectionnez aucune option si vous souhaitez appliquer l'option de mappage d'identité actuellement définie.	Type de mappage d'identité utilisé avec ce partenaire. Vous pouvez ne sélectionner aucune de ces options si vous souhaitez que ce partenaire choisisse l'option de mappage d'identité déjà configurée pour la fédération. Sinon, vous pouvez choisir une option de mappage spécifique et l'appliquer à ce partenaire. Pour choisir une option de mappage, vous devez savoir si vous allez utiliser un fichier XSLT pour le mappage d'identité ou un module de mappage personnalisé. Le mappage personnalisé est une option avancée. Si vous souhaitez utiliser cette option, vous devez créer votre module de mappage et l'ajouter à l'environnement en tant que module type et module d'instance *avant* de pouvoir l'utiliser dans votre configuration. Si vous choisissez d'utiliser un fichier XSLT, vous devez préparer le fichier pour la fédération.	Ne sélectionnez aucune option pour utiliser la configuration de mappage existante. L'une des valeurs suivantes : • Fichier XSLT (chemin et nom): • Nom de l'instance de module de mappage personnalisée :

Une fois que vous avez complété ce formulaire, poursuivez avec les étapes de la rubrique «Ajout à votre partenaire».

Ajout à votre partenaire

Après avoir configuré votre rôle dans la fédération et rassemblé les informations relatives à votre partenaire, vous devez procéder à l'ajout de ce dernier.

Avant de commencer

Avant de débuter cette procédure, complétez le formulaire d'informations relatives au partenaire approprié.

- Si vous êtes le fournisseur de services, ajoutez un partenaire fournisseur d'identité. Utilisez le formulaire destiné au partenaire fournisseur de services en fonction de la norme SAML que vous utilisez dans votre fédération :

- «Formulaire pour fournisseur de services partenaire SAML 1.x», à la page 207
- «Formulaire de fournisseur de services partenaire SAML 2.0», à la page 220

- Si vous êtes le fournisseur de services, ajoutez un partenaire fournisseur d'identité. Utilisez le formulaire destiné au partenaire fournisseur d'identité en fonction de la norme SAML que vous utilisez dans votre fédération :
  - «Formulaire pour fournisseur d'identité partenaire SAML 1.x», à la page 213
  - «Formulaire de fournisseur d'identité partenaire SAML 2.0», à la page 226

Pourquoi et quand exécuter cette tâche

Après avoir complété le fournisseur relatif au partenaire approprié, utilisez l'assistant Partenaire de la console pour ajouter la partenaire. Pour obtenir la description des zones que l'assistant vous invite à renseigner, consultez le formulaire et l'aide en ligne.

Remarque : Pendant la configuration, il se peut que vous soyez invité à redémarrer WebSphere Application Server. Avant de poursuivre la tâche, assurez-vous que le serveur a redémarré entièrement.

Procédure

1. Assurez-vous d'avoir rassemblé les informations relatives à votre partenaire, telles que décrites dans les formulaires. Si, par exemple, vous utilisez un fichier de métadonnées fourni par votre partenaire, copiez-le à un emplacement facilement accessible sur votre ordinateur.
2. Connectez-vous à la console. Cliquez sur **Tivoli Federated Identity Manager** → **Configurer la configuration unique fédérée** → **Fédérations**.
3. Le panneau Fédérations s'affiche. Sélectionnez la fédération dans laquelle vous allez ajouter le partenaire, puis cliquez sur **Ajouter un partenaire**. Suivant la norme SAML que vous utilisez dans votre fédération, l'un des panneaux suivants s'affiche :

   Options de métadonnées
   Ce panneau s'affiche si vous ajoutez un partenaire à une fédération SAML 1.x. Dans ce panneau, cliquez sur l'une des options suivantes :
   - **Importer les métadonnées**
   - **Spécifier manuellement les données SAML**

   Importer les métadonnées
   Ce panneau s'affiche si vous ajoutez un partenaire à une fédération SAML 2.0.
4. Utilisez le formulaire complété comme guide pour renseigner les zones affichées dans chacun des panneaux. Si vous avez besoin de revenir à un panneau précédent, cliquez sur **Précédent**. Si vous souhaitez mettre fin à la configuration, cliquez sur **Annuler**. Sinon, cliquez sur **Suivant** après avoir complété chaque panneau.
5. Vérifiez que les paramètres sont corrects, puis cliquez sur **Terminer**. Le panneau Ajout de partenaire terminé s'affiche. Le partenaire a été ajouté à la fédération, mais il est désactivé par défaut par mesure de sécurité. Vous devez activer le partenaire.
6. Cliquez sur **Activer le partenaire** pour activer ce partenaire.

Que faire ensuite

Si vous n'avez pas encire fourni vos informations de configuration à votre partenaire, vous pouvez le faire maintenant en suivant les instructions de la rubrique «Transmission des propriétés de la fédération au partenaire».

Transmission des propriétés de la fédération au partenaire

Si votre partenaire souhaite vous ajouter en tant que partenaire dans la configuration de sa fédération, vous devez lui fournir les informations nécessaires.

La procédure à suivre varie selon que vous pouvez fournir un fichier de métadonnées ou que vous devez saisir manuellement les informations.

- **Méthode utilisant un fichier de métadonnées**

  Si votre partenaire dispose d'un moyen pour importer vos données, vous pouvez appliquer la méthode du fichier de métadonnées, quel que soit le type de fédération SAML (1.x ou 2.0) configuré.

  1. A l'aide de la console, générez un fichier de métadonnées contenant les informations nécessaires pour la configuration de la fédération, ainsi qu'une clé permettant de valider les signature de message de réponse si vous exigez la validation des signatures. Pour plus d'informations, voir «Exportation des propriétés d'une fédération».
  2. Il se peut que vous deviez également fournir à votre partenaire les clés et certificats appropriés, suivant votre rôle et la norme SAML utilisés dans la fédération. Voir Chapitre 6, «Configuration de la sécurité des messages», à la page 29.

- **Méthode manuelle**

  Si vous avez configuré une fédération SAML 1.x, vous pouvez collecter manuellement la configuration nécessaire au lieu d'exporter les propriétés dans un fichier.

  Remarque : L'utilisation d'un fichier de métadonnées permet d'éliminer les risques d'erreurs susceptibles de se produire lors de l'entrée manuelle des données.

  Pour collecter manuellement des informations, procédez comme suit.

  1. Utilisez le panneau Propriétés de la fédération dans la console pour obtenir les propriétés. Pour afficher le panneau Propriétés de la fédération, voir «Affichage des propriétés d'une fédération», à la page 237.

     Utilisez le contenu du panneau Propriétés de la fédération pour accéder aux propriétés de votre fédération.
  2. Il se peut que vous deviez également fournir à votre partenaire les clés et certificats de votre fédération. Voir Chapitre 6, «Configuration de la sécurité des messages», à la page 29.

Exportation des propriétés d'une fédération

Si vous souhaitez rejoindre une fédération partenaire, vous devez indiquer vos propriétés de configuration de fédération. Vous pouvez exporter vos propriétés de fédération vers un fichier et les partager avec votre partenaire.

Procédure

1. Connectez-vous à la console, puis cliquez sur **Tivoli Federated Identity Manager → Configurer la connexion unique fédérée → Fédérations**.

2. Le panneau Fédérations s'affiche. Sélectionnez une fédération dans le tableau.
3. Cliquez sur **Exporter**. Le navigateur affiche une fenêtre de message qui vous invite à sauvegarder le fichier contenant les données exportées. Cliquez sur **OK**. La fenêtre de téléchargement du navigateur vous invite à entrer un emplacement de sauvegarde du fichier.
4. Sélectionnez un répertoire et un fichier de métadonnées, puis cliquez sur **Enregistrer**. La syntaxe des fichiers de métadonnées se présente comme suit :

   *nomdelafédération_nomdel'entreprise*_métadonnées.xml

   Par exemple, pour une fédération dénommée fédération1 et une entreprise nommée ABC, le nom du fichier de métadonnées sera libellé comme suit :

   fédération1_ABC_métadonnées.xml

   Placez ce fichier dans un endroit facilement accessible. Vous devez le fournir à votre partenaire lorsque ce dernier souhaite importer les informations de configuration de cette fédération.

Affichage des propriétés d'une fédération

Utilisez l'option Propriétés de la fédération pour afficher les caractéristiques d'une fédération existante ou pour modifier une fédération existante. Cette tâche peut être utile si vous devez collecter manuellement les propriétés de votre fédération afin de les partager avec votre partenaire.

Procédure

1. Connectez-vous à la console, puis cliquez sur **Tivoli Federated Identity Manager → Configurer la connexion unique fédérée → Fédérations**.
2. Le panneau Fédérations affiche une liste de fédérations configurées. Sélectionnez une fédération.
3. Cliquez sur **Propriétés** pour afficher les propriétés d'une fédération existante.
4. Sélectionnez les propriétés à modifier. Pour la description des propriétés d'une fédération, voir l'aide en ligne.
5. Une fois que vous avez terminé d'afficher ou de modifier les propriétés, cliquez sur **OK** pour fermer la fenêtre des propriétés de fédération.

Synchronisation des horloges système dans la fédération

Du fait que les jetons de sécurité possèdent des délais d'expiration, votre horloge système doit être synchronisée sur celle de votre partenaire.

Pourquoi et quand exécuter cette tâche

Vous devez vous assurer que, dans votre environnement, l'horloge du système sur lequel le composant d'exécution et les services de gestion de Tivoli Federated Identity Manager sont installés est synchronisé avec celui de votre partenaire.

Reportez-vous aux instructions contenues dans la documentation de votre système d'exploitation pour plus d'informations sur la synchronisation des horloges système. Envisagez d'utiliser le protocole de synchronisation d'horloge NTP (source d'horodatage null).

Chapitre 18. Planification d'une fédération Information Card

Le système Information Card permet aux utilisateurs de gérer leurs identités numériques obtenues auprès de différents fournisseurs et de les utiliser pour accéder à divers services qui acceptent ces identités numériques.

Ce guide de planification passe en revue la norme d'implémentation sous Tivoli Federated Identity Manager de la norme Information Card et explique comment planifier le processus de configuration. Ce guide ne constitue pas une présentation exhaustive de la norme Information Card.

Il convient que les administrateurs non familiarisés avec cette norme consultent les informations relatives à Information Card sur le site Web de Microsoft.

La prise en charge de Tivoli Federated Identity Manager pour Information Card inclut le déploiement de Tivoli Federated Identity Manager suivant les deux rôles fournis par Information Card : fournisseur d'identité gérée (Managed Identity Provider) et partie de confiance (Relying Party).

Le flux de protocole établi lorsque l'utilisateur fournit une carte d'information pour s'authentifier sur un site Web s'apparente à un flux de connexion à l'aide de masques de saisie, mais requiert quelques étapes complémentaires.

1. L'utilisateur dirige le navigateur sur une page Web protégée nécessitant une authentification.
2. Le site redirige le navigateur vers une page de connexion. Dans un navigateur compatible avec Information Card, la page de connexion contient une balise HTML qui permet à l'utilisateur de choisir une carte d'information afin de s'authentifier sur le site. Lorsque l'utilisateur sélectionne la balise, le navigateur fait appel à un *sélecteur d'identité*.

   Remarque : Un *sélecteur d'identité* est un module d'extension de navigateur qui permet à celui-ci d'utiliser le protocole Information Card. Les modules d'extension portent parfois le nom d'*agents d'identité*.
3. Le code permettant la prise en charge des cartes d'information dans le navigateur appelle le sélecteur d'identité, puis transmet les valeurs de paramètres fournies par la balise HTML d'Information Card obtenue à partir du site Web à l'étape 2.

   L'utilisateur sélectionne ensuite une carte d'information, qui représente une identité numérique utilisable pour s'authentifier sur le site.
4. Le sélecteur d'identité envoie la carte d'information au fournisseur d'identité Tivoli Federated Identity Manager. Le fournisseur d'identité utilise le service STS de Tivoli Federated Identity Manager pour traiter le message WS-Trust et les données de WS-Metadata Exchange, puis générer un jeton contenant les données d'identification de l'utilisateur. Le fournisseur d'identité renvoie le jeton au navigateur.
5. Le navigateur transmet les données d'identification de l'utilisateur au site Web qui protège les ressources demandées. Le site valide ces droits d'accès, puis redirige le navigateur sur la page demandée à l'origine.

Dans le flux de protocole, la partie de confiance et le fournisseur d'identité ne communiquent pas directement ensemble. Par défaut, aucune partie n'a connaissance de l'existence de l'autre partie. La partie de confiance ne sait pas quel

fournisseur d'identité a été sélectionnée par l'utilisateur tant que le jeton n'a pas été reçu à l'étape 5. A ce moment-là, la partie de confiance peut prendre connaissance de l'identité en examinant le continue de la zone de l'émetteur (Issuer) dans le jeton.

Information Card permet au fournisseur d'identité de demander l'identification de la partie de confiance, mais cette procédure n'est pas obligatoire et n'est généralement pas recommandée.

Présentation du fournisseur d'identité Information Card

Le fournisseur d'identité prend en charge les éléments suivants :

- Emission de cartes gérées

  L'émission de cartes gérées a lieu lorsqu'un utilisateur s'authentifie auprès d'un fournisseur d'identité Tivoli Federated Identity Manager et accède à une adresse URL de téléchargement de carte. L'adresse URL envoie à l'utilisateur un modèle de formulaire HTML lui demandant d'indiquer les informations requises pour émettre la carte. Une fois que l'utilisateur a fourni les informations requises, Tivoli Federated Identity Manager émet la carte et l'envoie vers le navigateur de l'utilisateur. Celui-ci peut alors la sauvegarder pour un usage ultérieur.
- Extraction des jetons de sécurité pour les cartes gérées

  Cette prise en charge est permise par le service de jeton de sécurité (STS). Ce composant prend en charge d eux types de messages SOAP issus d'un sélecteur d'identité Information Card. Les messages SOAP sont requis pour permettre à un sélecteur d'identité d'obtenir un jeton de sécurité destiné à la carte d'information gérée d'un utilisateur.

  Remarque : Un *sélecteur d'identité* est un module d'extension de navigateur. On l'appelle parfois *agent d'identité*.

  Seuls les jetons de sécurité SAML 1.1 sont pris en charge.

Lorsque Tivoli Federated Identity Manager fait office de fournisseur d'identité, il prend en charge l'émission des cartes gérées et émet des jetons de sécurité pour les cartes gérées. La prise en charge concerne les caractéristiques suivantes :

- Emission de cartes gérées
- Noeuds finals pour l'échange de métadonnées et traitement des messages WS-Trust
- Prise en charge des réclamations Information Card
- Fédération unique destinée à contenir les noeuds finals du fournisseur d'identité
- Une chaîne d'accréditation sécuritaire destinée à convertir les informations d'identité des utilisateurs en jetons SAML 1.1

Remarque : Les fédérations Information Card ne permettent pas de maintenir les paramètres de configuration sous forme de métadonnées. Cela signifie que que les dans le cas des déploiements Information Card, il n'existe aucune métadonnées à exporter ni à importer entre les fournisseurs d'identité et les parties de confiance.

Emission de cartes gérées

Tivoli Federated Identity Manager permet de prendre en charge l'émission de cartes gérées par des fournisseurs d'identité, ainsi que l'extraction de jetons de sécurité à partie de cartes gérées émises par d'autres autorités.

Tivoli Federated Identity Manager fournit un noeud final sécurisé permettant de télécharger une carte gérée. Lorsqu'un utilisateur accède au noeud final via un navigateur, un fichier modèle HTML est chargé, puis renvoyé à l'utilisateur. L'utilisateur est invité à fournir les informations requises pour permettre l'émission de la carte gérée.

Les informations obligatoires sont les suivantes :

- Nom d'utilisateur

  Valeur arbitraire attribuée à la carte par l'utilisateur.
- Ensemble des réclamations prises en charge par la carte.

  Une réclamation est un identificateur URI (Uniform Resource Indidentificator) qui représente des noms d'attributs qualifiés. Tivoli Federated Identity Manager utilise la liste des réclamations pour déterminer la nature des informations (chaque réclamation, ainsi que la valeur correspondante) qui doivent être placées dans le jeton de sécurité généré au moment de l'exécution, lorsque la carte gérée est traitée.
- Lorsque la fédération utilise une méthode d'authentification appelée *droit d'accès auto-émis* (ou *assertion SAML auto-signée*), l'utilisateur est invité à fournir un jeton généré par une carte auto-émise dans le cadre de la requête.

  Lorsque la fédération utilise une méthode d'authentification appelée *jeton de nom d'utilisateur*, l'utilisateur n'est pas tenu de spécifier ce paramètre.

Tivoli Federated Identity Manager fournit deux modèles de pages HTML.

- Lorsque la méthode d'authentification repose sur un jeton de nom d'utilisateur, le modèle utilisé est getcard_ut.html.
- Lorsque la méthode d'authentification repose sur des droit d'accès émis de façon autonome, le modèle utilisé est getcard_sss.html.

Les administrateurs peuvent modifier les fichiers modèles HTML afin que ceux-ci répondent au mieux aux exigences du déploiement local.

Les fichiers modèles getcard_* contiennent les macros suivantes, qui sont remplacées par les spécifiques à la demande émise par l'utilisateur final.

@FORMACTION@
: Cette macro est remplacée par l'action URL du formulaire requis vers laquelle le formulaire HTML est envoyé.

@USERNAME@
: Cette macro est remplacée par le nom d'utilisateur tel que spécifié soit par le nom de connexion de l'utilisateur Tivoli Access Manager, soit par un utilisateur WebSphere authentifié. Le nom d'utilisateur Tivoli Access Manager est employé lorsque WebSEAL est le serveur point de contact. Le nom d'utilisateur WebSphere est employé lorsque WebSphere est le serveur point de contact.

  Cette valeur peut être utilisée pour renseigner préalablement le paramètre du nom de carte dans le modèle.

Lorsque l'utilisateur renvoie le formulaire par requête POST à Tivoli Federated Identity Manager, les informations sont placées dans les macros contenues dans une fichier modèle XML appelé infocard_template.xml. Ce fichier modèle représente la carte gérée renvoyée à l'utilisateur via le navigateur.

Dans la plupart des déploiements, les administrateurs système n'ont pas besoin de modifier les macros pour pouvoir utiliser les macros du fichier infocard_template.xml. Toutefois, le fichier contient un certain nombre de macros qui peuvent être modifiées si nécessaire.

Remarque : Pour afficher la liste des macros, voir «Macros de remplacement dans le fichier XML infocard_template», à la page 269

La prise en charge d'Information Card par Tivoli Federated Identity Manager s'applique uniquement au type de jeton SAML 1.1. Deux représentations existent pour le type de jeton SAML 1.1 :

SAML 1.1
urn:oasis:names:tc:SAML:1.0:assertion

SAML 1.1
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1

La plupart des cartes d'information gérées prennent en charge les deux représentations. L'utilisateur final ne sélectionne pas le type de jeton. La macro @SUPPORTED_TOKENS@ contenue dans le fichier infocard_template.xml est définie dans les deux représentations SAML illustrées ci-dessus.

Tivoli Federated Identity Manager prend en charge deux méthodes utilisées par le sélecteur d'identité pour authentifier l'utilisateur auprès du noeud final du fournisseur d'identité (service STS). Chaque méthode prend en charge un modèle de remplacement distinct pour la macro @USERCRED@ dans le modèle de carte d'information (infocard_template.xml).

Le type d'authentification est spécifié par l'administrateur lors de la configuration de la fédération. Les valeurs de configuration du paramètre `authenticationMethod` correspondent aux fichiers modèles comme suit :

UsernameToken
Renvoie au fichier modèle **infocard_usercred_usernametoken.xml**

Le fichier modèle contient une macro de remplacement :

@USERNAME@
Cette macro est remplacée par le nom d'utilisateur tel que spécifié soit par le nom de connexion de l'utilisateur Tivoli Access Manager, soit par un utilisateur WebSphere authentifié. Le nom d'utilisateur Tivoli Access Manager est employé lorsque WebSEAL est le serveur point de contact. Le nom d'utilisateur WebSphere est employé lorsque WebSphere est le serveur point de contact.

SelfSignedSAML
Renvoie au fichier modèle **infocard_usercred_selfsignedsaml.xml**

Le fichier modèle contient une macro de remplacement :

@PPID@
La macro est remplacée par l'identificateur PPID de la carte auto-émise envoyée avec le formulaire getcard_sss.html. Ceci se produit lorsque la fédération utilise la méthode d'authentification SelfSignedSAML.

Tivoli Federated Identity Manager enregistre ces données sous forme d'alias pour l'utilisateur en cours dans le service d'alias de

Tivoli Federated Identity Manager. L'alias sert à mapper en retour la carte auto-émise avec l'utilisateur de Tivoli Federated Identity Manager lorsque cette carte est utilisée (lors de l'exécution) pour générer une SAML destinée à l'authentification auprès du service STS du fournisseur d'identité.

Fédérations de fournisseurs d'identité

La configuration de fédérations pour Information Card diffère singulièrement de la configuration de fédérations destinées aux autres protocoles de connexion unique tels que SAML 2.0, Liberty, WS-Federation ou OpenID. L'une des principales différences réside dans le fait que le fournisseur d'identité Information Card n'a pas besoin de connaître la partie de confiance récipiendaire du jeton de sécurité. Le service STS du fournisseur d'identité interagit uniquement avec le sélecteur d'identité. Cette configuration permet d'éliminer la nécessité de configurer des propriétés qui contiennent des informations relatives aux partenaires.

Le concept de configuration partenaire n'existe dans les configurations Information Card que dans le cadre de la configuration des modules de jetons utilisés par le service d'accréditation.

Les propriétés clés qui définissent une fédération pour un fournisseur d'identité sont les suivantes :

ProtocolID
Tivoli Federated Identity Manager utilise un ID de protocole en tant qu'identificateur unique. La fédération Information Card comporte la syntaxe protocolId suivante :

`https://<nom_hôte:port>/FIM/sps/<nom_fédération>/infocard`

Par exemple :

`https://www.exampleidentitydemo.com/FIM/sps/csip/infocard`

Noeud final permettant d'obtenir une carte gérée
Noeud final destiné au traitement de l'interaction HTML avec un utilisateur authentifié, afin de permettre la génération et le téléchargement d'une carte gérée.

L'adresse URL du noeud final repose sur le paramètre ProtocolID. Par exemple :

`https://www.exampleidentitydemo.com/FIM/sps/csip/infocard/getcard.crd`

Le composant Tivoli Federated Identity Manager (délégué du service de protocole de connexion unique) lié au noeud final exécute les tâches suivantes :

1. Invite l'utilisateur à indiquer les informations requises pour générer une carte d'information. Les données de la carte d'information concernent le nom de la carte et les réclamations prises en charge. Lorsque la méthode d'authentification repose sur des droit d'accès émis de façon autonome, une carte d'information personnelle est générée.
2. Lorsque le mécanisme d'authentification repose sur une carte émise de façon autonome ("SelfSignedSAML"), le délégué créer et enregistre un alias dans le service concerné. Une correspondance entre l'alias et la carte personnelle présentée par l'utilisateur durant ce processus est établie dans le compte utilisateur de la personne actuellement authentifiée dans la session de navigateur.

3. Génère la carte gérée à partir d'un modèle XML dont les divers composants sont alimentés dynamiquement. Le délégué signe la carte en utilisant la clé privée du certificat SSL associé au serveur point de contact, puis renvoie la carte au navigateur.

Noeud final d'échange de métadonnées

Un noeud final est utilisé par le sélecteur d'identité (au moment de l'exécution) pour échanger des métadonnées, afin de déterminer les exigences en termes de connexion et de formatage des messages (pour RST) liées au service de jeton de sécurité du fournisseur d'identité.

L'adresse URL du noeud final de métadonnées repose sur le paramètre ProtocolID. Par exemple :

```
https://www.exampleidentitydemo.com/FIM/sps/csip/infocard/mex
```

Le noeud final d'échange de métadonnées comporte un fichier modèle XML appelé metadata_template.xml. Ce fichier contient des macros disponibles en vue d'un remplacement.

Remarque : Les macros par défaut doivent normalement pouvoir être exécutées par les administrateurs. Il n'est pas nécessaire de modifier les macros pour pouvoir utiliser le fichier modèle.

Les macros de remplacement du fichier metadata_template.xml sont les suivantes :

@IPSTS@
Adresse URL du noeud final de service STS pour le fournisseur d'identité dans la fédération.

@IPPOLICY@
Cette valeur contient des informations WS-Policy. Les informations dépendent du type de jeton d'authentification utilisé pour l'authentification auprès du service STS du fournisseur d'identité. Les informations WS-Policy information sont lues à partir d'un fichier modèle.

@IPCERTIFICATE@
Certification SSL public codé sur base 64 du serveur point de contact

Chacune des méthodes d'authentification prend en charge un modèle de remplacement distinct pour la macro @IPPOLICY@ dans le modèle d'échange de métadonnées.

Les fichiers modèles de chaque méthode d'authentification sont les suivants :

Authentification avec UsernameToken
metadata_policy_usernametoken.xml

Authentification avec SelfSignedSAML
metadata_policy_selfsignedsaml.xml

Les fichiers metadata_policy_usernametoken.xml et metadata_policy_selfsignedsaml.xml ne comportent aucune macro de remplacement. Les fichiers modèles sont constitués de différents ensembles de règles adaptés à chaque méthode. Les administrateurs Information Card n'ont pas besoin de modifier ces fichiers.

Noeud final pour la réception des messages WS-Trust

Le service STS du fournisseur d'identité dispose d'un noeud final qui reçoit

les messages WS-Trust en provenance du sélecteur d'identité. Le module du fournisseur d'identité Information Card traite la demande entrante, y compris les modifications requises par le service d'accréditation Tivoli Federated Identity Manager, puis communique avec le service d'accréditation afin d'obtenir le jeton nécessaire.

Réclamations Information Card

Information Card utilise des informations appelées *réclamations* (claims) pour définir les attributs susceptibles d'être nécessaires lors de la satisfaction d'une requête d'utilisateur. Une carte d'information contient les indicateurs URI (Uniform Resource Indicators) relatifs à l'ensemble des réclamations prises en charge par leur émetteur.

Un sélecteur d'identité peut utiliser les informations des réclamations afin de déterminer si une carte d'identité peut être utile à la connexion auprès d'une partie de confiance spécifique. A titre d'exemple, lorsqu'une partie de confiance exige la réclamation relative à une adresse électronique et que le fournisseur d'identité associé à une carte gérée ne prend pas en charge cette réclamation, le fournisseur d'identité ne proposera pas la carte gérée en tant qu'option d'ouverture de session auprès de la partie de confiance concernée.

Le fournisseur de carte gérée de Tivoli Federated Identity Provider n'oppose aucune restriction quant à l'ensemble des réclamations qui peuvent être spécifiées dans les cartes. Les modèles (getcard_ut.html et getcard_sss.html) contiennent la série complète des réclamations standard prises en charge. Les administrateurs peuvent ajouter la prise en charge de réclamations supplémentaires en modifiant les modèles.

L'agent d'identité Information Card envoie une requête WS-Trust au module Tivoli Federated Identity Manager (délégué) portant sur le service du protocole de connexion unique. La requête WS-Trust contient un élément de réclamation (wst:Claims) dans lequel se trouve l'ensemble des réclamations émises.

La figure 17 illustre quelques exemples de réclamations.

```
<wst:Claims>
 <wsid:ClaimType
  Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname"
  xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity" />
 <wsid:ClaimType
  Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
  xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity" />
 <wsid:ClaimType
  Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"
  xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity" />
 <wsid:ClaimType
  Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
       privatepersonalidentifier"
  xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity" />
</wst:Claims>
```

Pour afficher la série standard des réclamations prises en charge sous Microsoft, voir : http://schemas.xmlsoap.org/ws/2005/05/identity/claims.xsd.

Figure 17. Exemples de réclamations provenant d'un agent d'identité Information Card

Pages d'erreurs Information Card

Les identificateurs de page suivants sont fournis :

/infocard/error_get_card.html
Renvoie à la page suivante :
`/infocard/error_get_card.html`

Permet d'afficher une erreur dans la sortie HTML lorsqu'un utilisateur tente de télécharger une carte.

/infocard/error_get_metadata.html
Renvoie à la page suivante :
`/infocard/error_get_metadata.html`

Permet d'afficher une erreur dans la sortie HTML lorsqu'un utilisateur sélectionnant une identité tente de télécharger des métadonnées via la requête HTTP GET (au lieu de SOAP sur HTTP/POST).

Présentation de la partie de confiance Information Card

Le rôle de la partie de confiance est similaire à celui d'un *fournisseur de services* en ce sens qu'elle est prise en charge par Tivoli Federated Identity Manager pour d'autres protocoles de connexion unique. La partie de confiance se compose d'un service de connexion implémenté dans un composant de service de connexion unique (délégué), ainsi qu'une chaîne WS-Trust. L'implémentation Tivoli Federated Identity Manager prend en charge les activités suivantes :

- Réception des jetons d'assertion SAML 1.x
- L'utilisation de la connexion à la fois avec les cartes auto-émises et les cartes gérées émises par les autres fournisseurs d'identité.

Dans le modèle Information Card, la clé publique SSL (Secure Socket Layer) sert à chiffrer le jeton qui est envoyé à la partie de confiance sur les noeuds finals. La clé SSL est la clé de la session SSL établie entre le navigateur et le site présentant la page Web (conformément à la spécification des balises OBJECT imbriquées). Ceci implique que Tivoli Federated Identity Manager a besoin d'accéder aux clés SSL utilisées par le serveur point de contact. L'administrateur est tenu de configurer l'accès à ces clés durant la configuration de Tivoli Federated Identity Manager Information Card.

Lors d'une identification d'entreprise, il est recommandé de veiller à ce que les sites Web emploient des certificats X509v3 comportant des logotypes (également appelés certificats de validation étendue) à la place des certificats serveur SSL.

Le terme de **partie de confiance** dans le contexte d'Information Card désigne un rôle similaire à celui de **fournisseur de services** dans d'autres protocoles de connexion unique pris en charge par Tivoli Federated Identity Manager.

En tant que partie de confiance, Tivoli Federated Identity Manager prend à la fois en charge les fournisseurs d'identité gérés et auto-émis.

La configuration de Tivoli Federated Identity Manager permet aux administrateurs de configurer la prise en charge d'un ou deux types de fournisseurs.

Avant de procéder à la configuration de Tivoli Federated Identity Manager, l'administrateur de la partie de confiance peut obtenir des clés publiques auprès du fournisseur d'identité, afin de les utiliser lors de la validation des signatures numériques sur les assertions reçues en provenance dudit fournisseur.

L'implémentation de Tivoli Federated Identity Manager inclut la prise en charge suivante :

- Accès de l'utilisateur à la partie de confiance
- Réclamations Information Card
- Fédérations pour le traitement de requêtes
- Echange de jetons

Accès de l'utilisateur à une partie de confiance

Lorsqu'un utilisateur tente d'accéder à une ressource protégée sur un site Web sans s'être préalablement vu octroyer des droits d'accès, un serveur Web *point de contact* invite généralement l'utilisateur à établir ses droits d'accès en renseignant une page de connexion. L'utilisation d'une carte d'information dans ce scénario dépend des conditions préalables suivantes :

- L'utilisateur doit utiliser un navigateur configuré pour Information Card. Les navigateurs compatibles avec les cartes d'information sont équipés d'un *sélecteur d'identité* installé sous forme de module d'extension.
- La page de connexion émise par le point de contact qui protège les ressources sur le site Web doivent comporter des balises OBJECT spécifiques. Les balises OBJECT contenues dans la page déclenchent l'interaction de Information Card avec le navigateur.
- L'adresse URL à laquelle accède le navigateur doit utiliser le protocole HTTPS.

```
<form method="post" action="/FIM/sps/infocard-fed/infocard/login">
   ...
   <input type="hidden" name="TARGET" value="/TheResource"/>
   <object type="application/x-informationCard" name="xmlToken">
      <param name="requiredClaims"
             value="http://schemas.xmlsoap.org/ws/2005/05/identity/
                    claims/privatepersonalidentifier" />
   </object>
   <input type="submit" value="Login"/>
   ...
</form>
```

Figure 18. Exemple de format de connexion utilisé par la partie de confiance

La figure 18 illustre des exemples d'éléments XML contenus dans le format de connexion requis. Le format de connexion requiert plusieurs paramètres importants :

Action de la méthode de formulaire

La valeur du paramètre `action` doit correspondre à l'adresse URL du noeud final de la fédération Information Card. Le navigateur compatible avec Information Card est redirigé vers ce noeud final afin de traiter le jeton de sécurité émis par le fournisseur d'identité.

Remarque : L'administrateur spécifie ce noeud final lors de la configuration de Tivoli Federated Identity Manager Information Card.

Nom masqué du type d'entrée

Le formulaire de connexion doit normalement comporter un élément `masqué` qui contient :

- Le paramètre `name` défini sur `TARGET`
- Le paramètre `value` défini selon l'adresse URL vers laquelle le navigateur est redirigé lorsque le processus de connexion aboutit.

Il existe une manière alternative de spécifier l'adresse URL vers laquelle le navigateur doit être redirigé. La cible peut être spécifiée au moyen d'un paramètre de requête au format chaîne appliqué à la valeur du paramètre `action`. Par exemple, en utilisant les valeurs de la figure 18, à la page 247 :

```
action=''FIM/sps/infocard-fed/infocard/login?TARGET=/theResource''
```

Lorsque WebSEAL tient le rôle de serveur point de contact, la macro `%URL%` prise en charge par WebSEAL peut être utilisée pour spécifier l'adresse URL cible.

Nom du type d'objet

La valeur du paramètre `name` contenu dans l'élément `OBJECT` doit être définie sur `xmlToken`.

Le navigateur envoie cette valeur à la partie de confiance. L'implémentation de Tivoli Federated Identity Manager pour la partie de confiance Information Card utilise ce paramètre pour accéder au jeton de sécurité.

Tivoli Federated Identity Manager défini en tant que partie de confiance prend en charge les types de jetons SAML suivants :

- Identificateur URI pris en charge par tous les types de fournisseurs :

  ```
  urn:oasis:names:tc:SAML:1.0:assertion
  ```

- Identificateur URI pris en charge uniquement par les fournisseurs d'identité autonomes :

  ```
  http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1
  ```

Il est possible de spécifier l'un ou plusieurs de ces types d'URI dans le paramètre `tokenType` de la balise `OBJECT`.

Fédérations de parties de confiance

Tivoli Federated Identity Manager établit et utilise les fédérations Information Card de manière similaire, mais pas totalement identique aux fédérations employées pour d'autres protocoles de connexion unique. Les différences sont :

- L'interaction entre parties de confiance fait partie du processus d'authentification utilisé par le serveur point de contact (par exemple WebSEAL) pour octroyer l'accès aux ressources protégées.

  Pour les autres protocoles de connexion unique, le serveur point de contact présente une page de connexion lors de l'accès à une ressource protégée, puis authentifie l'utilisateur et produit les droits d'accès destinés à l'utilisateur. Pour Information Card, Tivoli Federated Identity Manager agit en tant que partie de confiance pour exécuter le processus d'authentification et produire les droits d'accès destinés à l'utilisateur.

  La partie de confiance est avertie qu'une connexion utilisateur est en cours au moment où un jeton de sécurité (assertion) est reçu au niveau du noeud final de messages. La partie de confiance doit alors décider d'accepter ou rejeter le jeton de sécurité.

- Contrairement à un fournisseur de services dans le cas des autres protocoles de connexion unique, la partie de confiance n'envoie aucun message au fournisseur d'identité. Les messages sont envoyés par le *Sélecteur d'identité*, sans que la partie de confiance ne soit connue.
- Dans une fédération Information Card, les fournisseurs d'identité constituent une série l'entités fédérées de manière souple dont le site Web accepte les jetons d'assertion.
- Information Card prend en charge le fournisseur d'identité à émission autonome.

Information Card nécessite la création d'une fédération pour représenter la partie de confiance autonome (*self*). Le terme *self* ne doit pas être confondu avec l'autonomie d'émission du fournisseur d'identité. Le terme sert à distinguer l'origine (ou émetteur) de la fédération de tous les partenaires qui y sont ajoutés par la suite. Les propriétés de l'entité autonome sont les suivantes :

- Le noeud final de connexion
- Paramètres indiquant les types de jetons acceptés
- L'alias du fichier de clés issu du serveur point de contact destiné à être utilisé dans les connexions SSL (Secure Socket Layer).
- Une règle de mappage par défaut. La règle de mappage peut être remplacée par une configuration de partenaire.

La fédération Information Card utilise la convention de dénomination standard Tivoli Federated Identity Manager pour le paramètre **protocolID**. La syntaxe est la suivante :

```
https://<nom_hôte:port>/FIM/sps/<nom_fédération>/infocard
```

Si par exemple l'hôte défini pour les noeuds finals de la fédération est `rp.example.com`, que l'écoute s'effectue sur le port `443` et que le nom de la fédération est `MyInfoCard-rp`, l'ID de protocole est le suivant:

```
https://rp.example.com:443/FIM/sps/MyInfoCard-rp/infocard
```

Les fédérations de partenaires sont nécessaires pour représenter les fournisseurs d'identité. Il ne peut exister qu'un seul partenaire émettant des jetons de façon autonome. Le nombre de partenaires fournisseurs d'identité gérés est illimité. Il est également possible d'ajouter **n'importe quel** partenaire fournisseur d'identité. Ce partenaire peut être utilisé pour l'accès au compte invité.

Partenaire à émission automatique

Tivoli Federated Identity Manager configure un partenaire en définissant le paramètre protocolId comme suit :

```
http://schemas.xmlsoap.org/ws/2005/05/identity/issuer/self
```

Ce partenaire est utilisé pour traiter les cartes auto-émises.

Partenaire de fournisseur d'identité géré désigné

Un partenaire fournisseur géré doit posséder un élément `Issuer URI`. La zone `Issuer` du mappage de la chaîne d'accréditation est définie sur la valeur `protocolID`. Lors de la signature des assertions provenant de ce fournisseur, un alias de clé publique doit être configuré pour le partenaire. L'administrateur doit importer la clé publique dans un fichier de clés Tivoli Federated Identity Manager avant de configurer la fédération. Il convient d'importe la clé via le service de clés de Tivoli Federated Identity Manager.

Tout fournisseur d'identité partenaire

La configuration de `tout` partenaire permet d'effectuer une configuration générique. Les assertions provenant de ces fournisseurs doivent utiliser *une seule* des valeurs suivantes pour `<saml:SubjectConfirmationMethod>` :

```
urn:oasis:names:tc:SAML:1.0:cm:bearer
urn:oasis:names:tc:SAML:1.0:cm:sender-vouches
```

Lorsque l'assertion est signée, elle doit inclure un élément `<ds:KeyInfo>` inclus dans la signature, contenant une clé publique permettant la validation des signatures.

Remarque : Il convient d'utiliser cette configuration uniquement pour l'accès utilisateur invité. Dans une telle configuration, tous les utilisateurs sont rattachés à un compte invité.

Activation de site Web pour Information Card

L'implémentation Tivoli Federated Identity Manager du profil Information Card interagit avec l'implémentation Microsoft CardSpace™ version 1.0. Ces deux implémentations reposent sur le profil Information Card version 1.0. Cette version est prise en charge sous Microsoft Internet Explorer version 7.

Les navigateurs compatibles avec Information Card doivent reconnaître les balises HTML ou XHTML spéciales destinées à l'appel du sélecteur d'identité, transmettre les paramètres codés sur le sélecteur d'identité de la plateforme, puis renvoyer via une requête POST le jeton résultant à partir du type d'authentification sélectionné par l'utilisateur pour le choix d'une identité numérique.

Les sites Web employant l'authentification Information Card doivent prendre en charge deux ensembles de fonctionnalités :

- L'ajout de balises HTML ou XHTML à leur page de connexion afin de pouvoir demander une ouverture de session Information Card
- Le Code permettant à l'utilisateur de se connecter au site au moyen des droits d'accès qu'il fournit dans l'opération HTTP POST

En réponse à la connexion Information Card, le site Web se comporte généralement comme suit :

- Inscription du même cookie de navigateur côté client que celui qui serait utilisé si l'ouverture de session avait lieu à partir d'une authentification par nom d'utilisateur et mot de passe (ou suivant d'autres mécanismes)
- Emission des mêmes redirections du navigateur

Modifications des pages de connexion

Les extensions HTML telles que la balise OBJECT sont utilisées pour signaler au navigateur le moment où le sélecteur d'identité doit être appelé. Néanmoins, toutes les extensions HTML ne sont pas prises en charge par l'ensemble des navigateurs.

En outre, certaines extensions HTML couramment prises en charge sont désactivées dans les configurations de navigateur hautement sécurisées. A titre d'exemple, la balise OBJECT est désactivée par les paramètres de sécurité de certains navigateurs, y compris Internet Explorer.

Une alternative à l'utilisation d'extensions HTML consiste à employer une syntaxe XHTML qui n'est pas désactivée lors de la modification des paramètres de sécurité du navigateur. Toutefois, certains navigateurs n'offrent pas une prise en charge complète du format XHTML.

Pour fournir une solution répondant à tous les types de scénarios, deux formats d'extension HTML existent. Les navigateurs prennent en charge l'un ou l'autre de ces formats d'extension, voire les deux.

Syntaxe OBJECT

La figure 19 montre un exemple de page utilisant la syntaxe OBJECT pour demander que l'utilisateur se connecte à l'aide de données Information Card.

```
<html>
<head>
<title>Welcome to Fabrikam</title>
</head>
<body>
<img src='fabrikam.jpg'/>
<form name="ctl00" id="ctl00" method="post"
action="https://www.fabrikam.com/InfoCard-Browser/Main.aspx">
<center>
<img src='infocard.bmp' onClick='ctl00.submit()'/>
<input type="submit" name="InfoCardSignin" value="Log in"
id="InfoCardSignin" />
</center>
<OBJECT type="application/x-informationCard" name="xmlToken">
<PARAM Name="tokenType"
Value="urn:oasis:names:tc:SAML:1.0:assertion">
<PARAM Name="issuer" Value=
"http://schemas.xmlsoap.org/ws/2005/05/identity/issuer/self">
<PARAM Name="requiredClaims" Value=
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">
</OBJECT>
</form>
</body>
</html>
```

Figure 19. Exemple de syntaxe OBJECT

Veuillez noter le type OBJECT `application/x-informationCard`. Lorsque l'utilisateur sélectionne une carte, le jeton de sécurité résultant est inclus dans la réponse (POST) sous forme de valeur `xmlToken`. Les paramètres OBJECT d'Information Card sont utilisés pour encoder les informations WSSecurityPolicy requises dans le code HTML.

Dans cet exemple, la partie de confiance demande un jeton SAML 1.0 auprès d'un fournisseur d'identité délivré à titre autonome, en fournissant les réclamations requises `emailaddress`, `givenname` et `surname`.

Remarque : Vous pouvez omettre l'émetteur afin d'indiquer que *n'importe quel* émetteur Information Card disponible dans le navigateur de l'utilisateur est acceptable.

Syntaxe XHTML

La syntaxe XHTML est la suivante :

```
<html xmlns="http://www.w3.org/1999/xhtml" xmlns:ic>
<head>
<title>Welcome to Fabrikam</title>
</head>
<body>
<img src='fabrikam.jpg'/>
<form name="ctl00" id="ctl00" method="post"
action="https://www.fabrikam.com/InfoCard-Browser/Main.aspx">
<ic:informationCard name='xmlToken'
style='behavior:url(#default#informationCard)'
issuer="http://schemas.xmlsoap.org/ws/2005/05/identity/issuer/self"
tokenType="urn:oasis:names:tc:SAML:1.0:assertion">
<ic:add claimType=
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
optional="false" />
<ic:add claimType=
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"
optional="false" />
<ic:add claimType=
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname"
optional="false" />
</ic:informationCard>
<center>
<input type="submit" name="InfoCardSignin" value="Log in"
id="InfoCardSignin" />
</center>
</form>
</body>
</html>
```

Figure 20. Exemple de syntaxe XHTML InfoCard

Paramètres d'appel du sélecteur d'identité

Les paramètres contenus dans les objets Information Card OBJECT et XHTML servent à encoder les informations dans le code HTML. Dans les cas où un sélecteur d'identité est employé dans le contexte de services Web, ces informations sont fournies par une entité WS-WSSecurityPolicy via WSMetadataExchange.

La liste suivante indique les paramètres pris en charge par la norme Information Card pour l'appel du sélecteur d'identité.

Remarque : Tous les paramètres sont facultatifs. Aucun d'eux n'est obligatoire.

issuer Ce paramètre détermine l'adresse URL du service STS (Security Token Service) à partir duquel a lieu l'obtention d'un jeton. Lorsque ce paramètre est omis, aucun service STS spécifique n'est requis. La valeur spéciale `http://schemas.xmlsoap.org/ws/2005/05/identity/issuer/self` indique que le jeton doit provenir d'un fournisseur d'identité autonome.

Remarque : Ce paramètre n'est pas pris en charge par Tivoli Federated Identity Manager

issuerPolicy
Ce paramètre spécifie l'adresse URL d'un noeud final à partir duquel l'entité WS-SecurityPolicy peut être extraite via WS-MetadataExchange. S'il est omis, la valeur prise en compte est `<issuer>/mex`. Ce noeud final doit utiliser HTTPS.

Remarque : Ce paramètre n'est pas pris en charge par Tivoli Federated Identity Manager

tokenType
Ce paramètre spécifie le type du jeton demandé auprès du service STS, sous forme d'URI. Il est possible d'omettre ce paramètre lorsque le service STS et le point de contact du site Web sont préalablement convenus du type de jeton à fournir, ou encore si le site Web accepte *n'importe quel* type de jeton.

requiredClaims
Ce paramètre spécifie les types de réclamations qui doivent être fournis par l'identité. Si ce paramètre est omis, aucune réclamation n'est exigée. La valeur de `requiredClaims` est une liste d'URI délimitée par des espaces dont chaque entrée spécifie un type de réclamation requis.

optionalClaims
Ce paramètre spécifie les types de réclamations optionnelles qui peuvent être fournis par l'identité. Si ce paramètre est omis, il n'existe aucune réclamation optionnelle. La valeur de `optionalClaims` est une liste d'URI délimitée par des espaces dont chaque entrée spécifie un type de réclamation pouvant être soumis à titre facultatif.

privacyURL
Ce paramètre détermine l'adresse URL des règles de confidentialité lisibles par l'utilisateur et applicables au site, le cas échéant.

privacyVersion
Ce paramètre spécifie la version des règles de confidentialité. Il doit s'agir d'une valeur supérieure à 0 si un paramètre `privacyUrl` est spécifié. En cas de modification de cette valeur, l'utilisateur en est averti et est autorisé à consulter les modifications apportées aux règles de confidentialité.

Exemple de page de connexion WebSEAL

Voici un exemple de page WebSEAL login.html modifiée, dans laquelle les balises OBJECT sont indiquées en **gras**.

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML//EN">
<!-- Copyright (C) 2000 Tivoli Systems, Inc. -->
<!-- Copyright (C) 1999 IBM Corporation -->
<!-- Copyright (C) 1998 Dascom, Inc. -->
<!-- All Rights Reserved. -->
<HTML>
<HEAD>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<TITLE>Connexion Access Manager pour l'e-business</TITLE>
</HEAD>
<BODY BGCOLOR="#FFFFFF" TEXT="#000000">
<B>Connexion Access Manager pour l'e-business (www-default---2)</B>
<BR>
%ERROR%
<BR><BR>
<!--- DO NOT TRANSLATE OR MODIFY any part of the hidden parameter(s) --->

<!---
  The following block of code provides users with a warning message
  if they do not have cookies configured on their browsers.
  If this environment does not use cookies to maintain login sessions,
  simply remove or comment out the block below.
--->

<!--- BEGIN Cookie check block --->
<!---
<! ..... edited from this example for brevity ....
<!--- END Cookie check block --->

<BR>
   <form name="ctl00" id="ctl00" method="post"
        action="https://example.com:443/FIM/sps/infocard/login">
      <center>
          <input type="submit" name="InfoCardSignin" value="Log in"
          id="InfoCardSignin" />
      </center>
      <OBJECT type="application/x-informationCard" id="oCard" name="xmlToken">
        <PARAM Name="tokenType" Value="urn:oasis:names:tc:SAML:1.0:assertion">
        <PARAM Name="issuer" Value=
            "http://schemas.xmlsoap.org/ws/2005/05/identity/issuer/self">
        <PARAM Name="requiredClaims" Value=
"http://schemas.xmlsoap.org/ws/2005/05/identity/
   claims/privatepersonalidentifier">
        <PARAM Name="optionalClaims" Value=
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
">      </OBJECT>
    </form>
   </BODY>
</HTML>
```

Figure 21. Exemple de page de connexion WebSEAL avec des balises OBJECT

Configuration requise pour Information Card

Exigences relatives à WebSphere version 6.1

Tivoli Federated Identity Manager prend en charge Information Card sur WebSphere Application Server 6.1. Information Card n'est pas pris en charge sous WebSphere 6.0. Information Card repose sur l'algorithme de chiffrement

rsa-oaep-mgf1p pour la protection des clés. Cet algorithme est pris en charge par WebSphere 6.1, mais n'est pas disponible sous WebSphere 6.0.

Tivoli Federated Identity Manager nécessite l'application d'un groupe de correctifs pour WebSphere Application Server 6.1. Consultez les exigences relatives à la configuration logicielle et matérielle requise dans le centre de documentation de Tivoli Federated Identity Manager, en fonction du niveau du groupe de correctifs requis.

Mise à jour des règles de cryptographie pour Information Card

Les algorithmes de chiffrement employés par Information Card nécessitent un puissant support de bibliothèques cryptographiques. Ceci implique la nécessité de remplacer les fichiers de règles de sécurité Java par défaut, local_policy.jar et US_export_policy.jar.

Pourquoi et quand exécuter cette tâche

L'utilisation de la technologie de chiffrement est contrôlée par la législation des Etats-Unis. Les SDK IBM Java comprennent des fichiers de règles de juridiction strictes, mais limitées. Pour pouvoir déployer Information Card avec Tivoli Federated Identity Manager, vous devez vous procurer les fichiers de règles JCE (Java Cryptography Extension) de juridiction illimitée.

Pour consulter les informations de sécurité relatives aux kits de développement de logiciels IBM Java, accédez à l'adresse URL suivante :

`http://www.ibm.com/developerworks/java/jdk/security/index.html`

Pour vous procurer les fichiers de règles de juridiction illimitée, procédez comme suit :

Procédure

1. Mettez à jour WebSphere à l'aide de fichiers de règles JCE (Java Cryptography Extension) non limitées. Accès : http://www.ibm.com/developerworks/java/jdk/security/index.html
2. Sélectionnez le lien vers le SDK qui correspond à votre environnement, par exemple, pour Java 1.5, le SDK est J2SE 5.0. Une page affichant l'en-tête Security Information (informations de sécurité) apparaît.
3. Sélectionnez le lien suivant : **IBM SDK Policy Files**.

   Remarque : Lorsque vous cliquez sur ce lien, vous êtes redirigé vers le fichier de règles contenu dans le kit SDK compatible avec votre version de Java. Il est à noter, toutefois, que le numéro de version du kit SDK n'est pas nécessairement le même que celui de la version de Java utilisée. Par exemple, pour Java 1.5, vous pouvez être redirigé vers le kit SDK 1.4.
4. Le programme vous demande de vous connecter à l'aide de votre ID utilisateur et de votre mot de passe IBM. Si vous n'avez ni ID utilisateur, ni mot de passe IBM, vous devrez vous inscrire. Suivez le lien de la page de connexion relatif à l'inscription.
5. Connectez-vous au service de support IBM.
6. A l'invite, sélectionnez le fichier .zip correspondant à la version de Java que vous utilisez. Cliquez ensuite sur **Continuer** pour démarrer le téléchargement.
7. Décomprimez le fichier .zip. Les fichiers JAR sont les suivants :
   - local_policy.jar

- US_export_policy.jar

8. Placez les fichiers dans le répertoire suivant :
   rep_installation_composant_exec_Java/jre/lib/security

   Par exemple, il se peut que le composant d'exécution Java ait été installé dans le cadre de la version imbriquée de WebSphere Application Server. Dans ce cas, le répertoire peut être le suivant :
   /opt/IBM/FIM/*ewas*/java/jre/lib/security

Exigences liées à Information Card pour le service d'alias

Le service d'alias doit être configuré si des cartes gérées appuyées par une authentification sur la base de droits d'accès émis de façon autonome doivent être utilisées.

Clé de déchiffrement provenant d'un serveur point de contact

La configuration de la carte d'information nécessite la spécification d'une clé destinée au décryptage des messages au sein de la fédération. Le déchiffrement est un processus obligatoire.

Cela signifie qu'un alias de la clé de déchiffrement doit être ajouté dans le fichier de clés Tivoli Federated Identity Manager. La clé doit être la clé privée utilisée par le serveur point de contact. L'importation de cette clé doit être effectuée à l'aide du service de clés de Tivoli Federated Identity Manager.

Cela signifie qu'un alias de la clé de déchiffrement doit être ajouté dans le fichier de clés Tivoli Federated Identity Manager. La clé peut provenir de n'importe quel site Web qui présente au navigateur compatible Information la page HTML comportant les balises OBJECT requises. Le site peut être le serveur point de contact, mais cela n'est pas une condition obligatoire. L'adresse URL générée dans la page balisée doit *obligatoirement* utiliser le protocole SSL. Par exemple :
https://pointofcontact.example.com/FIM

La clé SSL utilisée pour l'adresse URL doit être importée dans un fichier de clés Tivoli Federated Identity Manager pour la partie de confiance.

Remarque : En cas de modification de la clé SSL ou de sa mise à jour pour les besoins du site Web ou du point de contact, l'administrateur doit également mettre à jour le fichier de clés Tivoli Federated Identity Manager en vue de prendre en compte la nouvelle clé SSL. Cette opération peut également impliquer des modifications de la configuration afin de mettre à jour l'alias du fichier de clés.

Exigences de synchronisation temporelle pour Information Card

Le succès d'un déploiement Information Card dépend de la synchronisation temporelle entre les systèmes. Les exigences suivantes doivent être satisfaites :

- Lorsque la méthode d'authentification UsernameToken est configurée pour une fédération, l'heure doit être synchronisée entre le fournisseur d'identité et les systèmes des parties de confiance.
- Lors de l'utilisation de la méthode d'authentification reposant sur des droits d'accès auto-générés pour l'obtention d'une carte gérée, le système du navigateur

(c'est-à-dire celui qui héberge le navigateur contenant les fonctionnalités Information Card) doit également être synchronisé temporellement.

- Lorsqu'une carte auto-générée est utilisée pour la connexion auprès de la partie de confiance, le système du navigateur (c'est-à-dire celui qui héberge le navigateur contenant les fonctionnalités Information Card) doit également être synchronisé temporellement.

La synchronisation temporelle requise peut être définie via la propriété **clock skew** pour chaque fédération Information Card. Pour modifier cette propriété à partir du panneau de propriétés du partenaire de fédération, vous pouvez utiliser la console d'administration de Tivoli Federated Identity Manager.

Mappage d'identité pour Information Card

Fournisseur d'identité

La prise en charge de Tivoli Federated Identity Manager pour les fournisseurs d'identité Information Card s'appuie sur une chaîne d'accréditation qui contient des modules destinés à accomplir des actions standard de validation, de mappage et d'envoi.

L'opération de validation est appliquée à un jeton d'authentification envoyé par le sélecteur d'identité afin de représenter l'utilisateur. Le jeton est soit un nom d'utilisateur, soit une assertion SAML. L'assertion SAML est employée lors de l'authentification sur la base de droits d'accès émis de façon autonome.

Le module de mappage peut être l'un des suivants :

- Module de mappage XSLT
- Module Tivoli Directory Integrator
- Module de mappage Java développé sur mesure

Tivoli Directory Integrator est généralement employé comme module de mappage associé à Information Card. Dans les déploiements Information Card, l'un des objectifs principaux de la chaîne d'accréditation est de permettre l'identification des valeurs d e réclamation et leur définition dans les données STSUU. Les valeurs des réclamations peuvent provenir de sources de données externes, telles qu'un registre LDAP. Le module Tivoli Directory Integrator peut, par exemple, convertir les entrées LDAP d'un utilisateur en valeurs de réclamations correspondantes, telles que définies dans le schéma spécifié par Microsoft.

Les modules Tivoli Directory Integrator peuvent également servir à combiner aisément des valeurs de réclamation issues de différentes sources. Certaines valeurs de réclamation peuvent par exemple provenir d'un registre LDAP, tandis que d'autres proviennent d'autres sources, telles que des bases de données, une source de code Java ou JavaScript, ou encore d'autres services Web.

La sortie du module de mappage est utilisée pour produire un jeton SAML 1.1 en mode *émission*.

Partie de confiance

La chaîne d'accréditation applicable pour une fédération de partie de confiance comprend :

- Un module de jeton SAML 1.1 en mode validation.

- Le module de mappage par défaut
- Le module de jeton IVCred en mode émission

L'assistant de fédération invite l'administrateur à spécifier les règles de mappage d'identité à l'aide de XSLT, suivant le déploiement. Les règles de mappage utilisent les attributs des assertions ou les informations contenues dans les réclamations afin de déterminer l'identité d'utilisation.

Les modules de jeton SAML créent les attributs STSUniversalUser destinés à chaque attribut de l'assertion SAML. Le nom, l'espace de nom et la valeur de chaque attribut SAML servent à définir le nom, le type et la valeur de STSUniversalUser.

Formulaire de configuration du fournisseur d'identité

Tivoli Federated Identity Manager comprend un assistant qui vous guidera tout au long de la configuration des fédérations Information Card. L'assistant vous invite à renseigner les propriétés nécessaires pour votre déploiement.

Ce formulaire décrit les invites. Ce formulaire vous permet de planifier vos propriétés et vous pouvez vous y référer lors de l'exécution de l'assistant.

Nom de la fédération
Chaîne arbitraire choisie pour dénommer cette fédération. Par exemple :
`infocard-idp`

Rôle de la fédération
Sélectionnez un fournisseur d'identité.

Nom de la société
L'assistant demande de spécifier les informations de contact. La zone Nom de la société est requise. Ce nom peut correspondre à n'importe quelle chaîne de caractères. Les autres zones sont facultatives.

Protocole de la fédération
Sélectionnez Information Card.

Serveur point de contact
Serveur qui agit en tant que point de contact initial pour les requêtes entrantes. Par exemple :
`https://pointofcontact.example.com/FIM`

Remarque : Pour le support d'Information Card, le serveur point de contact doit utiliser le protocole SSL (Secure Socket Layer). L'adresse URL spécifiée doit être du type `https://`.

Identificateur de clé de noeud final SSL

L'assistant de configuration vous invite à indiquer la clé à utiliser pour les opérations de déchiffrement dans la fédération. Il doit s'agir de la clé utilisée par le serveur point de contact pour les connexions SSL.

L'assistant vous demande cette clé dans le panneau **Paramètres de configuration Infocard**. Pour spécifier la clé, sélectionnez le fichier de clés, puis la clé.

Remarque : Vous devez importer cette clé du serveur point de contact vers le fichier de clés Tivoli Federated Identity Manager avant de configurer la fédération.

Fichier de clés
Fichier de clés Tivoli Federated Identity Manager contenant la clé

Par exemple : Tivoli Federated Identity Manager fournit un fichier de clés appelé DefaultKeystore.

Mot de passe du fichier de clés
Mot de passe requis pour accéder au fichier de clés spécifié.

Clé à sélectionner
L'assistant présente la liste des alias de clés (ou noms) stockés dans le fichier de clés. Vous devez sélectionner la clé à utiliser.

Option d'authentification

Vous devez choisir l'une des options d'authentification suivantes :

- Authentification avec une carte auto-émise
- Authentification avec un nom d'utilisateur et un mot de passe

L'option par défaut est l'authentification avec une carte auto-émise.

Le choix de l'option d'authentification détermine la valeur par défaut de la propriété **Fichier modèle de téléchargement de carte**.

Fichier modèle de téléchargement de carte
Il s'agit d'un fichier modèle HTML qui vous invite à saisir les paramètres requis pour émettre une carte d'information gérée. Des valeurs par défaut sont fournies par l'assistant de configuration. Vous pouvez appliquer les valeurs par défaut, sauf si vous avez modifié et renommé les fichiers modèle.

- Lorsque l'authentification avec une carte auto-émise est sélectionnée, la valeur par défaut est :

  `/infocard/getcard_sss.html`
- Lorsque l'authentification avec un nom d'utilisateur et un mot de passe est sélectionnée, la valeur par défaut est :

  `/infocard/getcard_ut.html`

Fichier modèle de carte d'information
Il s'agit d'un fichier modèle HTML contenant la carte d'information à vous renvoyer. fichier par défaut :

`/infocard/infocard_template.xml`

Fichier image de carte d'information
Fichier image à utiliser pour la carte d'information. Celui-ci doit se trouver dans le répertoire de l'environnement local en cours. La valeur par défaut est identique pour les deux options d'authentification. fichier par défaut :

`/infocard/fim_infocard.gif`

Expiration de la carte
cette propriété spécifie le nombre de jours de validité de la carte d'information à partir de la date d'émission. La valeur par défaut est identique pour les deux options d'authentification. Valeur par défaut :

`365`

Options de mappage d'identité
Vous devez sélectionner l'une des options suivantes :

- Utiliser XSL pour le mappage d'identité

  Sélectionnez cette option pour utiliser une règle de mappage XSLT. vous devez indiquer le nom d'un fichier contenant les règles de mappage d'identité. Tivoli Federated Identity Manager fournit un exemple de

fichier de règles de mappage d'identité destiné aux fédérations de fournisseurs d'identité Information Card :

/répertoire_installation/examples/ip_infocard.xsl

- Utiliser Tivoli Directory Integrator pour le mappage

  Sélectionnez cette option lorsque vous avez préalablement configuré une chaîne d'assemblage Tivoli Directory Integrator pour le mappage d'identité requis par votre fédération Information Card.

- Utiliser une instance de modèle de mappage personnalisé

  Sélectionnez cette option lorsque vous avez écrit et déployé un module de service d'accréditation personnalisé pour le mappage d'identité requis par votre fédération Information Card.

Tableau 97. Formulaire pour les propriétés d'une fédération de fournisseurs d'identité

Propriété	**Votre valeur**
Nom de la fédération	
Rôle	Fournisseur d'identité
Nom de l'entreprise	
Protocole de fédération	Carte d'information
Serveur point de contact	
Identificateur de clé de noeud final SSL : fichier de clés	
Identificateur de clé de noeud final SSL : mot de passe de fichier de clés	
Identificateur de clé de noeud final SSL : clé à sélectionner	
Option d'authentification	
Fichier modèle de téléchargement de carte	
Fichier modèle de carte d'information	
Fichier image de carte d'information	Valeur par défaut : /infocard/fim_infocard.gif
Expiration de la carte	Valeur par défaut : 365 jours
Options de mappage d'identité	Sélectionnez l'une des options suivantes : • Utiliser XSL pour le mappage d'identité • Utiliser Tivoli Directory Integrator pour le mappage • Utiliser une instance de modèle de mappage personnalisé
Fichier de règles de mappage d'identité	Si vous utilisez XSL pour le mappage d'identité, spécifiez le nom de fichier de règle de mappage suivant :
Module de mappage personnalisé	Si vous utilisez un module de mappage personnalisé, notez le nom du module :

Formulaire de configuration de la partie de confiance

Tivoli Federated Identity Manager comprend un assistant qui vous guidera tout au long de la configuration des fédérations Information Card. L'assistant vous invite à renseigner les propriétés nécessaires pour votre déploiement.

Ce formulaire décrit les invites. Ce formulaire vous permet de planifier vos propriétés et vous pouvez vous y référer lors de l'exécution de l'assistant.

Nom de la fédération
Chaîne arbitraire choisie pour dénommer cette fédération. Par exemple, `infocard-rp`.

Rôle de la fédération
Sélectionnez un fournisseur de services. Cette valeur est requise par la partie de confiance.

Nom de la société
L'assistant demande de spécifier les informations de contact. La zone Nom de la société est requise. Ce nom peut correspondre à n'importe quelle chaîne de caractères. Les autres zones sont facultatives.

Protocole de la fédération
Sélectionnez Information Card.

Serveur point de contact
Serveur qui agit en tant que point de contact initial pour les requêtes entrantes. Par exemple :

```
https://pointofcontact.example.com/FIM
```

Remarque : Pour le support d'Information Card, le serveur point de contact doit utiliser le protocole SSL (Secure Socket Layer). L'adresse URL spécifiée doit être du type `https://`.

Déchiffrement

L'assistant de configuration vous invite à indiquer la clé à utiliser pour les opérations de déchiffrement dans la fédération. Il doit s'agir de la clé utilisée par le serveur point de contact pour les connexions SSL.

L'assistant vous demande cette clé dans le panneau **Déchiffrement**. Pour spécifier la clé, sélectionnez le fichier de clés, puis la clé.

Remarque : Vous devez importer cette clé du serveur point de contact vers le fichier de clés Tivoli Federated Identity Manager avant de configurer la fédération.

Fichier de clés
Fichier de clés Tivoli Federated Identity Manager contenant la clé

Par exemple : Tivoli Federated Identity Manager fournit un fichier de clés appelé DefaultKeystore.

Mot de passe du fichier de clés
Mot de passe requis pour accéder au fichier de clés spécifié.

Clé à sélectionner
L'assistant présente la liste des alias de clés (ou noms) stockés dans le fichier de clés. Vous devez sélectionner la clé à utiliser.

Partenaire standard

L'assistant vous invite à sélectionner une option :

- Ajouter un partenaire pouvant gérer n'importe quel fournisseur d'identité

  Cette option est l'option par défaut.

  La sélection de cette option entraîne l'ajout automatique d'un partenaire. Cette configuration de partenaire peut accepter tout fournisseur d'identité pour les cartes d'information, y compris un fournisseur à émission automatique.
- Ajouter un partenaire pouvant gérer le fournisseur d'identité à émission automatique

  La sélection de cette option entraîne l'ajout automatique d'un partenaire. Ce partenaire Tivoli Federated Identity Manager accepte uniquement les cartes personnelles émises par le fournisseur à émission automatique intégré au navigateur.
- Ne pas ajouter de partenaire standard

  La sélection de cette option entraîne l'absence d'ajout de partenaires. L'administrateur doit ajouter explicitement des partenaires via l'assistant Ajout de partenaire de la console Tivoli Federated Identity Manager.

Options de mappage d'identité

Vous devez sélectionner l'une des options suivantes :

- Utiliser XSL pour le mappage d'identité

  Sélectionnez cette option pour utiliser une règle de mappage XSLT. vous devez indiquer le nom d'un fichier contenant les règles de mappage d'identité. Tivoli Federated Identity Manager fournit un exemple de fichier de règles de mappage d'identité destiné aux fédérations de fournisseurs d'identité Information Card :

  `/répertoire_installation/examples/rp_infocard.xsl`
- Utiliser Tivoli Directory Integrator pour le mappage

  Sélectionnez cette option lorsque vous avez préalablement configuré une chaîne d'assemblage Tivoli Directory Integrator pour le mappage d'identité requis par votre fédération Information Card.
- Utiliser une instance de modèle de mappage personnalisé

  Sélectionnez cette option lorsque vous avez écrit et déployé un module de service d'accréditation personnalisé pour le mappage d'identité requis par votre fédération Information Card.

Tableau 98. Formulaire pour les propriétés d'une fédération de parties de confiance

Propriété	**Votre valeur**
Nom de la fédération	
Rôle	Fournisseur de services
Nom de l'entreprise	
Protocole de fédération	Carte d'information
Serveur point de contact	
Déchiffrement : fichier de clés	
Déchiffrement : mot de passe du fichier de clés	
Déchiffrement : clé à sélectionner	

Tableau 98. Formulaire pour les propriétés d'une fédération de parties de confiance (suite)

Propriété	Votre valeur
Partenaire standard	Option par défaut : **Ajouter un partenaire pouvant gérer n'importe quel fournisseur d'identité.** Votre option :
Options de mappage d'identité	Sélectionnez l'une des options suivantes : • Utiliser XSL pour le mappage d'identité • Utiliser Tivoli Directory Integrator pour le mappage • Utiliser une instance de modèle de mappage personnalisé
Fichier de règles de mappage d'identité	Si vous utilisez XSL pour le mappage d'identité, spécifiez le nom de fichier de règle de mappage suivant :
Module de mappage personnalisé	Si vous utilisez un module de mappage personnalisé, notez le nom du module :

Formulaire de partenaire géré

Lors de la création d'une fédération pour un fournisseur d'identité, un partenaire est créé automatiquement.

Après avoir créé une fédération pour une partie de confiance, vous pouvez choisir l'une des nombreuses options de configuration d'un partenaire. Lorsque vous choisissez de ne pas ajouter de partenaire standard, vous pouvez créer un partenaire pour la fédération ultérieurement. Lorsque vous procédez de la sorte, vous devez fournir certaines valeurs de configuration.

La console de Tivoli Federated Identity Manager offre un assistant qui vous guidera tout au long de cette procédure.

Nom de la société du fournisseur d'identité
Informations de contact.

Emetteur de jeton de sécurité
Cette valeur sert à définir le paramètre protocolID et l'adresse URL du noeud final dans le fichier etc/feds.xml, ainsi que la zone Emetteur dans la configuration du mappage de chaîne STS. Par exemple :

```
https://example.com
```

Décalage d'horloge maximum autorisé entre les hôtes (en secondes)
Il s'agit de la valeur maximale d'écart d'horloge autorisée entre l'hôte de la partie de confiance et celui du fournisseur d'identité. La valeur de décalage d'horloge est utilisée durant la validation de la période de validité de l'assertion.

La valeur par défaut est de 60 secondes.

Valider des signatures sur les jetons de la carte d'information
Vous pouvez cocher cette case pour indiquer que les jetons de sécurité entrants doivent être signés. Lorsque vous sélectionnez cette option, vous devez, à l'aide des propriétés de configuration complémentaires, spécifier la clé publique qui sert à valider la signature numérique.

Type de clé de validation de signature
Vous devez sélectionner l'une des options suivantes :

- Clé publique fournie par le KeyInfo dans la signature du jeton de la carte d'information

  Vous pouvez choisir cette option si vous ne souhaitez pas distribuer ni mettre à jour la clé publique et que vous avez seulement besoin de vous assurer que l'intégrité du jeton est maintenue.
- Clé publique d'un fichier de clés

  Cette clé publique doit avoir été préalablement obtenue auprès du fournisseur de l'identité gérée, puis importée dans un fichier de clés Tivoli Federated Identity Manager à l'aide des services de clés.

Fichier de clés
Fichier de clés Tivoli Federated Identity Manager contenant la clé

Par exemple : Tivoli Federated Identity Manager fournit un fichier de clés appelé DefaultKeystore.

Mot de passe du fichier de clés
Mot de passe requis pour accéder au fichier de clés spécifié.

Clé à sélectionner
L'assistant présente la liste des alias de clés (ou noms) stockés dans le fichier de clés. Vous devez sélectionner la clé à utiliser.

Tableau 99. Formulaire des propriétés de configuration du partenaire géré

Propriété	Votre valeur
Nom de la société du fournisseur d'identité	
Emetteur de jeton de sécurité	
Décalage d'horloge maximum autorisé entre les hôtes (en secondes)	
Valider des signatures sur les jetons de la carte d'information	
Type de clé de validation de signature	En cas de validation de signatures, sélectionnez une option : • Clé publique fournie par le KeyInfo dans la signature du jeton de la carte d'information • Clé publique d'un fichier de clés
Fichier de clés	*Lors de l'utilisation d'une **clé publique provenant d'un fichier de clés*** :
Mot de passe du fichier de clés	
Clé à sélectionner	

Chapitre 19. Planification d'une fédération Information Card

Vérification des dépendances liées à Information Card

Avant de commencer

Avant d'utiliser l'assistant de création de fédération, assurez-vous que les conditions relatives aux dépendances Information Card sont satisfaites.

Procédure

1. Vérifiez que vous effectuez l'installation sur WebSphere Application Server 6.1 Les versions antérieures ne sont pas prises en charge. Voir «Exigences relatives à WebSphere version 6.1», à la page 254.
2. Vérifiez que vous possédez les bibliothèques de chiffrement correctes. Voir «Mise à jour des règles de cryptographie pour Information Card», à la page 255.
3. Déterminez su vous devez configurer le service d'alias. Voir «Exigences liées à Information Card pour le service d'alias», à la page 256.
4. Assurez-vous que vous avez importé la clé de chiffrement pour le serveur point de contact Cette clé doit être importée dans le service de clés de Tivoli Federated Identity Manager.

Planification d'une fédération Infocard

Utilisez l'assistant de fédération pour créer et configurer une fédération Infocard.

Avant de commencer

Assurez-vous que vous avez préparé les informations de configuration avant de créer la fédération au moyen de l'assistant. Les activités de planification sont décrites dans une série de rubriques du présent manuel. Voir Chapitre 2, «Présentation des tâches de configuration pour la connexion unique fédérée», à la page 15.

Pourquoi et quand exécuter cette tâche

Pour utiliser l'assistant de fédération afin de créer et configurer une fédération Infocard, procédez comme suit :

Procédure

1. Connectez-vous à Integrated Solutions Console et cliquez sur **Tivoli Federated Identity Manager → Configurer la connexion unique fédérée → Fédérations**. Les portlets IBM Domaines en cours et Fédérations apparaissent. Le portlet Fédérations affiche plusieurs boutons d'action.
2. Cliquez sur **Créer**. L'assistant de fédération démarre. L'assistant affiche une série de panneaux de configuration.
3. Utilisez votre formulaire complété afin d'indiquer des valeurs dans chaque panneau. Indiquez les valeurs nécessaires et cliquez sur **Suivant** pour poursuivre sur le panneau suivant. Si vous avez besoin de revenir en arrière pour ajuster un paramètre de configuration, cliquez sur **Précédent**. Pour obtenir des informations sur des zones spécifiques, affichez l'aide en ligne.

a. La première série de panneaux vous demande d'indiquer les paramètres relatifs au nom, au rôle et serveur point de contact de la fédération.
b. Puis, le panneau de configuration Infocard vous invite à indiquer les valeurs requises pour un fournisseur d'identité ou une partie de confiance Infocard.
c. La dernière série de panneaux vous invite à indiquer les paramètres de configuration du mappage d'identité.

Lorsque vous avez terminé d'entrer les paramètres de configuration, le panneau Récapitulatif s'affiche.

4. Vérifiez que les paramètres de configuration sont corrects, puis cliquez sur **Terminer**. Le portlet Création de fédération terminée s'affiche.

Configuration de WebSEAL en tant que serveur point de contact pour une fédération Information Card

Si vous envisagez d'utiliser WebSEAL en tant que serveur point de contact, vous devez le configurer pour la fédération Information Card.

Avant de commencer

Le portlet Création de fédération terminée comporte un bouton qui vous permet d'obtenir un utilitaire de configuration.

Pourquoi et quand exécuter cette tâche

Vous devez obtenir l'utilitaire, puis l'exécuter. Procédez comme suit :

Procédure

1. Cliquez sur **Télécharger l'outil de configuration Tivoli Access Manager**.
2. Enregistrez l'outil de configuration sur le système de fichiers de l'ordinateur hébergeant le serveur WebSEAL.
3. Revenez à la console de gestion et cliquez sur **Terminé** pour revenir au panneau Fédérations.

   Remarque : La console de gestion vous offre la possibilité d'ajouter immédiatement un partenaire, mais pour cette configuration initiale de la fédération, nous commencerons par exécuter d'abord les autres tâches.
4. Démarrez l'outil de configuration depuis une ligne de commande. La syntaxe est la suivante :

   ```
   java -jar /rép_téléchargement/tfimcfg.jar -cfgfile webseald-nom_instance.conf
    -action tamconfig
   ```

   Vous aurez besoin de l'ID (par défaut : sec_master) et du mot de passe de l'utilisateur d'administration Tivoli Access Manager. L'utilitaire configure les noeuds finals sur le serveur WebSEAL, crée une jonction WebSEAL, relie les listes de contrôle d'accès adaptées et active les méthodes d'authentification adéquates.

Exemple

Par exemple, lorsque vous avez mis le fichier tfimcfg.jar dans le répertoire `/tmp` et que le nom de l'instance WebSEAL est `default`, la commande est la suivante :

```
java -jar /tmp/tfimcfg.jar -cfgfile webseald-default -action tamconfig
```

Pour plus d'informations, accédez à l'adresse suivante :

- Annexe A, «Référence de tfimcfg», à la page 533

Configuration de WebSphere en tant que serveur point de contact

Tivoli Federated Identity Manager est configuré par défaut pour utiliser Tivoli Access Manager WebSEAL en tant que serveur point de contact. Pour configurer WebSphere en tant que serveur point de contact, vous devez procéder à une modification de la configuration.

Procédure

1. Connectez-vous à la console d'administration.
2. Cliquez sur Tivoli Federated Identity Manager > Gestion de la configuration > Point de contact
3. Sélectionnez **WebSphere**
4. Cliquez sur **Activer**.

Résultats

Le serveur WebSphere est désormais configuré en tant que point de contact.

Spécification d'un index de personnes

Un index de personnes est une collection comprenant plusieurs séries d'attributs, accessible à un utilisateur ou à un fournisseur d'identité. L'utilisateur peut spécifier les attributs qui décrivent une personne. Un utilisateur peut par exemple avoir des données professionnelles telles que son adresse électronique et son numéro de téléphone professionnels, et des données personnels relatives à son domicile, comme son adresse électronique et son numéro de téléphone à titre privé. Ces données personnelles peuvent porter respectivement les noms *work* et *home*.

Lorsqu'un utilisateur télécharge une carte gérée, il peut souhaiter associer celle-ci à des données personnelles particulières afin que, lorsqu'un jeton de connexion unique est demandé pour la carte, le fournisseur d'identité soit en mesure de déterminer quels ensembles d'attributs personnels doivent être utilisés pour alimenter les valeurs du jeton.

L'utilisation des données personnelles est permise grâce à un paramètre optionnel de zone de formulaire appelé `userdata`. Ce paramètre peut être inclus dans les pages des modèles getcard_ut.html et getcard_sss.html.

Bien que n'étant pas incluse dans les fichiers modèles fournis, cette zone d'entrée est néanmoins prise en charge.

Lorsque ce paramètre est spécifié, une macro de remplacement appelée @USERDATA@ peut être alimentée dans le fichier infocard_template.html. La macro @USERDATA@ est utilisée dans la section CardId du fichier infocard_template.html.

Le fichier infocard_template.html par défaut contient le modèle de macro suivant pour la section CardId :

```
<InformationCardReference>
  <CardId>@IPSTS@/@UUID@</CardId>
  <CardVersion>1</CardVersion>
</InformationCardReference>
```

Lorsque les administrateurs souhaitent utiliser la macro @USERDATA@, il leur est suggéré d'utiliser le modèle de macro suivant :

```
<InformationCardReference>
  <CardId>@IPSTS@/@UUID@/@USERDATA@</CardId>
  <CardVersion>1</CardVersion>
</InformationCardReference>
```

Les informations CardId font partie des données RST envoyées à Tivoli Federated Identity Manager par le sélecteur d'identité lors d'une demande de jeton de connexion unique. Ces informations permettent d'effectuer le mappage des règles visant à lire et différencier les données personnelles à utiliser.

Si ce modèle est appliqué, un utilisateur est invité à spécifier son index de données personnelles lors du téléchargement d'une carte gérée, et la carte est liée à un individu donné. Un utilisateur a la possibilité de télécharger différentes cartes pour chacun des ensembles de données personnelles qu'il a spécifiés auprès du fournisseur d'identité. La règle de mappage contenue dans la chaîne d'accréditation STS peut lire les données CardID (ainsi que, par là même, l'index des données personnelles) et spécifier, dans le jeton d'identité d'exécution, les attributs provenant des données personnelles valides.

Chapitre 20. Références pour Information Card

Macros de remplacement dans le fichier XML infocard_template

Les macros de remplacement pour le fichier infocard_template.xml sont les suivantes :

@IPSTS@
Adresse URL désignant le noeud final du fournisseur d'identité pour la fédération.

@IPMEX@
Adresse URL désignant le noeud final d'échange des métadonnées du fournisseur d'identité pour la carte gérée. Il est à noter que l'adresse URL est spécifique au type d'authentification utilisé.

@UUID@
Cette macro est remplacée par un UUID (identifiant d'utilisateur) généré de façon aléatoire. cette valeur permet de garantir que l'identité de la carte est unique.

@USERDATA@
cette macro n'est pas incluse dans le fichier par défaut. Vous pouvez l'ajouter au conteneur CardId lorsque vous souhaitez spécifier des attributs. Cette macro est utile lorsque des utilisateurs membres de votre déploiement ont de multiples identités. Les utilisateurs peuvent fournir des attributs destinés à identifier la personne à prendre en compte.

@CARDNAME@
Nom de la carte tel que spécifié par l'utilisateur dans l'envoi de réponse via le formulaire getcard_ut.html ou getcard_sss.html.

@CARDIMAGE@
Fichier image MIME (Multi-purpose Internet Email Extension) encodé qui est proposé à l'utilisateur par le sélecteur d'identité. Il existe un fichier image pour chaque fédération.

@ISSUETIME@
Heure d'émission de la carte. Le calcul de l'heure a lieu au moment de l'exécution.

@EXPIRETIME@
Heure d'expiration de la carte. L'heure est calculée en additionnant l'heure d'émission et la valeur de *lifetime* de la carte.

@IPCERTIFICATE@
Certificat public encodé en base 64 qui est configuré pour la fédération. Il convient qu'il s'agisse également du certificat public du noeud final SSL pour le serveur point de contact.

@USERCRED@
Bloc de métadonnées relatives aux droits d'accès utilisés par le sélecteur d'identité pour authentifier l'utilisateur auprès du noeud final du fournisseur d'identité (service STS). Les métadonnées proviennent d'un autre fichier modèle, suivant le type d'authentification en vigueur.

La prise en charge d'Information Card par Tivoli Federated Identity Manager s'applique à deux formes d'authentification :

- Jeton de nom d'utilisateur

  Les métadonnées correspondant aux données d'identification de l'utilisateur sont chargées à partir du fichier modèle inforcard_usercred_usernametoken.xml.

- Droits d'accès auto-émis

  Les métadonnées correspondant aux données d'identification de l'utilisateur sont chargées à partir du fichier modèle infocard_usercred_selfsignedsaml.xml.

@SUPPORTED_TOKENS@
La prise en charge d'Information Card par Tivoli Federated Identity Manager s'applique uniquement au type de jeton SAML 1.1. Deux représentations par défaut sont disponibles.

@SUPPORTED_CLAIMS@
Ensemble des réclamations prises en charge par cette carte. Ces valeurs sont héritées du formulaire envoyé par l'utilisateur dans le fichier getcard_*.html. Les valeurs doivent être présentées selon le format XML imposé par les spécifications Information Card.

Réclamations Information Card

La liste suivante indique les différents types de réclamations, en mentionnant l'URI et la description de chacun d'eux. Les types de réclamations sont récapitulés ici pour des raisons pratiques, mais il convient que les utilisateurs consultent la liste officielle dans le schéma référencé.

Remarque : La prise en charge d'Information Card dans Tivoli Federated Identity Manager ne se limite pas à cette série de réclamations.

Prénom
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname

Nom ou prénom préférentiel d'un individu. La spécification RFC 2256 indique que l'attribut `givenName` sert à contenir la partie du nom d'un individu qui ne correspond ni à son nom de famille, ni à son deuxième prénom.

Nom de famille
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname

Nom de famille d'un individu. La spécification RFC 2256 utilise `sn` et indique qu'il s'agit de l'attribut de nom X.500 contenant le nom de famille d'un individu.

Adresse électronique
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Adresse préférentielle indiquée pour la zone d'adresse électronique `To:` servant à l'envoi à destination du sujet, généralement spécifiée sous la forme `<utilisateur>@<domaine>`.

Le terme `mail` est utilisé par inetOrgPerson dans la spécification RFC1274, qui indique que ce type d'attribut spécifie un attribut d'adresse de messagerie électronique selon la syntaxe définie dans la spécification RFC 822.

Adresse
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddress

Composant concernant l'adresse postale dans les informations d'adresse du sujet.

La spécification RFC 2256 utilise le terme `street` et indique que cet attribut contient l'adresse physique de l'objet auquel l'entrée correspond, telle qu'une adresse de livraison. Son contenu est arbitraire, mais se présente généralement sous la forme d'une boîte postale ou d'un numéro d'appartement ou de maison suivi d'un nom de rue. Exemple : 303 rue des Jonquilles.

Nom de localité ou ville
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/locality

Composant concernant la localité dans les informations d'adresse du sujet. La spécification RFC 2256 utilise le terme `l` et indique que cet attribut contient le nom de la localité, par exemple une ville, un pays ou une autre région géographique. Exemple : Marseille.

Etat ou province
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince

Abréviation désignant le nom de l'état ou de la province dans les informations d'adresse du sujet. La spécification RFC 2256 utilise le terme `st` et indique que cet attribut contient le nom l'état ou de la province. Il convient d'harmoniser les valeurs à l'échelle nationale et, si des abréviations connues existent comme c'est le cas pour les abréviations à deux lettres est Etats américains, il convient de les privilégier par rapport aux noms entiers.

L'abréviation `TX`, par exemple, est utilisée pour désigner l'Etat du Texas.

Code postal
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcode

Composant concernant le code postal dans les informations d'adresse du sujet. La spécification X.500 (2001) emploie le terme `postalCode` et indique que le type d'attribut du code postal spécifie le code postal de l'objet nommé. Si cette valeur d'attribut est présente, elle fait partie de l'adresse postale de objet, c'est-à-dire le code postal aux Etats-Unis ou dans d'autres pays.

Pays http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country

Pays de résidence d'un sujet. La spécification RFC 2256 utilise le terme `c` et indique que cet attribut contient le code de pays à deux chiffres ISO 3166.

Numéro de téléphone
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/homephone

Numéro de téléphone principal ou secondaire d'un individu. Le terme `homePhone` est employé pour inetOrgPerson dans la spécification RFC 1274, qui indique que ce type d'attribut sert à spécifier le numéro de téléphone d'un domicile rattaché à une personne.

Il convient que les valeurs d'attribut respectent le format en vigueur pour les numéros téléphoniques internationaux. Exemple : +99 99 999 9999.

Numéro de téléphone secondaire ou de travail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone

Numéro de téléphone secondaire ou du lieu de travail d'un individu. La spécification X.500 (2001) emploie le terme `telephoneNumber` et indique que ce type d'attribut spécifie un numéro téléphonique professionnel ou scolaire associé à une personne.

Il convient que les valeurs d'attribut respectent le format en vigueur pour les numéros téléphoniques internationaux. Exemple : +99 99 999 9999.

Numéro de téléphone mobile
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone

Numéro de téléphone mobile d'un individu. Le terme `mobile` est employé pour inetOrgPerson dans la spécification RFC 1274, qui indique que ce type d'attribut sert à spécifier le numéro de téléphone mobile rattaché à une personne.

Il convient que les valeurs d'attribut respectent le format en vigueur pour les numéros téléphoniques internationaux. Exemple : +99 99 999 9999.

Date de naissance
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirth

Date de naissance d'un sujet, suivant le format autorisé par le type de données `xs:date`.

Sexe http://schemas.xmlsoap.org/ws/2005/05/identity/claims/gender

Sexe d'un individu. La valeur doit être l'une des chaînes suivantes :

0 Non spécifié

1 Homme

2 Femme

L'utilisation de ces valeurs rend les paramètres indépendants de la langue.

Identificateur personnel privé
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier

Identificateur de type PPID (Private Personal Identifier) qui identifie le sujet auprès d'une partie de confiance. Le terme **privé** signifie ici que l'identificateur du sujet est spécifique par rapport à une partie de confiance donnée et qu'il n'est par conséquent connu que de celle-ci (d'où le terme *privé*). Le PPID d'un individu auprès d'une partie de confiance unique ne peut être corrélé à celui du même individu auprès d'une autre partie de confiance.

Page Web
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/webpage

Page Web d'un individu exprimée sous forme d'adresse URL.

Propriétés de fédération pour les fournisseurs d'identité

Lorsque vous créez une fédération Information Card pour un fournisseur d'identité, l'assistant de configuration assigne automatiquement les valeurs par défaut à certaines propriétés. Il n'est pas possible de modifier ces propriétés durant la configuration initiale, mais vous pouvez les modifier une fois que celle-ci est terminée.

Identification de la fédération

Nom de la fédération
Chaîne arbitraire choisie pour dénommer cette fédération.

Par exemple, pour un fournisseur d'identité géré :

```
infocard-idp
```

Nom de la société
L'assistant demande de spécifier les informations de contact. Il s'agit de la seule zone obligatoire. Ce nom peut correspondre à n'importe quelle chaîne de caractères.

Propriétés de connexion unique

ID fournisseur
Identificateur unique permettant au fournisseur de se faire reconnaître par le fournisseur de services. Cette valeur est constituée du protocole et du nom d'hôte de l'URL du fournisseur d'identité. Elle peut également contenir un numéro de port. Par exemple, pour une fédération nommée infocard_fed :

```
https://idp.example.com/sps/infocard_fed/infocard
```

Noeud final de téléchargement de la carte
Noeud final permettant de créer et de télécharger une carte gérée. L'extension du fichier doit être .crd. La valeur par défaut est :

ID_fournisseur/getCard.crd

Noeud final d'échange de métadonnées
Noeud final utilisé par les sélecteurs d'identité pour demander les métadonnées relatives au service de jeton de sécurité (STS) du fournisseur d'identité. La valeur par défaut est :

ID_fournisseur/mex

Noeud final du service de jeton de sécurité
Noeud final utilisé par les sélecteurs d'identité pour demander les jetons de sécurité dans le cadre d'une authentification de carte d'information. La valeur par défaut est :

ID_fournisseur/sts

Noeud final de gestion d'alias
Noeud final utilisé pour gérer l'association, ou le lien, entre une carte auto-émise et le compte Tivoli Federated Identity Manager d'un utilisateur. Le lien est établi lorsque l'utilisateur télécharge une carte gérée au moyen de la méthode d'authentification "carte auto-émise" et ce noeud final peut être utilisé pour vérifier ou supprimer ce lien. La valeur par défaut est :

ID_fournisseur/alias

Cette propriété n'est pas utilisée si vous avez sélectionné l'option d'authentification par nom d'utilisateur et mot de passe.

Option d'authentification

Vous pouvez changer l'option d'authentification et choisir l'une des possibilités suivantes :

- Authentification avec une carte auto-émise
- Authentification avec un nom d'utilisateur et un mot de passe

Fichier modèle de téléchargement de carte
Il s'agit d'un fichier modèle HTML qui invite l'utilisateur à saisir les paramètres requis pour émettre une carte d'information gérée.

- Lorsque l'authentification avec une carte auto-émise est sélectionnée, la valeur par défaut est :

  `/infocard/getcard_sss.html`
- Lorsque l'authentification avec un nom d'utilisateur et un mot de passe est sélectionnée, la valeur par défaut est :

  `/infocard/getcard_ut.html`

Fichier modèle de carte d'information
Il s'agit d'un fichier modèle HTML contenant la carte d'information à vous renvoyer. fichier par défaut :

`/infocard/infocard_template.xml`

La valeur par défaut est identique pour les deux options d'authentification.

Fichier image de carte d'information
Fichier image à utiliser pour la carte d'information. Celui-ci doit se trouver dans le répertoire de l'environnement local en cours. La valeur par défaut est identique pour les deux options d'authentification. fichier par défaut :

`/infocard/fim_infocard.gif`

La valeur par défaut est identique pour les deux options d'authentification.

Modèle de carte de métadonnées
Nom du fichier à utiliser comme modèle pour les métadonnées de la carte d'information. Le fichier par défaut est :

`/infocard/metadata_template.xml.`

Règles des métadonnées de droits d'accès SAML d'auto-signature
Nom du fichier de règles à utiliser pour les métadonnées de droits d'accès SAML d'auto-signature. Le fichier par défaut est :

`/infocard/metadata_policy_selfsignedsaml.xml`

Cette zone s'affiche si vous avez sélectionné **Authentification avec une carte auto-émise**.

Règles des métadonnées de droits d'accès du nom d'utilisateur
Nom du fichier de règles à utiliser pour les métadonnées de droits d'accès de l'utilisateur. Le fichier par défaut est :

`/infocard/metadata_policy_usernametoken.xml`

Cette zone s'affiche si vous avez sélectionné **Authentification avec un nom d'utilisateur et un mot de passe**.

Expiration de la carte
cette propriété spécifie le nombre de jours de validité de la carte d'information à partir de la date d'émission. La valeur par défaut est identique pour les deux options d'authentification. Valeur par défaut :

`365`

Identificateur de clé de noeud final SSL

Remarque : Il s'agit de la clé que devez importer depuis le serveur point de contact vers le fichier de clés Tivoli Federated Identity Manager avant de configurer les fédérations.

Fichier de clés
Fichier de clés Tivoli Federated Identity Manager contenant la clé

Par exemple : Tivoli Federated Identity Manager fournit un fichier de clés appelé DefaultKeystore.

Mot de passe du fichier de clés
Mot de passe requis pour accéder au fichier de clés spécifié.

Liste des clés
L'assistant présente la liste des alias de clés (ou noms) stockés dans le fichier de clés. Vous devez sélectionner la clé à utiliser.

Identificateur de la clé de signature Information Card

Paire de clés publique/privée utilisée par les cartes d'information récemment émises.

Fichier de clés
Fichier de clés Tivoli Federated Identity Manager contenant la clé

Par exemple : Tivoli Federated Identity Manager fournit un fichier de clés appelé DefaultKeystore.

Mot de passe du fichier de clés
Mot de passe requis pour accéder au fichier de clés spécifié.

Liste des clés
L'assistant présente la liste des alias de clés (ou noms) stockés dans le fichier de clés. Vous devez sélectionner la clé à utiliser.

Propriétés du module de jeton

Lors de la configuration initiale de la fédération Information Card, la chaîne d'accréditation est générée et configurée automatiquement. La chaîne d'accréditation contient les modules d'accréditation qui nécessitent une configuration. Les propriétés de cette section peuvent être modifiées.

Activer l'utilisation unique des assertions
Utiliser l'assertion une seule fois et ne pas la mettre en mémoire cache pour l'utiliser ultérieurement. Cette option est activée par défaut.

Cette propriété est utilisée uniquement avec l'authentification par carte auto-émise.

Sauter la validation du mot de passe
Ne pas effectuer la validation du mot de passe pour le jeton Username. L'option par défaut est désélectionnée, ce qui signifie que la validation du mot de passe a lieu.

Cette propriété est utilisée uniquement avec l'authentification par nom d'utilisateur et mot de passe.

Durée de validité (en secondes) d'une assertion avant sa date d'émission
Valeur par défaut : 60 secondes Aucune valeur minimale ou maximale n'est appliquée.

Durée de validité (en secondes) de l'assertion après émission.
Valeur par défaut : 60 secondes Aucune valeur minimale ou maximale n'est appliquée.

Propriétés de mappage d'identité

Les propriétés de mappage d'identité sont identiques pour tous les protocoles pris en charge par Tivoli Federated Identity Manager.

Instance du module de mappage d'identité
Cette valeur correspond à votre choix lors de la configuration initiale.

Modifier l'instance du module de mappage d'identité
Appelle le panneau Options de mappage d'identité. Le panneau Options de mappage d'identité permet de sélectionner une transformation XSL, Tivoli Directory Integrator, ou une instance de module de mappage.

Modification des propriétés en cours
Appelle un autre panneau permettant de modifier des propriétés :

- Si la fédération utilise une transformation XSL, ce bouton appelle le panneau Règle de mappage d'identité. Ce panneau permet de modifier ou de supprimer la règle de mappage d'identité.
- Si la fédération utilise un module de mappage personnalisé, ce bouton appelle un panneau permettant d'afficher ou de modifier les propriétés d'instance de mappage personnalisé.

Propriétés de fédération pour les parties de confiance

Identification de la fédération

Nom de la fédération
Chaîne arbitraire choisie pour dénommer cette fédération.

Par exemple, pour un fournisseur de confiance :

```
infocard-rp
```

Nom de la société
L'assistant demande de spécifier les informations de contact. Il s'agit de la seule zone obligatoire. Ce nom peut correspondre à n'importe quelle chaîne de caractères.

Propriétés de connexion unique

ID fournisseur
Identificateur unique permettant au fournisseur de se faire reconnaître par le fournisseur de services. Cette valeur est constituée du protocole et du nom d'hôte de l'URL du fournisseur d'identité. Elle peut également contenir un numéro de port. Par exemple, pour une fédération nommée infocard_fed :

```
https://rp.example.com/sps/infocard_fed/infocard
```

URL d'authentification
URL à laquelle l'utilisateur envoie les demandes d'authentification. Cette valeur ne peut pas être modifiée sur le panneau Propriétés. Par exemple, pour une fédération nommée infocard_fed, l'URL d'authentification serait :

```
https://idp.example.com/sps/infocard_fed/infocard/login
```

Propriétés de la clé de déchiffrement

Clé à utiliser pour déchiffrer les jetons entrants. Il est à noter que celle-ci doit être identique à la clé utilisée pour SSL par le point de contact (par exemple, WebSEAL).

Fichier de clés
Fichier de clés Tivoli Federated Identity Manager contenant la clé

Par exemple : Tivoli Federated Identity Manager fournit un fichier de clés appelé DefaultKeystore.

Mot de passe du fichier de clés
Mot de passe requis pour accéder au fichier de clés spécifié.

Liste des clés
L'assistant présente la liste des alias de clés (ou noms) stockés dans le fichier de clés. Vous devez sélectionner la clé à utiliser.

Propriétés de mappage d'identité

Les propriétés de mappage d'identité sont identiques pour tous les protocoles pris en charge par Tivoli Federated Identity Manager.

Instance du module de mappage d'identité
Cette valeur correspond à votre choix lors de la configuration initiale.

Modifier l'instance du module de mappage d'identité
Appelle le panneau Options de mappage d'identité. Le panneau Options de mappage d'identité permet de sélectionner une transformation XSL, Tivoli Directory Integrator, ou une instance de module de mappage.

Modification des propriétés en cours
Appelle un autre panneau permettant de modifier des propriétés :

- Si la fédération utilise une transformation XSL, ce bouton appelle le panneau Règle de mappage d'identité. Ce panneau permet de modifier ou de supprimer la règle de mappage d'identité.
- Si la fédération utilise un module de mappage personnalisé, ce bouton appelle un panneau permettant d'afficher ou de modifier les propriétés d'instance de mappage personnalisé.

Caractéristiques des partenaires des fournisseurs d'identité dans les fédérations de parties de confiance

Identification de la fédération

Nom du membre de la fédération
Fédération à laquelle ce partenaire a été ajouté. Vous ne pouvez pas modifier cette propriété.

Exemple : le fournisseur d'identité est dorénavant un partenaire de la fédération de fournisseurs de confiance :

```
infocard-rp
```

Rôle du partenaire
Fournisseur d'identité. Vous ne pouvez pas modifier cette propriété.

Etat La fenêtre des propriétés du partenaire permet de savoir si un partenaire est activé ou désactivé. Les partenaires doivent être activés pour pouvoir participer à une fédération.

- Si l'état d'un partenaire est désactivé, cliquez sur Activer pour activer ce partenaire.
- Si l'état du partenaire est activé, cliquez sur Désactiver pour le désactiver.

Nom de la société du fournisseur d'identité
Nom de la société du partenaire. Ce nom peut correspondre à n'importe quelle chaîne de caractères. Vous pouvez utiliser des espaces. Cette zone est obligatoire.

Adresse URL de la société
URL de la société du partenaire. Cette zone est facultative. Par exemple :

```
http://www.example.com
```

Personne à contacter
Informations de contact optionnelles pour l'administrateur. Vous pouvez également utiliser la zone Autres informations si nécessaire.

Propriétés des jetons

Emetteur de jeton de sécurité
Spécifiez l'URI (Uniform Resource Identifier) de l'émetteur unique du fournisseur d'identité. Cette valeur doit être utilisée dans l'élément saml:Issuer de saml:Assertion. Voici un exemple :

```
https://example.com
```

Vous pouvez entrer une astérisque (*) pour indiquer qu'un fournisseur d'identité est acceptable.

Décalage d'horloge maximum autorisé entre les hôtes (en secondes)
Spécifiez une valeur entière qui indique le décalage d'horloge maximum autorisé, en secondes, entre l'hôte de la partie de confiance et l'hôte du fournisseur d'identité. Vous devez spécifier une valeur minimale de zéro secondes dans cette zone. La valeur par défaut est 60. Cette zone s'affiche uniquement si la fédération utilise l'option Authentification avec une carte auto-émise.

Propriétés de la clé de validation de signature

Valider des signatures sur les jetons Infocard
Lorsque cette option est sélectionnée, cela indique que vous devez signer les jetons de la carte d'information puis indiquer le type de clé publique à utiliser pour valider la signature numérique. Décochez cette case pour désactiver la validation de signature. Cette case est cochée par défaut.

Type de clé de validation de signature

- **Clé publique fournie par le KeyInfo dans la signature du jeton de la carte d'information**

  Choisissez d'utiliser la clé publique fournie par le KeyInfo dans la signature du jeton de la carte d'information. Il s'agit de la sélection par défaut.

- **Clé publique d'un fichier de clés**

  Sélectionnez une clé publique dans un fichier de clés. Lorsque vous sélectionnez cette option, vous devez sélectionner le fichier de clés et la clé.

Fichier de clés
Fichier de clés Tivoli Federated Identity Manager contenant la clé

Par exemple : Tivoli Federated Identity Manager fournit un fichier de clés appelé DefaultKeystore.

Mot de passe du fichier de clés
Mot de passe requis pour accéder au fichier de clés spécifié.

Liste des clés
L'assistant présente la liste des alias de clés (ou noms) stockés dans le fichier de clés. Vous devez sélectionner la clé à utiliser.

Propriétés de mappage d'identité

Les propriétés de mappage d'identité sont identiques pour tous les protocoles pris en charge par Tivoli Federated Identity Manager.

Instance du module de mappage d'identité
Cette valeur correspond à votre choix lors de la configuration initiale.

Modifier l'instance du module de mappage d'identité
Appelle le panneau Options de mappage d'identité. Le panneau Options de mappage d'identité permet de sélectionner une transformation XSL, Tivoli Directory Integrator, ou une instance de module de mappage.

Modification des propriétés en cours
Appelle un autre panneau permettant de modifier des propriétés :

- Si la fédération utilise une transformation XSL, ce bouton appelle le panneau Règle de mappage d'identité. Ce panneau permet de modifier ou de supprimer la règle de mappage d'identité.
- Si la fédération utilise un module de mappage personnalisé, ce bouton appelle un panneau permettant d'afficher ou de modifier les propriétés d'instance de mappage personnalisé.

Caractéristiques des partenaires de confiance pour les fédérations de fournisseurs d'identité

Identification de la fédération

Nom du membre de la fédération
Fédération à laquelle ce partenaire a été ajouté. Vous ne pouvez pas modifier cette propriété.

Exemple : la partie de confiance est dorénavant un partenaire de la fédération de fournisseurs d'identité :

```
infocard-idp
```

Rôle du partenaire
Fournisseur de services (partie de confiance). Vous ne pouvez pas modifier cette propriété.

Etat La fenêtre des propriétés du partenaire permet de savoir si un partenaire est activé ou désactivé. Les partenaires doivent être activés pour pouvoir participer à une fédération. Cette propriété n'est pas modifiable, car elle s'applique à toutes les parties de confiance.

Nom de la société du fournisseur de services
Cette valeur indique que cette configuration partenaire est appliquée à tous les partenaires.

Par exemple, pour une fédération de fournisseurs d'identité dénommée infocard-idp, la valeur par défaut est :

```
toutes les parties de confiance de infocard-idp
```

Adresse URL de la société
URL de la société du partenaire. Cette zone est facultative. Par exemple :

```
http://www.example.com
```

Personne à contacter
Informations de contact optionnelles pour l'administrateur. Vous pouvez également utiliser la zone Autres informations si nécessaire.

Paramètres de configuration globale Infocard

Décalage d'horloge maximum autorisé entre les hôtes (en secondes)
Spécifiez une valeur entière qui indique le décalage d'horloge maximum autorisé, en secondes, entre l'hôte de la partie de confiance et l'hôte du fournisseur d'identité. Vous devez spécifier une valeur minimale de zéro secondes dans cette zone. La valeur par défaut est 60. Cette zone s'affiche uniquement si la fédération utilise l'option Authentification avec une carte auto-émise.

Sélectionner la clé de signature des assertions
Indiquez la clé à utiliser pour la signature des assertions SAML.

Fichier de clés
Fichier de clés Tivoli Federated Identity Manager contenant la clé

Par exemple : Tivoli Federated Identity Manager fournit un fichier de clés appelé DefaultKeystore.

Mot de passe du fichier de clés
Mot de passe requis pour accéder au fichier de clés spécifié.

Liste des clés
L'assistant présente la liste des alias de clés (ou noms) stockés dans le fichier de clés. Vous devez sélectionner la clé à utiliser.

Propriétés des jetons

Inclure les types d'attribut suivants
Indiquez les types d'attributs à inclure dans l'assertion. L'astérisque (*), qui est le paramètre par défaut, indique que tous les types d'attributs spécifiés dans le fichier de mappage personnalisé ou par le module de mappage personnalisé seront inclus dans l'assertion. Pour spécifier un ou plusieurs types d'attributs individuellement, tapez chaque type d'attribut dans la case. Utilisez && pour séparer plusieurs types d'attributs.

Inclure l'élément InclusiveNamespaces à la canonicalisation de l'assertion lors de la création de la signature
Sélectionnez cette option pour inclure l'élément InclusiveNamespaces à la canonicalisation de l'assertion lors de la création de la signature. Par défaut, cette option est désélectionnée.

Inclure les données de certificat X509 dans l'élément KeyInfo de la signature
Sélectionnez cette option pour utiliser les données de certificat X509 dans l'élément KeyInfo de la signature. Par défaut, cette option est sélectionnée.

Inclure les données de clé publique dans l'élément KeyInfo de la signature
Sélectionnez cette option pour utiliser les données de clé publique (clé publique RSA/DSA X509) dans l'élément KeyInfo de la signature. Par défaut, cette option est sélectionnée. L'élément KeyInfo contient des informations sur la clé nécessaires pour valider la signature.

Propriétés de mappage d'identité

Les propriétés de mappage d'identité sont identiques pour tous les protocoles pris en charge par Tivoli Federated Identity Manager.

Instance du module de mappage d'identité
Cette valeur correspond à votre choix lors de la configuration initiale.

Modifier l'instance du module de mappage d'identité
Appelle le panneau Options de mappage d'identité. Le panneau Options de mappage d'identité permet de sélectionner une transformation XSL, Tivoli Directory Integrator, ou une instance de module de mappage.

Modification des propriétés en cours
Appelle un autre panneau permettant de modifier des propriétés :

- Si la fédération utilise une transformation XSL, ce bouton appelle le panneau Règle de mappage d'identité. Ce panneau permet de modifier ou de supprimer la règle de mappage d'identité.
- Si la fédération utilise un module de mappage personnalisé, ce bouton appelle un panneau permettant d'afficher ou de modifier les propriétés d'instance de mappage personnalisé.

Chapitre 21. Présentation de la planification sous OpenID

Tivoli Federated Identity Manager prend en charge les connexions uniques via le protocole OpenID.

Cette présentation décrit l'implémentation sous Tivoli Federated Identity Manager d'OpenID. Les informations de la présentation permettent à un administrateur de déployer et configurer des fédérations de connexion unique.

Les spécifications OpenID font référence à une partie nommée *fournisseur OpenID ou fournisseur d'identité*, qui a pour rôle de certifier qu'un utilisateur possède une adresse URL d'identité particulière. Une partie de confiance ou un *consommateur* reçoit ces informations de la part du fournisseur d'identité. Sous Tivoli Federated Identity Manager, le terme de *fournisseur d'identité* correspond directement à la notion de *fournisseur OpenID ou fournisseur d'identité* d'OpenID. Le *consommateur* OpenID correspond bien au concept de fournisseur de service de Tivoli Federated Identity Manager.

La prise en charge par Tivoli Federated Identity Manager de l'authentification OpenID permet de définir tous les modes pour les messages OpenID :

associate
Mode permettant d'établir un secret partagé avec le consommateur

checkid_immediate
Mode permettant d'exécuter un contrôle non bloquant si un utilisateur détient l'URL de l'identificateur réclamé.

checkid_setup
Mode permettant d'exécuter un contrôle si un utilisateur détient l'URL de l'identificateur réclamé.Le contrôle peut, le cas échéant, inclure une interaction avec l'utilisateur.

check_authentication
Mode permettant de déterminer la validité d'une signature de message. Ce mode est généralement sélectionné pour les consommateurs muets ou dépourvus d'état.

Remarque : Pour obtenir une description complète des spécifications OpenID, consultez le site Web d'OpenID :

http://www.openid.net

Prise en charge d'OpenID 1.1 et 2.0

OpenID 1.1 et OpenID 2.0 sont tous les deux pris en charge.

Adresses URL d'ID OpenID

Une adresse URL d'identité OpenID est une identité numérique conçue pour authentifier les utilisateurs et leur accorder l'accès aux services.

URL d'identité avec un point de contact WebSEAL

Prenons les exemples suivants de valeurs pour créer une URL d'identité avec un point de contact WebSEAL :

- Une fédération de fournisseur d'identité appelée `openidfedip`
- Un serveur Tivoli Federated Identity Manager dont le serveur point de contact est WebSEAL et portant le nom d'hôte `webseal.example.com`.
- Une identité d'utilisateur (dans le cas présent, un utilisateur Tivoli Access Manager) intitulée `john`.

L'URL d'identité OpenID peut être n'importe quelle adresse URL répondant aux exigences suivantes :

- Pouvoir être résolue sur votre site Web. Dans notre exemple :
  - Lancez l'adresse `http(s)://webseal.example.com`
  - Ou bien, si vous utiliser des entrées de DNS génériques et un certificat de site pour `*.example.com`, il peut s'agir d'une valeur du type `http(s)://john.example.com`
- Il doit contenir un identificateur unique à l'utilisateur. En général, cet identificateur est votre identité d'utilisateur au niveau du fournisseur d'identité. Toutefois, il peut s'agir d'un alias généré pour des raisons de confidentialité.
- Elle doit correspondre à une expression régulière que vous avez configurée pour votre fédération de fournisseur d'identité OpenID.
- Le point final de fournisseur d'identité OpenID doit être reconnaissable à l'aide de la reconnaissance Yadis ou HTML à partir de votre URL d'identité tel que décrit dans les spécifications OpenID.

URL d'identité avec un point de contact WebSphere

Prenons les exemples de valeurs suivants pour créer l'URL d'identité avec un point de contact WebSphere :

- Une fédération de fournisseur d'identité appelée `openidfedip`
- Un serveur Tivoli Federated Identity Manager sur lequel le serveur de point de contact est WebSphere, avec le nom d'hôte `poc.example.com`
- Une identité d'utilisateur intitulée `john`

Le exigences qui s'appliquent à l'adresse URL sont les mêmes que dans le premier exemple. La figure 22 illustre un exemple de code lorsqu'un serveur de point de contact WebSphere est déployé et que la reconnaissance HTML est utilisée.

```
<html>
<head>
<link rel="openid.server"
href="https://poc.example.com/sps/openidfedip/openid/sso">
<link rel="openid2.provider"
href="https://poc.example.com/sps/openidfedip/openid/sso">
</head>
...
</html>
```

Figure 22. Exemple de code pour le renvoi d'un pointeur vers votre serveur OpenID à partir de votre URL d'identité à l'aide de la reconnaissance HTML

Remarque : Vous pouvez également utiliser la reconnaissance Yadis pour renvoyer un pointeur à votre serveur OpenID à partir de votre URL d'identité.

Exemple d'URL d'identité

Lorsque vous configurez une fédération pour OpenID, définissez une expression régulière pour les URL d'identité. Un moyen simple de vous assurer qu'un lien au noeud final de votre serveur OpenID est renvoyé par votre URL d'identité consiste à vérifier les points suivants :

1. Assurez-vous que la page d'URL d'identité est une page non protégée.
2. Intégrez le lien au serveur OpenID dans le formulaire de connexion du serveur point de contact.

   Le serveur point de contact est généralement une instance WebSEAL ou WebSphere.

La restriction imposée par cette méthode est qu'une seule fédération de fournisseur d'identité OpenID peut résider sur l'ordinateur. Cette restriction ne donne théoriquement lieu à aucun problème et correspond à un déploiement typique d'OpenID.

Exemples :

- Par exemple, lorsque l'expression régulière configurée est :

```
http://webseal.example.com/@ID@
```

un exemple d'URL d'identité est le suivant :

```
http://webseal.example.com/john
```

Cette méthode de configuration simple ne nécessite aucune interaction avec l'utilisateur pour pouvoir établir une URL d'identité. Tivoli Federated Identity Manager détermine si un utilisateur possède cette URL d'identité en :

1. Remplaçant la macro `@ID@` dans l'expression régulière configurée par le nom d'utilisateur de Tivoli Federated Identity Manager, et en
2. Vérifiant qu'une correspondance exacte existe avec l'URL d'identité réclamée par l'utilisateur dans la demande de connexion unique.

- Un autre exemple est celui dans lequel le déploiement :
  - Utilise un certificat de site avec `CN=*.example.com`
  - Utilise une entrée DNS générique correspondant à `*.example.com` pour un site protégé par WebSEAL.
  - Permet à l'utilisateur de détenir au choix des URL OpenID `http` ou `https`.

  Pour cet exemple, les URL d'identité suivantes sont valides :
  - `john.example.com`
  - `http://john.example.com`
  - `https://john.example.com`

  Remarque :
  - Lorsque le protocole n'est pas spécifié, comme dans le premier exemple, le protocole utilisé est HTTP.

    L'expression régulière configurée pour cette fédération inclut dans ce cas un nom d'hôte générique et une prise en charge multi-protocole. Par exemple :

    ```
    http[s]?://@ID@.example.com
    ```

    La macro `@ID@` est mappée à un nom d'utilisateur.

– Dans certains environnements d'application, l'utilisation d'une barre oblique de fin peut être souhaitée dans les modèles d'URL d'identité :

  ```
  webseal.example.com/john/
  ```

  Certaines applications ajoutent une barre oblique de fin (/) lors de la normalisation de l'entrée utilisateur. Une non concordance se produit lorsqu'une barre oblique de fin est ajoutée par l'application mais pas spécifiée pour l'URL d'identité. L'accès est refusé.

  Pour ces environnements, assurez-vous que l'expression régulière configurée inclut la barre oblique de fin. Par exemple :

  ```
  http://webseal.example.com/@ID@/
  ```

Générateur d'identificateur personnel privé

Dans certains scénarios d'authentification, vous pouvez conserver la confidentialité de l'utilisateur en masquant son identité à la partie de confiance. En outre, vous pouvez vouloir le même utilisateur pour vous connecter à deux parties de confiance différentes à l'aide d'identificateurs demandés. Le générateur d'identificateur personnel privé (PPID) crée l'identificateur. Les identités d'utilisateur de la partie de confiance n'entrent ainsi pas en collision car ils utilisent des identificateurs demandés différents.

Ce type de scénario d'authentification est appelé *identité dirigée*. L'identité dirigée exige que l'utilisateur lance la connexion au niveau de la partie de confiance à l'aide de l'identificateur de fournisseur d'identité. Par exemple `https://example.ibm.com`

Selon la configuration, le fournisseur OpenID génère un identificateur pour l'utilisateur d'une partie de confiance spécifique. Un générateur d'identificateur personnel privé (PPID) crée l'identificateur. Le fournisseur OpenID génère un identificateur distinct pour chaque partie de confiance à laquelle le même utilisateur s'authentifie. La création d'identificateurs demandés différents empêche le partage des informations entre les parties de confiance. Cette fonction protège également efficacement l'identité de l'utilisateur.

L'utilisation de la fonction PPIG implique que le fournisseur OpenID informe son serveur d'informations de noeud final à l'aide du document Extensible Resource Descriptor Sequence (XRDS). Le document XRDS est requis. Un utilisateur peut uniquement se connecter à une partie de confiance à l'aide d'un identificateur de fournisseur d'identité inclus au document XRDS. Le document XRDS représente le seul moyen, pour la partie de confiance, de distinguer l'identificateur demandé d'un utilisateur et l'identificateur du fournisseur d'identité.

Un plug-in fournit un générateur PPIG dans l'implémentation de fournisseur d'identité. Le plug-in fournit plusieurs implémentations de générateur standard. Un administrateur peut utiliser le plug-in pour écrire et intégrer un IDGenerator personnalisé. Cette fonction détermine comment générer l'identité d'un identificateur demandé pour un utilisateur particulier au niveau d'une partie de confiance donnée.

Lorsqu'un identificateur de fournisseur d'identité est utilisé au niveau de la partie de confiance pour lancer l'authentification, le fournisseur d'identité est responsable de la génération de l'identificateur demandé pour l'utilisateur. Tivoli Federated

Identity Manager génère un identificateur demandé à l'aide d'un simple modèle d'adresse URL configuré. L'adresse URL doit contenir la macro `@ID@`. La valeur de `@ID@` est générée par le générateur PPID.

Par exemple, la configuration par défaut est la suivante :

```
https://myidp.com/@ID@
```

Les valeurs IDGenerators suivantes peuvent être utilisées pour remplacer la macro `@ID@` de l'URL d'identité :

- Générateur d'ID de nom d'utilisateur
- Générateur d'ID de hachage
- Générateur d'ID de service d'alias

Générateur d'ID de nom d'utilisateur

Lorsque le générateur d'ID de nom d'utilisateur est utilisé, un nom d'utilisateur est renvoyé en portion `@ID@` de l'expression pour les URL d'identité.

Par exemple, lorsque l'expression d'URL d'identité est la suivante :

```
http://webseal.example.com/@ID@
```

un exemple d'URL d'identité est le suivant :

```
http://webseal.example.com/john
```

Ce paramètre représente le comportement par défaut de Tivoli Federated Identity Manager.

Générateur d'ID de hachage

Le générateur d'ID de hachage remplace la valeur `@ID@` par une valeur de hachage sha256. Cette valeur de hachage représente une combinaison de l'ID de fédération en cours, du nom d'utilisateur et de la racine de la partie de confiance.

L'avantage du hachage est que le nom d'utilisateur n'est pas exposé sur chaque site visité pour la connexion unique OpenID. La valeur de hachage est rapide à générer, sans recherche externe. ce masquage du nom de compte permet de protéger l'utilisateur du détournement de son identité par des pirates informatiques. L'exposition du nom de compte fournit un point de départ pour les attaques malignes ou pour le verrouillage d'un utilisateur sur un compte.

Par exemple, lorsque l'expression régulière configurée est :

```
http://webseal.example.com/@ID@
```

un exemple d'URL d'identité est le suivant :

```
http://webseal.example.com/
3d0f1d5e9a3a617771608b390b5c7fc1601a3839f161060cbad8e93b98f034c2
```

Générateur d'ID de service d'alias

L'implémentation de service d'alias affecte automatiquement un UUID généré de manière aléatoire pour la valeur `@ID@`. Lors de la première utilisation, un UUID est généré et stocké dans le service d'alias. La clé de recherche pour l'UUID est basée sur le nom d'utilisateur, l'ID de fédération en cours et la racine de la partie de confiance. Lors des utilisations suivantes, le même UUID est extrait du service d'alias. Cette méthode permet de s'assurer qu'un identificateur cohérent est utilisé pour l'utilisateur au niveau de cette partie de confiance spécifique.

Comme dans le cas du mode de hachage, le nom d'utilisateur n'est pas exposé sur chaque site utilisé pour la connexion unique OpenID.

Par exemple, lorsque l'expression régulière configurée est :

```
http://webseal.example.com/@ID@
```

Voici un exemple d'URL d'identité : `http://webseal.example.com/c84911b2-0124-14f0-991a-a5a8f0e6f99d`

Evitez de réutiliser les identités d'utilisateur pour définir des URL d'identité

Les URL d'identité OpenID ne doivent jamais être réutilisés. Une fois l'adresse URL attribuée à un utilisateur individuel, il convient de ne jamais la réaffecter à un autre utilisateur. Cette règle est importante, car pour tout site Web de consommation sur lequel l'utilisateur d'origine s'est authentifié, il est possible qu'un compte associé à l'adresse URL soit encore existant.

Les exigences concernant la non réutilisation des URL d'identité OpenID doivent être mises en oeuvres par l'environnement de déploiement. Tivoli Federated Identity Manager ne peut pas effectuer de vérification de la réutilisation. L'application des accès des noms d'utilisateurs doit suivre un processus permettant de s'assurer que chaque adresse URL est affectée une seule fois.

Fédérations de fournisseurs d'identité

Les fédérations de fournisseur d'identité OpenID partagent des similarités avec d'autres fédérations de connexion unique prises en charge par Tivoli Federated Identity Manager. Toutefois, les concepts de *fédération* et *partenaires* s'appliquent différemment. Une différence majeure est qu'un fournisseur d'identité OpenID n'a pas besoin de connaître d'avance la partie consommatrice. La négociation de secret partagé fait partie du protocole et aucune pré-configuration des clés ou des partenaires n'est nécessaire.

Dans OpenID, l'utilisateur est impliqué dans sa décision de faire confiance à des partenaires consommateurs particuliers. Cette décision est prise en examinant l'adresse URL *trust_root* de la page de consentement d'authentification. Ceci implique le concept de fournisseurs de services partenaires.

Remarque : Dans OpenID 2.0, la racine *trust_root* porte le nom de domaine (*realm*).

La configuration de la fédération comprend certaines propriétés de configuration des partenaires, mais celles-ci sont utilisées par les modules de jeton destinés au service de jetons de sécurité (STS).

La dénomination de la fédération OpenID est conforme à la norme Tivoli Federated Identity Manager relative à l'identificateur unique ou ID de protocole `protocolID`. La syntaxe est la suivante :

`https://<nom_hôte:port>/FIM/sps/<nom_fédération>/openid`

Par exemple :

`https://www.example.com/FIM/sps/openidfedip/openid`

Noeud final de connexion unique

Le noeud final de connexion unique correspond à l'URL du serveur OpenID. Il prend en charge les requêtes émises par le consommateur et le navigateur lorsqu'elles sont redirigées par le consommateur. Cette adresse URL nécessite un accès non authentifié, afin que les requêtes émises par les clients consommateurs anonymes puissent être générées selon les modes de message suivants :

- associate
- checkid_immediate
- check_authentication

Lorsqu'une requête checkid_setup est reçue et que l'utilisateur n'a encore jamais reçu accrédité le consommateur, cette adresse URL fournit également l'invite de consentement d'authentification, *consent-to-authenticate*.

Ce noeud final renvoie les résultats de l'authentification aux sites de consommation.

Exemple de noeud final :

`https://webseald.example.com/FIM/sps/openidfedip/openid/sso`

Noeud final d'authentification

Lorsqu'un utilisateur ne s'est pas encore connecté à un fournisseur d'identité, le noeud final de connexion unique redirige le navigateur vers le noeud final d'authentification. L'utilisateur est alors authentifié. Ce noeud final est requis durant les opérations de type 'checkid_setup', lorsque l'utilisateur ne s'est pas encore authentifié auprès du fournisseur d'identité et que la connexion unique est initiée à partir d'un consommateur.

En cas de succès de l'authentification, le noeud final redirige généralement l'utilisateur vers le noeud final de connexion unique pour la permettre la suite du traitement. Cette redirection est commandée par un paramètre de requête au format chaîne. La syntaxe est la suivante :

```
<protocolID>/authn?return=<url>
```

Voici un exemple de chaîne continue unique :

```
https://webseald.example.com/FIM/sps/openidfedip/openid/authn?return=
      https://webseald.example.com/FIM/sps/openidfedip/sso
```

Noeud final de gestion de site

Lorsque le fournisseur d'identité reçoit un message checkid_setup, il demande à l'utilisateur la permission (ou le consentement) de fournir les informations d'authentification et d'attribut relatives à l'utilisateur.

Le fournisseur d'identité utilise un modèle de page et un cookie de navigateur pour cet utilisateur de sorte à mémoriser les préférences utilisateur. Le fournisseur d'identité doit être en mesure d'extraire les préférences sauvegardées pour pouvoir répondre aux messages en mode checkid_setup.

Tivoli Federated Identity Manager sauvegarde les préférences utilisateur au moyen d'un point d'extension de gestionnaire de sites dignes de confiance. Le point d'extension utilise une interface connectable qui permet aux administrateurs de remplace l'implémentation d'extension par défaut par une implémentation personnalisée qui prend par exemple en charge un modèle de stockage côté serveur. Un autre objectif de ce point d'extension est le fait qu'une implémentation personnalisée peut être utilisée pour consentir automatiquement toutes les décisions de confiance dans des environnements d'authentification fermés.

Le fournisseur d'identité utilise ce gestionnaire de sites dignes de confiance pour gérer les sites de consommation sécurisés et non sécurisés. Lorsque le gestionnaire de site demande à l'utilisateur de donner son consentement d'authentification, l'utilisateur peut spécifier des règles applicables au consommateur spécifié, en procédant comme suit :

- Toujours autoriser (Always Allow)
- Autoriser une fois (Allow Once)
- Refuser une fois (Deny Once)
- Toujours refuser (Always Deny)

L'utilisateur peut, par la suite, utiliser ce gestionnaire de site pour accéder aux préférences sauvegardées et les modifier. Les utilisateurs peuvent, en option, supprimer définitivement de la liste un site sécurité ou non sécurisé. Lors d'une telle opération, l'utilisateur est amené à donner son consentement d'authentification dès sa tentative de connexion unique suivante sur ce site consommateur.

Le gestionnaire de site sécurisé mémorise également les attributs facultatifs éventuels demandés par un fournisseur de services (si l'utilisateur ait autorisé le partage de ces attributs).

Le noeud final exécute les tâches suivantes :

1. Utilise un modèle HTML pour inviter l'utilisateur à indiquer la liste définitive de ses sites dignes et non dignes de confiance
2. Permet à l'utilisateur de supprimer des sites dans la liste permanente

La syntaxe de l'URL du noeud final est la suivante :

```
<protocolID>/sites
```

Par exemple :

```
https://webseald.example.com/FIM/sps/openidfedip/openid/sites
```

Chaînes d'accréditation de fournisseur d'identité

Dans le modèle OpenID, le consommateur peut exiger que des attributs spécifiques soient fournis pour chaque identité d'utilisateur. Tivoli Federated Identity Manager utilise une chaîne du service d'accréditation spécifiée sur le fournisseur d'identité pour obtenir les attributs et les placer dans un jeton XML simple.

Lorsqu'un utilisateur contacte le fournisseur d'identité en présentant une URL d'identité OpenID, le fournisseur d'identité vérifie l'identification de l'utilisateur. Lorsque le fournisseur d'identité fonctionne en mode checkid_immediate ou checkid_setup, le service d'accréditation est appelé afin d'intercepter et fournir les données d'attributs. En outre, le service de confiance est utilisé pour confirmer que toutes les exigences d'authentification PAPE (Provider Authentication Policy Extension) sont satisfaites.

Le fournisseur d'identité utilise une chaîne de modules de services d'accréditation principalement dans le but de permettre l'extraction des valeurs d'attributs obligatoires et facultatives. Le service d'accréditation s'appuie sur le flux de modules standard suivant :

1. Validate (Validation)

   L'opération de validation est exécutée sur un jeton IVCred généré à partir des droits d'authentification de l'utilisateur.
2. Mappage

   Le module de mappage peut appartenir à n'importe lequel des types pris en charge. Lorsque les données d'attributs de l'utilisateur peuvent être extraites du jeton d'entrée IVCred, la définition d'une règle de mappage XSLT constitue souvent une bonne option. Un module de mappage de Tivoli Directory Integrator, ou un module de mappage Java personnalisé, est utile lorsque les données d'attributs doivent être obtenues depuis une source externe.
3. Issue (Emission)

   L'opération d'émission génère un jeton STSUU (Security Token Service Universal User). Le jeton fournit l'ensemble d'attributs requis et facultatifs au service de protocole de connexion unique, avec les informations d'authentification PAPE validées. Cette opération permet au service de générer une réponse de connexion OpenID ou de demander à nouveau une authentification si cela est nécessaire pour satisfaire les autres règles PAPE demandées.

Pour que le module de mappage puisse fournir les attributs obligatoires et facultatifs, il doit connaître la liste de ces attributs. La liste des attributs requis et facultatifs est envoyée au service d'accréditation sous forme de réclamations. Les informations PAPE demandées sont également disponibles à la règle de mappage en informations de réclamations.

La liste des réclamations peut également contenir des données de préférence utilisateur. Un index des identités peut par exemple être inclus dans le formulaire de consentement d'authentification. L'index est extrait via le point d'extension de gestion des consommateurs accrédités, puis inclus dans les réclamations.

```
<fimopenid:OpenIDClaims xmlns:fimopenid="urn:ibm:names:ITFIM:openid"
    xmlns:fimpape="urn:ibm:names:ITFIM:openid:PAPE"
    xmlns:fimqs="urn:ibm:names:ITFIM:queryservice"
    ClaimedId="http://specs.openid.net/auth/2.0/identifier_select"
    DiscoveredIdentifier="https://www.myidp.ibm.com/FIM/op/
85da8845-0127-1a04-9a9f-dca9f50a9649"
    IdentityURL="http://specs.openid.net/auth/2.0/identifier_select"
    IsOPIdentifierLogin="true"
    IsRPReturnToValidated="false"
    OPLocalId="http://specs.openid.net/auth/2.0/
identifier_select"
    OpenIDServerURL="https://www.myidp.ibm.com/
FIM/sps/openididp/openid/sso"
    PolicyURL="http://www.ibm.com"
    ReauthCount="0"
    ReturnTo="https://www.myrp.ibm.com/sps/myrp/openid/
loginreturn?nonce=uuid85d96a6f-0127-1f6e-bafb-c3b7deb3ed5d"
    TrustRoot="https://www.myrp.ibm.com/"
    Userdata=""
    Version="http://specs.openid.net/auth/2.0">
  <fimopenid:PrincipalName>shane</fimopenid:PrincipalName>
  <fimqs:RequestedAttributes>
    <fimqs:Attribute name="openid.sreg.email" optional="false" />
    <fimqs:Attribute name="openid.sreg.nickname" optional="true" />
    <fimqs:Attribute name="openid.sreg.fullname" optional="true" />
  </fimqs:RequestedAttributes>
  <fimpape:OpenIDPAPEClaims>
    <fimpape:Attribute name="openid.pape.preferred_auth_levels">
      <fimpape:Value>urn:ibm:names:ITFIM:5.1:accessmanager</fimpape:Value>
    </fimpape:Attribute>
    <fimpape:Attribute name="openid.pape.preferred_auth_policies">
      <fimpape:Value>http://schemas.xmlsoap.org/ws/2005/05/
identity/claims/privatepersonalidentifier</fimpape:Value>
      <fimpape:Value>http://www.idmanagement.gov/schema/2009/05/
icam/openid-trust-level1.pdf</fimpape:Value>
    </fimpape:Attribute>
  </fimpape:OpenIDPAPEClaims>
</fimopenid:OpenIDClaims>
```

Figure 23. Exemples de réclamations durant l'appel du service d'accréditation par le fournisseur d'identité

La figure 23 illustre un exemple de réclamations transmises au service d'accréditation. Notez les réclamations optionnelles contenues dans la liste `RequestedAttributes` :

- `openid.sreg.email`
- `openid.sreg.nickname`
- `openid.sreg.fullname`

Lorsque des attributs sont requis, la valeur facultative est définie sur `false`.

Dans l'exemple, vous pouvez remarquer que la propriété `userdata` est une chaîne vide. Cette chaîne vide indique qu'aucune donnée optionnelle n'a été définie durant la phase de consentement pour l'authentification. Ces données (ainsi que leur consultation dans le module de mappage de la chaîne) sont celles dans lesquelles l'extraction d'attributs spécifiques à une personne peut être accomplie pour un utilisateur.

Gestion de grandes quantités de données d'attributs d'utilisateur

L'authentification OpenID fonctionne sur la base d'adresses URL redirigées. Lorsqu'une réponse à une authentification de la part du fournisseur d'identité doit contenir plus de 2 Ko de données de registre d'utilisateurs, Tivoli Federated Identity Manager commute automatiquement les données en messages POST. Ce comportement est conforme à la spécification OpenID 2.0, qui permet d'appliquer l'envoi automatique de transactions POST aux messages indirects.

Remarque : La commutation automatique en messages POST n'est pas prise en charge dans les déploiements OpenID 1.1.

Reconnaissance du correspondant associé

A l'aide de la reconnaissance RP, les fournisseurs OpenID peuvent détecter et vérifier les adresses `return_to` des domaines prenant en charge OpenID.

La reconnaissance de partie de confiance s'effectue lorsqu'un fournisseur OpenID reçoit une demande de connexion unique sollicitée. La partie de confiance effectue alors le processus de reconnaissance sur l'URL spécifiée dans le paramètre `openid.realm` du message de connexion. Les parties de confiance peuvent publier leur URL `return_to` dans XRDS.

Un administrateur peut configurer le panneau de propriétés du fournisseur d'identité pour appliquer la reconnaissance de partie de confiance réussie. Il existe également une macro à la page consent.html qui permet page au fournisseur d'identité d'indiquer que la reconnaissance de partie de confiance n'a pas été réalisée. Pour plus d'informations sur la page d'accord d'authentification, voir «Modèle de page pour le consentement d'authentification», à la page 328

Cette spécification permet aux fournisseurs OpenID de vérifier les demandes d'authentification et de s'assurer que les réponses sont redirigées vers des noeuds finaux `return_to` valides.

Si la reconnaissance ne peut pas vérifier l'URL `return_to` sur le domaine de la partie de confiance, Tivoli Federated Identity Manager affiche une erreur ou un avertissement selon la configuration.

L'attribut de réclamation IsRPReturnToValidated indique à la règle de mappage si la validation d'URL `return_to` s'est produite. Tivoli Federated Identity Manager ajoute cet attribut dans l'élément OpenIDClaims transmis au service de jeton de sécurité. Il permet à une règle de mappage de détecter les échecs de reconnaissance de la partie de confiance et de procéder à l'action appropriée. La valeur de cet attribut de réclamation peut être `true` ou `false`.

Modes d'authentification

OpenID prend en charge deux modes d'authentification :

- checkid_immediate
- checkid_setup

Le mode d'authentification checkid_immediate s'emploie généralement dans les environnements comprenant de nombreux clients, dans lesquels un objet fenêtre intelligent a pour rôle d'exécuter les tâches suivantes :

- Déterminer si l'utilisateur d'un navigateur détient une adresse URL OpenID particulière réclamée
- Eviter l'interaction entre le navigateur et l'utilisateur

Pour qu'un consommateur puisse adresser une requête checkid_immediate à un fournisseur d'identité, ajoutez ce paramètre d'entrée dans le formulaire de connexion :

```
<input type=''hidden'' name=''openid.mode'' value=''checkid_immediate''>
```

Le noeud de situé à l'URL du protocole de connexion unique Tivoli Federated Identity Manager initie la connexion à partir du consommateur.

- Lorsque la réponse fournie par le fournisseur d'identité est une assertion valide selon laquelle l'utilisateur est détenteur de l'URL d'identité, Tivoli Federated Identity Manager procède à un échange de jetons avec le service STS, puis établit la connexion avec le serveur point de contact. Ce comportement est le même que pour checkid_setup.
- Lorsque la réponse renvoyée par le fournisseur d'identité est une assertion ayant échoué, un modèle de page HTML est chargé à partir de la fabrique de pages. La macro de remplacement contenue dans la page est complétée avec la valeur du paramètre `open.user_setup_url` renvoyée par le fournisseur d'identité.

Le mode d'authentification checkid_setup permet au fournisseur d'identité d'interagir avec l'utilisateur, afin d'émettre une demande d'authentification ou d'auto-enregistrement avant que le résultat ne soit renvoyé au consommateur. Lorsqu'aucun mode d'authentification n'est spécifié dans le formulaire de connexion, le mode par défaut est checkid_setup.

Etant donné que checkid_setup est le mode par défaut, il n'est pas nécessaire de spécifier le mode dans le formulaire de connexion. Toutefois, le consommateur peut demander ce mode de manière spécifique. Le code à utiliser dans ce cas est le suivant :

```
<input type=''hidden'' name=''openid.mode'' value=''checkid_setup''>
```

Le support de Tivoli Federated Identity Manager pour checkid_setup est un flux de connexion unique fédérée comportant une redirection vers le fournisseur d'identité pour l'authentification, ainsi qu'une interaction avec l'utilisateur pour l'approbation de la connexion. Le flux d'authentification a pour résultat le renvoi au consommateur des attributs de réponse signés. Lorsque la signature numérique est validée, les attributs sont intégrés à un jeton STSUU (Security Token Service Universal User), puis envoyés au service d'accréditation pour obtenir l'échange avec des droits d'accès IVCred. Les droits d'accès sont ensuite utilisés pour la connexion.

Fédérations de consommateurs

Le *consommateur* OpenID de Tivoli Federated Identity Manager joue un rôle similaire à celui que joue un *fournisseur de services* dans d'autres protocoles de connexion unique. Le consommateur OpenID utilise une fédération Tivoli Federated Identity Manager qui présente un certain nombre de similitudes, mais aussi différences significatives avec les fédérations liées aux autres protocoles de connexion unique.

Il n'est notamment pas nécessaire d'associer directement les partenaires du fournisseur d'identité à des fédérations de consommateurs OpenID. L'échange de clés et l'association avec des fournisseurs d'identité particuliers sont contrôlés par l'URL d'identification OpenID, telle que déterminée au moment de l'exécution. Aucun ajout ni aucune configuration des partenaires n'a lieu pour une fédération de fournisseur de services OpenID.

L'entité de la fédération Tivoli Federated Identity Manager destinée au consommateur contient les éléments suivants :

- Un noeud final de connexion
- Un noeud final de renvoi de connexion
- Une adresse URL racine authentifiée (connue sous forme de *domaine* (realm) dans OpenID 2.0)
- Des paramètres indiquant le type de module de mappage dans la chaîne d'accréditation
- Les paramètres de configuration éventuellement associés
- Les règles d'agent d'utilisateur qui contrôlent la plage d'adresse IP autorisée, les réseaux et/ou les modèles de noms d'hôte destinés aux URL d'identification OpenID, ainsi qu'aux noeuds finals de serveurs OpenID.

La syntaxe de l'ID de protocole pour la fédération OpenID est la suivante :

`https://<nom_hôte:port>/FIM/sps/<nom_fédération>/openid`

Par exemple :

`https://webseald.example.com/FIM/sps/openidfedsp/openid`

Le noeud final de connexion

Le client Tivoli Federated Identity Manager prend en charge une adresse URL de renvoi de connexion. L'URL de connexion reçoit la requête POST du formulaire de connexion initial et lance le programme checkid_setup ou checkid_immediate.

Conformément au paramètre de fédération protocolID dans l'exemple précédent, le noeud final est :

`https://webseald.example.com/FIM/sps/openidfedsp/openid/login`

Remarque : Voici un exemple de noeud final pour les les déploiements effectués avec WebSphere en tant que serveur point de contact :

`https://poc.example.com/sps/openidfedsp/openid/login`

Le délégué de la connexion unique situé sur le noeud final exécute les tâches suivantes :

1. Détermine le nom de connexion entrant à partir de l'adresse URL d'identité OpenID, ainsi que les paramètres d'extension.

2. Déterminez la forme canonique de l'adresse URL d'identification conformément à la spécification d'authentification OpenID applicable. La reconnaissance HTML et Yadis sont prises en charge.
3. Effectuez l'extraction de l'adresse URL d'identification finale, y compris les délégués, de l'utilisateur. Déterminez le serveur OpenID associé à l'utilisateur.
4. Si aucune association avec un fournisseur d'identité n'existe, créez-en une.
5. Adressez une requête checkid_setup ou checkid_immediate au serveur OpenID et redirigez le navigateur vers le fournisseur d'identité.

Noeud final de renvoi de connexion

Tivoli Federated Identity Manager prend en charge une adresse URL de renvoi de connexion. Le navigateur est redirigé vers cette adresse par le fournisseur d'identité une fois le processus de connexion unique terminé. Ce noeud final est transmis en tant que paramètre openid.return_to lors de la requête de connexion unique.

Ce noeud final est par exemple :

```
https://webseald.example.com/FIM/sps/openidfedsp/openid/loginreturn
```

Le délégué de connexion unique situé sur ce noeud final traite les réponses aux requêtes checkid_setup et checkid_immediate. Le délégué traite les réponses, ainsi que toute demande check_authentication ou invalidation de gestionnaire d'association susceptible d'être générée dans le résultat.

- Lorsqu'une réponse est renvoyée avec une signature validée avec succès, le service d'accréditation utilise les paramètres contenus dans la réponse. Les paramètres sont utilisés pour créer un jeton STSUU (Security Token Service Universal User). Le délégué utilise le service d'accréditation pour échanger le jeton STSUU avec une accréditation IVCred. Les droits d'accès sont ensuite utilisés pour l'authentification de Tivoli Federated Identity Manager.
- Lors du renvoi d'une réponse sans succès, une page d'erreur s'affiche.

Racine d'accréditation ou adresse URL de domaine

Le consommateur Tivoli Federated Identity Manager fournit également une *racine d'accréditation* ou une adresse URL de *domaine*. Cette adresse URL sert de base affichée pour l'utilisateur au niveau du fournisseur d'identité.

Tivoli Federated Identity Manager lit l'adresse URL de la racine d'accréditation à partir des propriétés de configuration. Cette propriété est initialement générée par les entrées de l'administrateur, afin de combiner les valeurs suivantes :

- Protocole

  Par exemple, `https`.
- Nom d'hôte

  Nom d'hôte du serveur point de contact
- Port

  Facultatif. Spécifié uniquement lorsqu'il ne s'agit pas du port standard.
- Barre oblique (/)

Par exemple :

```
https://webseald.example.com/
```

Connexion OpenID

Le consommateur Tivoli Federated Identity Manager présente un formulaire de connexion afin de demander l'URL OpenID de l'utilisateur. Ce formulaire peut comporter au choix des méthodes POST ou GET adressées au noeud final de connexion du consommateur Tivoli Federated Identity Manager. Les paramètres inclus peuvent comporter plusieurs adresses URL si nécessaire.

Tivoli Federated Identity Manager prend en charge :

- Les spécifications d'authentification OpenID 1.1
- Les spécifications d'authentification OpenID 2.0
- L'extension OpenID Simple Registration Extension 1.0
- L'extension OpenID Simple Registration Extension 1.1
- L'extension OpenID Attribute Exchange
- L'extension PAPE (Provider Authentication Policy Extension) 1.0

Remarque : La méthode de connexion utilisée par le consommateur Tivoli Federated Identity Manager consumer est la même que lors de l'accès au fournisseur d'identité Tivoli Federated Identity Manager ou à un autre fournisseur d'identité.

Considérons par exemple le scénario de déploiement suivant :

- WebSEAL est le point de contact d'un hôte appelé `www.example.com`
- Une fédération de consommateurs OpenID porte le nom `openidfedsp`

La figure 24 montre un exemple de formulaire de connexion valable pour cet exemple.

```
<html>
  <form method="post"
  action="https://www.example.com/FIM/sps/openidfedsp/openid/login">
    <img src="login-bg.gif" /> 
    <input type="text" name="openid_identifier" /> 
    <input type="submit" value="Login"/>
  </form>
</html>
```

Figure 24. Formulaire de connexion OpenID simple

Le fournisseur de services Tivoli Federated Identity Manager procède comme suit :

1. Lit le paramètre `openid_identifier`
2. Exécute le flux d'authentification spécifié pour l'authentification OpenID 2.0
3. Exécute une connexion EAI (External Authentication Interface) sur WebSEAL

Après une réponse checkid_immediate ou checkid_setup positive, le consommateur Tivoli Federated Identity Manager appelle le service d'accréditation afin de traiter les éventuelles manipulations sur les attributs obligatoires ou l'identité de l'utilisateur.

Au cours du processus de connexion, le consommateur peut demander des attributs auprès du fournisseur d'identité en spécifiant des paramètres additionnels dans le formulaire de connexion. Ces paramètres doivent correspondre aux noms des paramètres décrits dans l'extension OpenID ERS (Simple Registration

Extension) 1.0. Vous pouvez également utiliser d'autres spécifications prises en charge, telles que Simple Registration Extension 1.1, Attribute Exchange 1.0 and Private Personal Identifier Generator 1.0.

A titre d'exemple, la figure 25 illustre un formulaire de connexion qui accomplit les exigences suivantes à l'aide de Simple Registration Extension :

- Demande d'adresse électronique au fournisseur d'identité
- Demande de la date de naissance au fournisseur d'identité
- Eventuellement, demande du nom complet de l'utilisateur
- Attribution d'une adresse URL renvoyant à une page descriptive des règles de confidentialité

```
<html>
  <form method="post"
  action="https://www.example.com/FIM/sps/openidfedsp/openid/login">
    <input type="hidden" name="openid.sreg.required"
     value="email,dob" />
    <input type="hidden" name="openid.sreg.optional"
     value="fullname" />
    <input type="hidden" name="openid.sreg.policy_url"
value="http://www.example.com/privacy_policy.html" />
    <img src="login-bg.gif" /> 
    <input type="text" name="openid_identifier" /> 
    <input type="submit" value="Login"/>
  </form>
</html>
```

Figure 25. Formulaire de connexion OpenID comportant les paramètres d'extension de registre

Lorsque ces paramètres sont présents dans la demande de connexion, Tivoli Federated Identity Manager les envoie au fournisseur d'identité. Cette action est effectuée lors des requêtes checkid_immediate et checkid_setup.

Les paramètres ne doivent pas nécessairement être masqués, ni organisés sous forme de liste séparée par des virgules.

Les paramètres peuvent être constitués d'attributs à valeurs multiples. L'usage des attributs à valeurs multiples permet au serveur de présenter à l'utilisateur des boutons d'option, de s zones de liste ou d'autres objets fenêtre à valeur multiples dans le code HTML. Tivoli Federated Identity Manager traite chaque valeur sous forme de liste séparée par des virgules. Les valeurs multiples constituées d'une seule entrée par valeur sont autorisées.

Vous pouvez mettre en oeuvre une connexion avec redirection automatique vers une adresse URL spécifiée. Lorsque WebSEAL est le serveur point de contact, les règles de traitement de l'authentification EAI s'appliquent. Vous pouvez inclure un paramètre `TARGET` optionnel dans le formulaire de connexion afin de rediriger l'utilisateur à la suite d'une authentification ayant abouti.

Modèles de pages

Le client Tivoli Federated Identity Manager utilise plusieurs modèles de pages HTML lors du traitement des demandes et erreurs d'authentification :

- Lorsque le consommateur traite une requête checkid_immediate et que le fournisseur d'identité ne parvient pas à déterminer la validité de l'adresse URL OpenID fournie par l'utilisateur, un fichier modèle est renvoyé par le consommateur.

  Voir «Modèle de page renvoyé pour checkid_immediate», à la page 339.
- Le consommateur utilise un fichier modèle pour les besoins de prise en charge du transport POST des messages indirects volumineux. Le consommateur Tivoli Federated Identity Manager prend en charge le transport POST des messages indirects volumineux. La prise en charge utilise un fichier modèle.

  Voir «Modèle de page pour l'envoi indirect de requêtes OpenID 2.0», à la page 338.
- Lorsque le traitement d'une requête checkid_immediate ou checkid_setup produit une erreur, le consommateur renvoie celle-ci au moyen d'un fichier modèle.

  Voir «Modèle de page renvoyé pour les erreurs du serveur», à la page 340.
- Lorsqu'une erreur se produit sur le consommateur et qu'elle entraîne un blocage du traitement, le consommateur renvoie une erreur au moyen d'un fichier modèle.

  Voir «Modèle de page pour les erreurs liées à OpenID», à la page 336.

Chaînes d'accréditation du consommateur

Au cours du processus de connexion, Tivoli Federated Identity Manager gère le mappage des attributs et des identités.

Lorsqu'une réponse checkid_immediate ou checkid_setup renvoyée par le fournisseur d'identité signale une assertion ayant abouti, Tivoli Federated Identity Manager génère tous les attributs et données de réponse PAPE renvoyés par le fournisseur d'identité dans un jeton STSUU (Security Token Service Universal User) puis utilise le service d'accréditation pour échanger ce jeton avec une accréditation IVCred.

La chaîne d'accréditation est constituée des éléments suivants :

- Un jeton STSUU en mode validation

  Le jeton contient l'URL d'identité OpenID ainsi que tous les paramètres d'extension dont les attributs utilisateur. Le jeton STSUU est généré par le délégué chargé du renvoi de la connexion OpenID une fois que la signature a été vérifiée en réponse à une connexion lancée par le fournisseur d'identité.
- Un module de mappage

  L'usage du module de mappage permet au consommateur d'exécuter le mappage nécessaire des identités et des attributs.

  Le type de module de mappage à appliquer pour la fédération de consommateur est défini lors de la configuration de celle-ci. Les types de module de mappage standard sont pris en charge :

  – Règles de mappage XSLT ou Javascript
  – Module de mappage de Tivoli Directory Integrator
  – Modules de mappage personnalisés.

  Dans de nombreux cas, l'utilisation des règles de mappage de script est suffisante, puisqu'elles ne nécessitent généralement l'extraction d'aucun attribut externe.

  La distribution du produit Tivoli Federated Identity Manager inclut plusieurs exemples de règles de mappage de script et un exemple de chaîne d'assemblage Tivoli Directory Integrator (module de mappage).
- Une accréditation IVCred en mode émission

Liaisons avec les comptes

L'un des scénarios importants pour le consommateur du point de vue d'OpenID consiste à exécuter une liaison de compte. Si, par exemple, un utilisateur s'est authentifié directement sur un site Web faisant également office de consommateur OpenID, ce site Web peut autoriser l'utilisateur à lier son compte à une identification OpenID. En effectuant une connexion OpenID alors que l'utilisateur est déjà connecté au site Web site, le site de consommation peut associer cet identificateur OpenID avec le compte actuellement connecté.

Pour permettre la prise en charge de ce scénario, Tivoli Federated Identity Manager envoie des réclamations dans un appel WS-Trust adressé au service STS. L'appel inclut le nom de l'utilisateur actuellement connecté lorsqu'une session d'authentification existe.

La figure 26 illustre un exemple de format pour les réclamations adressées au service d'accréditation. Ce format est disponible pour mapper des implémenteurs de modules via le jeton STSUU.

```
<fimopenid:OpenIDClaims xmlns:fimopenid="urn:ibm:names:ITFIM:openid"
xmlns:fimpape="urn:ibm:names:ITFIM:openid:PAPE"
ClaimedId="https://www.myidp.ibm.com/FIM/op/
85da8845-0127-1a04-9a9f-dca9f50a9649"
IdentityURL="https://www.myidp.ibm.com/FIM/op"
IsOPIdentifierLogin="true"
IsRPReturnToValidated="false"
NormalizedIdentityURL="https://www.myidp.ibm.com/FIM/op/
85da8845-0127-1a04-9a9f-dca9f50a9649"
OPLocalId="https://www.myidp.ibm.com/FIM/op/
85da8845-0127-1a04-9a9f-dca9f50a9649"
OpenIDServerURL="https://www.myidp.ibm.com/FIM/
sps/openididp/openid/sso"
ReauthCount="0"
ReturnTo="https://www.myrp.ibm.com/sps/myrp/openid/
loginreturn?nonce=uuid85e85b2a-0127-1286-99d4-d5e72a774a5f"
Signed="openid.op_endpoint,openid.return_to,
openid.response_nonce,openid.assoc_handle,
openid.claimed_id,openid.identity,
openid.sreg.dob,openid.sreg.gender,
openid.sreg.email,openid.sreg.language,
openid.sreg.timezone,openid.sreg.fullname,
openid.sreg.postcode,openid.sreg.country,
openid.sreg.nickname,openid.ns.sreg,
openid.ns.pape,openid.pape.auth_time,
openid.pape.auth_policies,openid.pape.auth_level.ns1,
openid.pape.auth_level.ns.ns1"
Target="https://www.myrp.ibm.com/fimivt/protected/ivtlanding.jsp"
Version="http://specs.openid.net/auth/2.0">
<fimpape:OpenIDPAPEClaims>
<fimpape:Attribute name="satisfied_auth_age">
<fimpape:Value>true</fimpape:Value>
</fimpape:Attribute>
<fimpape:Attribute name="openid.pape.preferred_auth_levels">
<fimpape:Value>urn:ibm:names:ITFIM:5.1:accessmanager
</fimpape:Value>
</fimpape:Attribute>
<fimpape:Attribute name="satisfied_auth_policies">
<fimpape:Value>true</fimpape:Value>
</fimpape:Attribute>
<fimpape:Attribute name="openid.pape.preferred_auth_policies">
<fimpape:Value>http://www.idmanagement.gov/schema/
2009/05/icam/openid-trust-level1.pdf</fimpape:Value>
<fimpape:Value>http://schemas.xmlsoap.org/ws/2005
/05/identity/claims/privatepersonalidentifier</fimpape:Value>
</fimpape:Attribute>
</fimpape:OpenIDPAPEClaims>
</fimopenid:OpenIDClaims>
```

Figure 26. Réclamations OpenID lors d'un appel consommateur WS-Trust

L'attribut PrincipalName, lorsqu'il est présent dans les réclamations, contient le nom d'utilisateur Tivoli Federated Identity Manager qui désigne l'utilisateur actuellement connecté. Ceci permet aux chaînes d'accréditation d'associer automatiquement, par le biais de règles de mappage, un OpenID particulier à un compte existant.

L'exemple contient d'autres réclamations sous forme de paramètres issus de la réponse à une connexion unique à partir du serveur OpenID. L'attribut relatif à l'URL d'identité correspond à celle qui est fournie par l'utilisateur dans le formulaire de connexion. L'attribut NormalizedIdentityURL représente la forme canonique de l'URL d'identité qui résulte de la normalisation accomplie dans le cadre du procédure de reconnaissance.

Le jeton STSUU envoyé au service d'accréditation avec la requête contient des attributs relatifs à chacun des composants répertoriés dans le jeu d'attributs de `Signed`, ainsi que certains autres paramètres portant sur des chaînes de requête.

La figure 27 illustre le jeton STSUU généré à partir de l'appel WS-Trust illustré à la figure 26, à la page 301.

```
<?xml version="1.0" encoding="UTF-8"?>
<stsuuser:STSUniversalUser xmlns:stsuuser="urn:ibm:names:ITFIM:1.0:stsuuser">
<stsuuser:Principal><stsuuser:Attribute name="name"><stsuuser:Value>https://www.myidp.ibm.com/FIM/
op/85da8845-0127-1a04-9a9f-dca9f50a9649</stsuuser:Value></stsuuser:Attribute>
</stsuuser:Principal><stsuuser:AttributeList><stsuuser:Attribute name="openid.identity">
<stsuuser:Value>https://www.myidp.ibm.com/FIM/op/85da8845-0127-1a04-9a9f-dca9f50a9649</stsuuser:Value>
</stsuuser:Attribute></stsuuser:AttributeList><stsuuser:RequestSecurityToken />
<stsuuser:ContextAttributes><stsuuser:Attribute name="openid.op_endpoint">
<stsuuser:Value>https://www.myidp.ibm.com/FIM/sps/openididp/openid/sso</stsuuser:Value>
</stsuuser:Attribute><stsuuser:Attribute name="openid.sreg.email">
<stsuuser:Value>jsmith@ibm.com</stsuuser:Value></stsuuser:Attribute>
<stsuuser:Attribute name="openid.sig"><stsuuser:Value>NuKNV1ypZC16d3og6HbvjbCedPVjhRbWAWZ9Gq6g1DU=
</stsuuser:Value></stsuuser:Attribute>
<stsuuser:Attribute name="openid.pape.auth_level.ns1"><stsuuser:Value>1</stsuuser:Value>
</stsuuser:Attribute><stsuuser:Attribute name="openid.claimed_id">
<stsuuser:Value>https://www.myidp.ibm.com/FIM/op/85da8845-0127-1a04-9a9f-dca9f50a9649</stsuuser:Value>
</stsuuser:Attribute><stsuuser:Attribute name="openid.ns">
<stsuuser:Value>http://specs.openid.net/auth/2.0</stsuuser:Value>
</stsuuser:Attribute><stsuuser:Attribute name="openid.sreg.language">
<stsuuser:Value>en</stsuuser:Value></stsuuser:Attribute>
<stsuuser:Attribute name="openid.sreg.fullname"><stsuuser:Value>John Smith</stsuuser:Value>
</stsuuser:Attribute><stsuuser:Attribute name="nonce">
<stsuuser:Value>uuid85e85b2a-0127-1286-99d4-d5e72a774a5f</stsuuser:Value>
</stsuuser:Attribute><stsuuser:Attribute name="openid.pape.auth_time">
<stsuuser:Value>2010-03-22T12:47:41Z</stsuuser:Value> </stsuuser:Attribute>
<stsuuser:Attribute name="openid.return_to"><stsuuser:Value>https://www.myrp.ibm.com/sps/myrp/
openid/loginreturn?nonce=uuid85e85b2a-0127-1286-99d4-d5e72a774a5f</stsuuser:Value>
</stsuuser:Attribute><stsuuser:Attribute name="openid.signed"><stsuuser:Value>
op_endpoint,return_to,response_nonce,assoc_handle,claimed_id,identity,sreg.dob,
sreg.gender,sreg.email,sreg.language,sreg.timezone,sreg.fullname,
sreg.postcode,sreg.country,sreg.nickname,ns.sreg,ns.pape,pape.auth_time,
pape.auth_policies,pape.auth_level.ns1,pape.auth_level.ns.ns1</stsuuser:Value>
</stsuuser:Attribute><stsuuser:Attribute name="openid.sreg.nickname">
<stsuuser:Value>Smithy</stsuuser:Value></stsuuser:Attribute>
<stsuuser:Attribute name="openid.identity">
<stsuuser:Value>https://www.myidp.ibm.com/FIM/
op/85da8845-0127-1a04-9a9f-dca9f50a9649</stsuuser:Value>
</stsuuser:Attribute><stsuuser:Attribute name="openid.ns.sreg">
<stsuuser:Value>http://openid.net/extensions/sreg/1.1</stsuuser:Value>
</stsuuser:Attribute><stsuuser:Attribute name="openid.pape.auth_level.ns.ns1">
<stsuuser:Value>urn:ibm:names:ITFIM:5.1:accessmanager</stsuuser:Value>
</stsuuser:Attribute><stsuuser:Attribute name="openid.sreg.dob">
<stsuuser:Value>1980-12-25</stsuuser:Value></stsuuser:Attribute>
<stsuuser:Attribute name="openid.sreg.postcode"><stsuuser:Value>99999</stsuuser:Value>
</stsuuser:Attribute><stsuuser:Attribute name="openid.assoc_handle">
<stsuuser:Value>uuid85ca8353-0127-1776-9b7b-c75a4586c507</stsuuser:Value>
</stsuuser:Attribute><stsuuser:Attribute name="openid.sreg.country">
<stsuuser:Value>AU</stsuuser:Value></stsuuser:Attribute>
<stsuuser:Attribute name="openid.pape.auth_policies">
<stsuuser:Value>http://schemas.xmlsoap.org/ws/2005/05/
identity/claims/privatepersonalidentifier http://www.idmanagement.gov/schema/2009/05/icam/
openid-trust-level1.pdf</stsuuser:Value></stsuuser:Attribute>
<stsuuser:Attribute name="openid.mode"><stsuuser:Value>id_res</stsuuser:Value>
</stsuuser:Attribute><stsuuser:Attribute name="openid.sreg.timezone">
<stsuuser:Value>Australia/Brisbane</stsuuser:Value>
</stsuuser:Attribute><stsuuser:Attribute name="openid.ns.pape">
<stsuuser:Value>http://specs.openid.net/extensions/pape/1.0</stsuuser:Value>
</stsuuser:Attribute><stsuuser:Attribute name="openid.sreg.gender">
<stsuuser:Value>M</stsuuser:Value> </stsuuser:Attribute>
<stsuuser:Attribute name="openid.response_nonce">
<stsuuser:Value>2010-03-22T12:48:08Zuuid85ea7849-0127-1515-b2b5-e9223d6c6970
</stsuuser:Value></stsuuser:Attribute></stsuuser:ContextAttributes>
<stsuuser:AdditionalAttributeStatement />
</stsuuser:STSUniversalUser>
```

Figure 27. Exemple de jeton STSUU lors d'une requête de service d'accréditation sur le consommateur OpenID

Règles relatives à l'agent d'utilisateur

Le consommateur fait appel à un *agent d'utilisateur* (client HTTP) pour établir directement la connexion avec les adresses URL d'identité OpenID, ainsi que les adresses URL de serveurs OpenID auxquels elles font référence. Le fournisseur utilise également le même type de configuration de règle d'agent utilisateur pour les opérations de reconnaissance de partie de confiance.

Il est possible de configurer l'agent d'utilisateur en vue de restreindre la liste des emplacements auxquels il a tenté d'accéder. Cette configuration est réalisée pour dissuader les utilisateurs mal intentionnés de se connecter aux ressources internes par l'intermédiaire de l'agent d'utilisateur.

Les restrictions sont gérées au moyen de la configuration de règles de connexion statique et d'un module d'autorisation de point final dynamique personnalisable. Le module de point final dynamique peut être utilisé pour limiter davantage l'accès aux points finaux lors de l'exécution.

Chaque fédération Tivoli Federated Identity Manager possède une configuration de règles globales. La configuration par défaut définit le comportement par défaut lorsque l'hôte ne figure pas explicitement dans les listes des accès autorisés ou refusés. Ce paramètre permet, selon les cas, d'autoriser ou de refuser l'accès aux adresses URL en tant que comportement par défaut. En plus des règles globales, les administrateurs peuvent créer des plug-ins d'accès de point finaux dynamiques personnalisés. Ces plug-ins peuvent vérifier une liste en ligne de points finaux dignes de confiance ou non. Les administrateurs peuvent ajouter les plug-ins personnalisés à la liste de modules d'autorisation d'accès de pointa finaux dynamiques.

Règle de connexion statique

Avec une règle de connexion statique, un administrateur peut répertorier les hôtes autorisés et refusés. Selon le comportement par défaut sélectionné, l'administrateur peut également spécifier une liste d'hôtes dans la liste autorisée ou refusée.

Lorsque le comportement par défaut sélectionné consiste à **refuser** l'accès, seuls les hôtes contenus dans les listes **autorisées** sont accessibles via l'agent d'utilisateur. Ce paramètre est restrictif. Chaque URL d'identité OpenID et chaque serveur dont vous souhaitez autoriser l'accès doit figurer dans les listes d'autorisation. Lorsque le comportement défini par défaut est un accès **refusé**, toutes les *listes d'accès refusés* ne sont pas forcément utiles.L'accès à tous les hôtes est par défaut refusé, sauf si ceux-ci sont inclus de manière explicite dans une liste d'autorisation.

Lorsque le comportement défini par défaut sélectionné est un accès **autorisé**, l'hôte est contacté, sauf s'il figure dans une *liste d'accès refusés*. Ce paramètre est plus tolérant et permet généralement aux utilisateurs de se connecter à partir d'un serveur OpenID légitime sur Internet. Toutefois, lorsque le paramètre par défaut consiste à **autoriser** les connexions, les listes de refus d'accès doivent être configurées avec soin.

Tivoli Federated Identity Manager prend en charge les types de listes suivants :

Listes d'**autorisation** :

- Liste d'expressions régulières représentant des noms d'hôte et configurable par l'utilisateur
- Liste des masques réseau d'adresse IP (IPv4 et IPv6), configurable par l'utilisateur

Listes de **refus** :

- Liste d'expressions régulières représentant des noms d'hôte et configurable par l'utilisateur
- Liste des masques réseau d'adresse IP (IPv4 et IPv6), configurable par l'utilisateur

- Liste intégrée d'expressions régulières représentant des noms d'hôte refusés par défaut
- Liste intégrée d'expressions régulières représentant des masques réseau d'adresses IP refusées par défaut

Remarque : Les listes d'autorisation sont prioritaires sur les listes de refus.

Les listes d'accès aux noms d'hôtes sont conformes à la syntaxe d'expressions régulières Java comme défini dans le classe de modèles. La liste utilise des expressions régulières pour la concordance avec les noms d'hôtes.

Les listes de refus intégrées ne peuvent pas être modifiées par les utilisateurs. Toutefois, la liste peut être substituée afin d'autoriser certaines entrées via l'ajout d'expressions régulières de noms d'hôte ou de masques de réseau aux listes d'autorisation configurables par l'utilisateur.

La figure 28 illustre les noms d'hôte refusés par défaut. Les valeurs par défaut assurent une protection contre les attaques consistant à tenter d'accéder à des adresses URL arbitraires sur le système local.

```
.*\.localdomain
localhost
```

Figure 28. Expressions régulières représentant des noms d'hôte avec refus par défaut

La figure 29 illustre les masques réseau l'adresse IP default-deny. Ces masques de réseau incluent plusieurs adresses IPv4 et IPv6 non transférables. Cette liste peut être remplacée en ajoutant les réseaux pour lesquels vous souhaitez autoriser les connexions avec la liste des masques de réseau IP autorisés.

```
0.0.0.0/8
10.0.0.0/8
127.0.0.0/8
169.254.0.0/16
172.16.0.0/12
192.168.0.0/16
255.255.255.255
::/128
::1/128
::/96
fc00::/7
fe80::/10
ff00::/8
```

Figure 29. Masques réseau des adresses IP default-deny

Plug-in d'accès aux noeuds finaux dynamiques

Un plug-in d'accès aux noeuds finaux dynamiques est un module personnalisé. Un administrateur peut créer le plug-in d'accès aux noeuds finaux dynamiques personnalisés pour vérifier les listes externes d'hôtes de confiance ou non.

Lorsqu'un administrateur sélectionne un **plug-in d'accès aux noeuds finaux dynamiques** dans le module d'autorisation d'accès aux noeuds finaux dynamiques personnalisé, le logiciel vérifie les noeuds finaux spécifiés. Les noeuds finaux indiqués sont vérifiés afin de déterminer s'ils sont dignes de confiance. Vous pouvez utiliser ce paramètre avec la liste d'autorisation ou de refus d'accès.

Toutefois, si vous définissez l'autorisation de noeuds finaux dynamiques dans la liste d'autorisation d'accès par défaut, le logiciel utilise uniquement les noeuds finaux dans les listes de refus ou d'autorisation.

Exemple : autoriser n'importer quel serveur Internet OpenID, refuser l'accès à l'intranet 9.x.x.x

- Pour configurer cet environnement, la règle d'accès par défaut indiquée est **autoriser**
- La liste d'hôtes autorisés est ignorée.
- La liste d'hôtes refusés est ignorée.
- Le masque de réseau de l'adresse IP refusé est 9.0.0.0/8.

  Plusieurs masques de réseau peuvent être ajoutés s'il existe plusieurs réseaux intranet et il convient d'ajouter les équivalents IPv6 si le réseau prend en charge à la fois les protocoles IPv4 et IPv6.

Exemple : autoriser l'accès OpenID uniquement aux sociétés example1 et example2

- Pour configurer cet environnement, la règle d'accès par défaut indiquée est **refuser**
- La liste des hôtes non autorisés et des maques de réseau IP est ignorée.
- La liste des expressions régulières pour les hôtes autorisés est :

  ```
  .*\.example1\.com,openid\.example2\.com,openidserver\.example2\.com
  ```

Les identificateurs OpenID de 'example1' se présentent sous la forme `john.example1.com` et le serveur OpenID résolu par les URL d'identité est le suivant :

```
https://www.example1.com/openidProcessing.action
```

Pour l'exemple 2, les identificateurs OpenID ont la forme `openid.example2.com/<example2_screenname>` et se résolvent en une page HTML pointant vers le serveur OpenID :

```
https://api.screenname.example2.com/auth/openidServer
```

La nécessité de cette adresse URL est la raison pour laquelle ces deux noms d'hôte apparaissent dans la liste.

Exemple : autoriser tout nom d'hôte contenant la chaîne .ibm.com

Cet exemple indique des paramètres autorisant un utilisateur à accéder tout nom d'hôte contenant la chaîne .ibm.com.

- Pour configurer cet environnement, sélectionnez un plug-in personnalisé
- La liste d'hôtes autorisés est vérifiée.
- La liste d'hôtes refusés est vérifiée.
- Le plug-in de noeuds finaux dynamiques personnalisés est :

```
package com.tivoli.am.fim.demo.ibmaccessapproval;

import java.net.MalformedURLException;
import java.net.URL;
import java.util.Map;
import java.util.logging.Level;
import java.util.logging.Logger;

import com.tivoli.am.fim.useragent.AccessApproval;
```

```
public class IBMAccessApproval implements AccessApproval {

 final static String CLASS = IBMAccessApproval.class.getName();

 final static Logger _log = Logger.getLogger(CLASS);

 public IBMAccessApproval() {
 }

 public boolean canAccess(Map ctx) {
  String methodName = "canAccess";
  _log.entering(CLASS, methodName, new Object[] { ctx });
  boolean result = false;
  boolean finestLoggable = _log.isLoggable(Level.FINEST);
  try {
   String endpoint = (String) ctx.get(AccessApproval.CTX_ENDPOINT);
   String fedname = (String) ctx
     .get(AccessApproval.CTX_FEDERATION_NAME);
   String fedid = (String) ctx
   .get(AccessApproval.CTX_FEDERATION_ID);

   if (finestLoggable) {
    _log.logp(Level.FINEST, CLASS, methodName, "Fedname: "
      + fedname + " Fedid: " + fedid + " Endpoint: " + endpoint);
   }

   try {
    URL u = new URL(endpoint);
    String hostname = u.getHost();
    if (hostname != null && hostname.indexOf(".ibm.com") > 0) {
     result = true;
    }
   } catch (MalformedURLException e) {
    e.printStackTrace();
   }

  } finally {
   _log.exiting(CLASS, methodName, "" + result);
  }
  return result;
 }
}
```

Extensions OpenID

Extension OpenID Simple Registration Extension

Au cours du processus de connexion, le consommateur peut demander des attributs auprès des fournisseurs d'identité en spécifiant des paramètres additionnels dans le formulaire de connexion. Ces paramètres doivent correspondre aux noms des paramètres décrits dans l'extension OpenID Simple Registration Extension 1.0 ou Attribute Exchange Extension 1.0, selon applicable.L'extension Simple Registration Extension (SREG) est une extension au protocole d'authentification OpenID et prend en charge une simple liste d'informations d'enregistrement utilisateur commun. Pour plus d'informations, voir la documentation OpenID à l'adresse : http://openid.net/specs/openid-simple-registration-extension-1_0.html

```
<form name="openidLoginForm" method="post"
action="https://sp.example.com/FIM/sps/openidsp/openid/login">
<input name="openid.mode" type="hidden"
value="checkid_setup">
<input name="openid.sreg.required" type="hidden"
value="email">
<input name="openid.sreg.optional" type="hidden"
value="fullname,dob">
<input name="openid.sreg.policy_url" type="hidden"
value="https://sp.example.com/privacy_policy.html">
<input name="TARGET" type="hidden"
value="https://sp.example.com/myapp">
<input name="openid_identifier" type="text">
<input value="OpenID Login" type="submit">
</form>
```

Figure 30. Exemple d'extension Simple Registration Extension

Extension OpenID Attribute Exchange

Les fournisseurs d'identité peuvent utiliser des extensions OpenID pour obtenir les attributs utilisateur et les communiquer aux clients.

L'extension d'échange d'attribut fournit aux fournisseurs d'identité la possibilité de communiquer les attributs utilisateur aux clients.

Le protocole AX (Attribute Exchange Extension) peut être étendu pour accommoder plusieurs types d'attributs et des attributs à plusieurs valeurs. Les attributs sont identité par un URI unique et correspondent en général à des informations d'identité personnelles. Pour plus d'informations, voir la documentation OpenID à l'adresse : http://openid.net/specs/openid-attribute-exchange-1_0.html

Le protocole Attribute Exchange Extension fournit une compatibilité stricte avec OpenID 2.0. Vous pouvez utiliser l'une ou les deux extensions en même temps. Utilisez le protocole Attribute Exchange Extension à moins que vous ne deviez être compatible avec une ancienne implémentation OpenID 1.1 qui ne prend en charge que SREG.

En tant qu'administrateur, vous pouvez ajouter un ensemble de paramètres au formulaire de connexion OpenID envoyé au noeud final de connexion.

L'exemple montre un formulaire de connexion avec les conditions requises suivantes :

- Demande l'adresse électronique au fournisseur d'identité
- Demande éventuellement le nom complet, la date de naissance, les amis et groupes.

```
<form name="openidLoginForm" method="post"
action="https://sp.example.com/FIM/sps/openidsp/openid/login">
<input name="openid.mode" type="hidden" value="checkid_setup">
<input name="openid.ax.required" type="hidden" value="axemail">
<input name="openid.ax.if_available" type="hidden"
value="axfullname,axdob,axfriends,axgroups">
<input name="openid.ax.type.axemail" type="hidden"
value="http://axschema.org/contact/email">
<input name="openid.ax.type.axfullname" type="hidden"
value="http://axschema.org/namePerson">
<input name="openid.ax.type.axdob" type="hidden"
value="http://axschema.org/birthDate">
<input name="openid.ax.type.axfriends" type="hidden"
value="http://example.com/myschema/friends">
<input name="openid.ax.count.axfriends" type="hidden"
value="5">
<input name="openid.ax.type.axgroups" type="hidden"
value="http://example.com/myschema/groups">
<input name="openid.ax.count.axgroups" type="hidden"
value="unlimited">
<input name="TARGET" type="hidden"
value="https://sp.example.com/myapp">
<input name="openid_identifier" type="text">
<input value="OpenID Login" type="submit">
</form>
```

Figure 31. Exemple d'extension Attribute Exchange Extension

Remarque : Si aucun chiffre explicite n'est demandé pour un paramètre d'échange d'attribut, la valeur maximale par défaut est 1.

Tivoli Federated Identity Manager envoie des paramètres au fournisseur d'identité lors des demandes `checkid_immediate` et `checkid_setup`. Les messages d'extraction envoyés avec la demande extrait les attributs d'identité personnelle de l'utilisateur. Pour plus d'informations sur les messages d'extraction, voir la documentation OpenID : http://openid.net/specs/openid-attribute-exchange-1_0.html#fetch

Paramètres de demande d'extraction Attribute Exchange Extension

Attribute Exchange Extension prend en charge un modèle d'information qui combine un identificateur de sujet, un identificateur de type d'attribut et une valeur. L'inclusion d'autres paramètres relie la demande d'extraction Attribute Exchange à une requête d'authentification standard. Pour permettre au client d'extraire des informations à partir du fournisseur d'identité, spécifiez les paramètres de zone de formulaire suivants dans le formulaire de connexion.

openid.ax.required
: Extrait les attributs requis à partir du fournisseur d'identité. La valeur représente une liste d'alias, qui sont des étiquettes représentant des attributs individuels au niveau du fournisseur d'identité. Reliez chaque alias sur un URI qui identifie l'attribut dans un paramètre `openid.ax.type.`*`alias`* distinct. *(facultatif)*

openid.ax.if_available
: Extrait un attribut disponible à partir du fournisseur d'identité. La valeur a les mêmes exigences que `openid.ax.required`. *(facultatif)*

Remarque : Vous devez spécifier `openid.ax.required` ou `openid.ax.if_available` dans la reqête. Chaque alias d'attribut demandé doit avoir un paramètre `openid.ax.type.`*`alias`* associé.

openid.ax.type.*alias*
Relie l'alias à un URI définissant la signification de l'attribut. Vous devez spécifier un paramètre pour chaque alias défini dans `openid.ax.required` ou `openid.ax.if_available`. *(facultatif)*

Un grand nombre d'attributs classiques ont défini des URI de type à http://www.axschema.org/types/

openid.ax.sendalways
Inclut les informations Attribute Exchange Extension OpenID dans les demandes d'authentification au niveau du fournisseur d'identité. L'environnement exécution du client envoie les informations de requête Attribute Exchange Extension si le fournisseur d'identité prend en charge Attribute Exchange Extension avec XRDS. La valeur par défaut est false. *(facultatif)*

Paramètres de réponse d'extraction Attribute Exchange Extension

Une fois les droits d'accès accordés à un fournisseur d'identité, un message de réponse d'extraction fournit les informations dans les paramètres de demande d'extraction. Les paramètres de réponse d'extraction facultatifs suivants spécifient les attributs personnels extraits à partir du fournisseur d'identité.

openid.ax.type.*alias*
Spécifie le type d'URI pour l'attribut d'extraction identifié par l'alias. *(facultatif)*

openid.ax.count.*alias*
Renvoie le nombre de valeurs spécifiées pour l'attribut correspondant à l'alias. Si vous ne spécifiez pas de valeur spécifique, une seule valeur est renvoyée.

openid.ax.value.*alias*
Affecte une valeur spécifiée pour l'attribut correspondant à l'alias. *(facultatif)*

openid.ax.value.*alias***.number**
Affecte une valeur spécifiée pour l'attribut correspondant à l'alias. Ce paramètre est requis si `openid.ax.count.`*`alias`* est envoyé et qu'au moins une valeur est configuré pour l'attribut associé. Il doit y avoir un paramètre distinct pour chaque valeur de l'alias, avec des nombres incrémentiels.

Extension de règle d'authentification de fournisseur OpenID

Lorsqu'un utilisateur lance l'authentification à partir d'une partie de confiance avec un identificateur OpenID, la partie de confiance demande le fournisseur d'identité pour authentifier l'utilisateur.

L'extension PAPE (Provider Authentication Policy Extension) OpenID est un mécanisme qui autorise une partie de confiance à :

- Demander aux fournisseurs d'identité d'utiliser des règles d'authentification spécifiques lors de l'authentification d'un utilisateur.

- Demander au fournisseur d'identité d'informer la partie de confiance des règles d'authentification utilisées lors de l'authentification.
- Demander au fournisseur d'identité de communiquer les niveaux d'authentification tels que défini dans les ensembles de niveaux d'assurance personnalisés demandés.

Utilisez la console d'administration pour configurer l'extension PAPE OpenID. Selon votre rôle dans la fédération, certains paramètres sont disponibles dans le panneau de propriétés de la configuration.

Remarque : Les paramètres PAPE peuvent uniquement être configurés APRES la création d'une fédération. Utilisez le panneau de propriétés de fédération pour indiquer les paramètres de la configuration.

Implémentation PAPE de partie de confiance

Utilisez le panneau de propriétés de configuration de la partie de confiance pour activer PAPE. Une fois que le paramètre est activé, les attributs PAPE indiqués sont envoyés au fournisseur d'identité dans la demande d'authentification. Lorsqu'une partie de confiance envoie la demande d'authentification avec les attributs PAPE indiqués, le fournisseur d'identité envoie une réponse. La réponse indique quelles exigences sont remplies et lesquelles ne le sont pas. Grâce à la réponse, la partie de confiance peut déterminer s'il faut authentifier l'utilisateur.

Spécifiez les paramètres suivants dans le panneau de propriétés de configuration de la partie de confiance :

Mode d'application

- Strict

  Indique qu'un utilisateur n'est pas authentifié si les exigences PAPE ne sont pas remplies.
- Lenient

  Indique qu'un utilisateur est authentifié même si les exigences PAPE ne sont pas remplies. La règle de mappage utilisée dans la fédération accède aux informations de réponse. La réponse indique quelles exigences sont remplies et lesquelles ne le sont pas. Ce paramètre permet à l'auteur de la règle de mappage de choisir s'il souhaite connecter l'utilisateur en se basant sur ces informations.La règle de mappage fournit une autorisation plus limitée.

Règles d'authentification

Indique un ensemble d'URI de règles d'authentification. Les URI représentent les règles d'authentification que le fournisseur d'identité doit respecter lors de l'authentification d'un utilisateur. Si plusieurs règles sont requises, le fournisseur d'identité doit en respecter le plus grand nombre possible. Le fournisseur d'identité indique ensuite quelles règles d'authentification ont été respectées dans la réponse.

Age maximal de l'authentification

Indique la période pendant laquelle l'utilisateur doit avoir été authentifié. Si cette période a expiré, le fournisseur d'identité doit authentifier de nouveau l'utilisateur.

Niveaux d'assurance préférés

Indique une liste ordonnée des URI préférés d'espace de nom du niveau d'assurance. Les valeurs d'espace de nom du niveau d'assurance déterminent le niveau du certificat contenu dans l'authentification de

l'utilisateur. Les parties de confiance demandent des informations concernant ces espaces de nom du niveau d'assurance provenant du fournisseur d'identité.

Implémentation PAPE du fournisseur d'identité

Le panneau de propriétés de configuration du fournisseur d'identité indique les conditions sous lesquelles un utilisateur doit s'authentifier.

Remarque : Si vous comptez utiliser la gestion de cookie WebSEAL avec l'implémentation OpenID PAPE, assurez-vous que la liste des cookies gérés n'inclut pas le cookie de session WebSphere. Voir «Configuration de WebSEAL pour gérer les cookies», à la page 430.

Spécifiez les paramètres suivants dans le panneau de propriétés de configuration du fournisseur d'identité :

Authentification imposée à tout âge d'authentification maximal PAPE demandé
Ce paramètre indique qu'un utilisateur doit toujours s'authentifier. Si cette option est sélectionnée, la zone Maximum authentication age allowable clock skew (Décalage horloge maximal autorisé de l'âge d'authentification) est désactivée.

Décalage horloge maximal autorisé de l'âge d'authentification
Lorsqu'un âge d'authentification maximum est demandé par un fournisseur de services au cours d'une connexion unique, la règle de mappage du fournisseur d'identité doit renvoyer la dernière heure d'authentification de l'utilisateur. Ce paramètre permet de calculer le décalage d'horloge entre :

- la dernière heure d'authentification retournée par la règle de mappage du fournisseur d'identité
- l'horloge du fournisseur d'identité

Généralement, l'heure de décalage est un petit nombre, mais qui peut prendre en compte les différences entre la machine du point de contact et la machine d'exécution.

Formulaire de configuration du fournisseur d'identité

Tivoli Federated Identity Manager comprend un assistant qui vous guidera tout au long de la configuration des fédérations OpenID. L'assistant vous invite à renseigner les propriétés nécessaires pour votre déploiement. Ce formulaire décrit les propriétés.

Ce formulaire vous permet de planifier vos propriétés et vous pouvez vous y référer lors de l'exécution de l'assistant.

Nom de la fédération
Le nom peut correspondre à n'importe quelle chaîne de caractères. Par exemple, `openid-idp`. Cette zone est obligatoire.

Rôle de la fédération
Votre rôle est *Fournisseur d'identité*.

Nom de la société
Nom de la société qui crée la fédération. La valeur peut correspondre à n'importe quelle chaîne de caractères. Vous pouvez utiliser des espaces. Cette zone est obligatoire.

Protocole de la fédération
OpenID.

Serveur point de contact
Adresse URL du serveur qui agit en tant que point de contact initial pour les requêtes entrantes. L'adresse est constituée d'une spécification de protocole, du nom d'hôte du serveur et (en option) d'un numéro de port. Lorsque WebSEAL est le serveur point de contact, la jonction WebSEAL est spécifiée.

Exemple de valeur :

```
https://webseald.example.com/FIM
```

Remarque : Pour le support d'OpenID, le serveur point de contact doit utiliser le protocole SSL (Secure Socket Layer). L'adresse URL spécifiée doit être du type `https://`.

Expiration d'association (secondes)
Définit la durée de vie de l'indicateur d'association. Ce fournisseur d'identité contrôle cette valeur. Entrez un nombre positif. La valeur par défaut est de 3 600 secondes.

Délai d'expiration de réponse de l'élément Nonce (secondes)
Indique le nombre de secondes restant à un correspondant associé fonctionnant sans association établie avant de devoir exécuter la demande `check_authentication`. Si ce nombre est paramétré sur un nombre positif, cette option empêche de refaire un `contrôle_d_authentification`. Cette restriction s'applique aux clients disposant de parties de confiance incapables de créer ou de stocker des associations. La valeur par défaut est 30 secondes.

Générateur d'ID
Indique quel générateur d'ID crée une valeur remplaçant `@ID@` dans l'URL d'identité. Des générateurs d'ID différents créent des valeurs différentes pour `@ID@`.

Structure de l'URL d'identité OpenID

Représente l'expression régulière à laquelle les URL d'identité sont comparés pour la fédération. Tivoli Federated Identity Manager remplace la partie `@ID@`. La valeur par défaut est l'URL du nom d'hôte de protocole de connexion unique fournie par l'assistant d'installation.

Par exemple, si vous avez défini le serveur de point de contact suivant dans l'assistant :

```
https://webseald.example.com/FIM
```

la structure d'URL d'identité par défaut est la suivante :

```
https://webseald.example.com/@ID@
```

URL de configuration d'utilisateur
Spécifie l'URL envoyée en réponse à une requête `checkid_immediate` provenant d'un consommateur. L'URL est utilisée lorsque le fournisseur d'identité ne peut pas déterminer si un propriétaire possède une URL d'identité précise.

L'URL par défaut est l'URL du serveur point de contact que vous avez définie sur le panneau Serveur point de contact.
A titre d'exemple, lorsque vous avez précédemment spécifié, dans l'assistant, le serveur point de contact suivant :

```
https://webseald.example.com/FIM
```

l'URL de configuration d'utilisateur par défaut est :

```
https://webseald.example.com/
```

Gestionnaire de sites de confiance
Sélectionne la classe d'implémentation pour un gestionnaire de sites fiable. L'implémentation contient des données concernant les décisions d'accord d'authentification prises par un utilisateur lors des authentifications OpenID.

Prise en charge de l'identificateur OP
Indique si l'option `identifier_select` est prise en charge lorsqu'un consommateur lance une connexion unique. Utilisez cette option si un fournisseur d'identité utilise XRDS. Si vous ne sélectionne pas cette option, toutes les autres options de `identifier_select` sont désactivées.

Modèle d'identificateur OP demandé créé
Spécifie une URL valide qui doit contenir la chaîne `@ID@`. Elle active une partie de confiance qui peut lancer une connexion unique avec un identificateur demandé paramétré sur `identifier_select`.

L'URL par défaut est l'URL du serveur de point de contact définie lors de la configuration de la fédération.

Par exemple, si l'URL de point de contact a été définie comme :

```
https://webseal.example.com/FIM
```

le modèle d'identificateur demandé généré via OP par défaut est le suivant :

```
https://webseal.example.com/@ID@
```

Options de reconnaissance de la partie de confiance
Propose deux options :

Exécuter une reconnaissance RP
Indique s'il faut tenter la reconnaissance de la partie de confiance. Si vous ne sélectionnez pas cette option, toutes les autres options de reconnaissance de la partie de confiance sont désactivées.

Réussite de la reconnaissance RP obligatoire
Spécifie si Tivoli Federated Identity Manager est interrompu avec une erreur lorsqu'il ne peut pas exécuter la reconnaissance de la partie de confiance pour le fournisseur d'identité. Cette option s'applique uniquement si vous activez Perform RP Discovery (Exécuter la reconnaissance de la partie de confiance).

Délai d'expiration de la mise en cache de la reconnaissance RP
Détermine le nombre de secondes nécessaire pour mettre en mémoire cache les informations reconnues concernant les parties de confiance. Si vous saisissez une valeur inférieure à zéro, les informations ne sont jamais mises en mémoire cache.

Protocoles serveur OpenID autorisés
Définit les protocoles autorisés des serveurs OpenID avec lesquels l'agent d'utilisateur autorise l'établissement d'une connexion. Vous pouvez choisir l'une des valeurs ou les deux. Il est généralement recommandé de définir ce paramètre uniquement sur HTTPS.

Sélectionnez l'une ou l'autre des options suivantes, ou les deux :

- HTTPS

- HTTP

Délai d'attente de connexion HTTP
Spécifie le nombre de secondes avant l'expiration du délai d'attente durant les communications avec le client HTTP. Entrez un nombre positif. Si vous entrez zéro (0), le logiciel utilise les valeurs par défaut Java pour les objets URLConnection. La valeur par défaut est 30 secondes.

Fichier de clés
Indique le fichier de clés utilisé pour valider les certificats des noeuds finaux SSL au cours des communications pour la reconnaissance du correspondant associé. Ce fichier de clés doit contenir les certificats de signataire de droits certifiés de tous les correspondants associés pour lesquels la reconnaissance du correspondant associé doit être effectuée.

Règles de connexion agent d'utilisateur
Spécifie les règles de connexion de l'agent utilisateur. Vous devez sélectionner l'une des options suivantes.

- Autoriser l'accès aux hôtes OpenID par défaut

  L'hôte est contacté, à moins qu'il ne soit compris dans la liste de refus. Ce paramètre est plus tolérant et permet généralement aux utilisateurs de se connecter à partir d'un serveur OpenID légitime sur Internet.
- Refuser l'accès aux hôtes OpenID par défaut

  Seuls les hôtes de la liste d'autorisation sont accessibles pour l'agent d'utilisateur. Ce paramètre est restrictif et chaque URL d'identité OpenID et chaque serveur dont vous souhaitez autoriser l'accès doit figurer dans les listes d'autorisation.

Pour passer en vue les différents choix de règles, consultez la rubrique «Règles relatives à l'agent d'utilisateur», à la page 303.

Expressions régulières de nom d'hôte autorisées
Indique une liste d'expressions régulières identifiant les noms d'hôtes auxquels l'agent d'utilisateur peut demander à accéder. Entrez une chaîne par ligne.

Par exemple :

```
.*\.ibm\.com
```

La valeur est facultative.

Adresses IP autorisées / Masques de réseau
Indique les adresses IP ou les masques de réseau auxquels l'agent d'utilisateur peut demander à accéder. Utilisez des expressions régulières, et entrez une chaîne par ligne. Entrez une chaîne par ligne.

Par exemple :

```
10.1.1.0/24
192.168.0.10
```

Cette valeur est facultative.

Module d'autorisation d'accès aux noeuds finaux dynamiques
Spécifie une liste de plug-ins d'accès de point final dynamiques personnalisés. Les plug-ins peuvent vérifier les listes externes d'hôtes dignes de confiance ou non. Ce paramètre est utilisé en plus de la configuration des règles de connexion agent d'utilisateur. Si l'option est défiie sur l'approbation d'accès par défaut, les paramètres de configuration spécifiés sous les règles de connexion agent d'utilisateur sont utilisés.

Expressions régulières de nom d'hôte refusées

Indique les noms d'hôte auxquels l'agent d'utilisateur ne peut pas demander à accéder. Utilisez des expressions régulières, et entrez une chaîne par ligne.

- Lorsque l'option Règles de connexion agent d'utilisateur est paramétrée de manière à refuser l'accès aux hôtes OpenID par défaut, cette propriété n'est pas utilisée.
- Lorsque l'option Règles de connexion agent d'utilisateur est paramétrée de manière à autoriser l'accès aux hôtes OpenID par défaut, l'utilisation de cette propriété est facultative.

Par exemple :

```
.*\.example\.com
.*\.example2\.com
```

Adresses IP refusées / masques de réseau

Indique une liste d'expressions régulières identifiant les adresses IP ou les masques de réseau auxquels l'agent d'utilisateur ne peut pas demander à accéder. Entrez une chaîne par ligne.

- Lorsque l'option Règles de connexion agent d'utilisateur est paramétrée de manière à refuser l'accès aux hôtes OpenID par défaut, cette propriété n'est pas utilisée.
- Lorsque l'option Règles de connexion agent d'utilisateur est paramétrée de manière à autoriser l'accès aux hôtes OpenID par défaut, l'utilisation de cette propriété est facultative.

Par exemple :

```
11.12.13.0/24
192.168.0.10
```

Options de mappage d'identité

Sélectionnez une des options suivantes :

- **Utilisez des règles de mappage XSLT ou Javascript pour le mappage d'identité**

  Sélectionnez cette option lorsque vous créez une règle de mappage XSLT ou Javascript qui fournit des règles de mappage d'identité.

  Tivoli Federated Identity Manager fournit un exemple de fichier de règles de mappage d'identité destiné aux fédérations de fournisseurs d'identité OpenID :

  /répertoire_installation/examples/ip_openid.xsl

- **Utilisez Tivoli Directory Integrator pour le mappage**

  Sélectionnez cette option lorsque vous avez une chaîne d'assemblage Tivoli Directory Integrator pour le mappage d'identité requis par votre fédération OpenID.

- **Utiliser une instance de modèle de mappage personnalisé**

  Sélectionnez cette option lorsque vous avez un module de service d'accréditation personnalisé pour le mappage d'identité requis par votre fédération OpenID.

Tableau 100. Formulaire pour les propriétés d'identification d'une fédération

Propriété à spécifier	Votre valeur
Nom de la fédération	
Rôle	fournisseur d'identité
Nom de la société	

Tableau 100. Formulaire pour les propriétés d'identification d'une fédération (suite)

Propriété à spécifier	**Votre valeur**
Protocole de fédération	OpenID
Serveur point de contact	
Délai d'expiration d'association	Valeur par défaut : 3 600 secondes.
Délai d'expiration de réponse de l'élément Nonce (secondes)	Valeur par défaut : 30 secondes
Générateur d'ID (génère la valeur @ID@)	
Structure de l'URL d'identité OpenID	
URL de configuration d'utilisateur	
Prise en charge de l'identificateur OP	Modèle d'identificateur OP demandé créé
Modèle d'identificateur OP demandé créé	
Exécuter une reconnaissance RP	
Réussite de la reconnaissance RP obligatoire	
Délai d'expiration de la mise en cache de la reconnaissance RP	
Protocoles serveur OpenID autorisés	
Délai d'attente de connexion HTTP	
Fichier de clés	
Règles de connexion agent d'utilisateur	
Expressions régulières de nom d'hôte autorisées	
Adresses IP autorisées / Masques de réseau	
Module d'autorisation d'accès aux noeuds finaux dynamiques	
Expressions régulières de nom d'hôte refusées	
Adresses IP / Masques de réseau refusés	
Options de mappage d'identité	Sélectionnez l'une des options suivantes : • Utiliser XSLT ou JavaScript pour le mappage d'identité • Utiliser Tivoli Directory Integrator pour le mappage • Utiliser une instance de modèle de mappage personnalisé

Tableau 100. Formulaire pour les propriétés d'identification d'une fédération (suite)

Propriété à spécifier	Votre valeur
Fichier de règles de mappage d'identité	Si vous utilisez XSLT ou JavaScript pour le mappage d'identité, spécifiez le nom du fichier de règle de mappage :
Module de mappage personnalisé	Si vous utilisez un module de mappage personnalisé, notez le nom du module :

Formulaire de configuration du consommateur

Tivoli Federated Identity Manager comprend un assistant qui vous guidera tout au long de la configuration des fédérations OpenID. L'assistant vous invite à renseigner les propriétés nécessaires pour votre déploiement. Ce formulaire décrit les propriétés.

Ce formulaire vous permet de planifier vos propriétés et vous pouvez vous y référer lors de l'exécution de l'assistant.

Nom de la fédération
Chaîne arbitraire choisie pour dénommer cette fédération. Par exemple, `openid-consumer`.

Rôle de la fédération
Votre rôle est *Fournisseur de services*. Vous devez sélectionner l'option *fournisseur de services* lors de la configuration du rôle de consommateur.

Nom de la société
Valeur au format chaîne désignant le nom de la société. Vous pouvez éventuellement fournir des informations de contact supplémentaires.

Protocole de la fédération
OpenID.

Serveur point de contact
Adresse URL du serveur qui agit en tant que point de contact initial pour les requêtes entrantes. L'adresse est constituée d'une spécification de protocole, du nom d'hôte du serveur et (en option) d'un numéro de port. Lorsque WebSEAL est le serveur point de contact, la jonction WebSEAL est spécifiée. Exemple de valeur :

```
https://webseald.example.com/FIM
```

Remarque : Pour le support d'OpenID, le serveur point de contact doit utiliser le protocole SSL (Secure Socket Layer). L'adresse URL spécifiée doit être du type `https://`.

Certificat racine digne de confiance annoncé
Cette valeur est une adresse URL qui constitue la *racine* des URL accréditées pour la fédération. Elle renvoie par défaut à l'URL de base de la fédération, qui représente le chemin d'accès au nom d'hôte du service de protocole de connexion unique. Lorsque le numéro de port ne correspond pas à la valeur par défaut, la valeur du port est également incluse. La valeur doit se terminer par une barre oblique (/).

Cette valeur doit être une URL parente du noeud final délégué pour le renvoi du nom de connexion. Elle est utilisée en tant que paramètre openid.trust_root dans la requête de connexion unique adressée au fournisseur d'identité.

A titre d'exemple, lorsque vous avez précédemment spécifié, dans l'assistant, le serveur point de contact suivant :

```
https://webseald.example2.com/FIM
```

le certificat racine digne de confiance par défaut est :

```
https://webseald.example2.com/
```

Activer le protocole Yadis
Indique s'il faut effectuer la reconnaissance Yadis. Pour obtenir les meilleures pratiques, choisissez de désactiver cette option.

Activer des identificateurs XRI
Indique s'il faut résoudre les identificateurs demandés URL ou XRI. Si vous ne sélectionnez pas d'option, le logiciel utilise uniquement les identificateurs demandés URL.

Proxys XRI
Indique une liste d'URL permettant de résoudre les identificateurs XRI. L'URL doit contenir la macro `@XRI@`.

Expiration des informations reconnues
Indique le temps pendant lequel la mémoire cache stocke les informations reconnues. Si vous n'entrez pas de nombre positif, le cache est désactivé et la reconnaissance est effectuée à chaque connexion.

Délai de décalage de réponse de l'élément Nonce
Indique une valeur, en secondes, utilisée pour valider la réponse de l'élément Nonce provenant des fournisseurs d'identité OpenID 2.0. La validation est uniquement assurée si ce décalage est un nombre positif. La validation est assurée en prenant la durée de la réponse de l'élément Nonce et le décalage configuré de la réponse de l'élément Nonce. Si le nombre de secondes n'est pas compris dans cette plage, la réponse d'authentification est refusée. Si le nombre de secondes est compris dans cette plage, une mémoire cache de la réponse de l'élément Nonce est contrôlée. Le contrôle permet de s'assurer que la réponse d'authentification ne correspond pas à une nouvelle lecture. Lorsque la validation est effectuée avec succès, la réponse de l'élément Nonce est ajoutée à la mémoire cache de la réponse de l'élément Nonce tant qu'elle est comprise dans la période du décalage. La réponse de l'élément Nonce est ajoutée à la mémoire cache de l'élément Nonce afin de vérifier que les réponses d'authentification à venir ne sont pas de nouvelles lectures.

Protocoles serveur OpenID autorisés
Cette valeur représente l'ensemble des protocoles autorisés sur les serveurs OpenID pour lesquels l'agent d'utilisateur autorise les connexions. Il est généralement recommandé de définir ce paramètre uniquement sur HTTPS.

Sélectionnez l'une ou l'autre des options suivantes, ou les deux :

- HTTPS
- HTTP

La valeur HTTPS est configurée par défaut. Vous devez sélectionner au moins un protocole.

Délai d'attente de connexion HTTP
Cette valeur spécifié le délai d'attente de communication sur le client HTTP. Cette valeur doit être un entier positif valide. La valeur maximale est définie par la valeur entière la plus élevée. La valeur zéro (0) signifie que les valeurs Java par défaut doivent être appliquées aux objets URLConnection. La valeur par défaut est 30 secondes.

Fichier de clés
Cette valeur correspond au nom du fichier de clés qui a été précédemment configuré dans le service de clés de Tivoli Federated Identity Manager. Le magasin de clés doit contenir les certificats de signataires émis par l'autorité de certification uniquement.

Le client HTTP du consommateur utilise ce fichier de clés lors de la communication avec les fournisseurs d'identité compatibles avec SSL. Le magasin de clés est utilisé pour déterminer si l'hôte avec lequel la connexion doit être établie est digne de confiance. Cette vérification a lieu lors du traitement des messages `associate` et `check_authentication`.

Valeur par défaut :

```
DefaultTrustedKeyStore
```

Règles de connexion agent d'utilisateur
Cette valeur définir les règles des connexions établies par l'agent d'utilisateur. Vous devez sélectionner l'une des options suivantes.

- Autoriser l'accès aux hôtes OpenID par défaut
- Refuser l'accès aux hôtes OpenID par défaut

Pour passer en vue les différents choix de règles, consultez la rubrique «Règles relatives à l'agent d'utilisateur», à la page 303.

Expressions régulières de nom d'hôte autorisées
Liste des expressions régulières qui spécifient les noms d'hôte auxquels l'agent d'utilisateur peut demander l'accès. Entrez une chaîne par ligne. Par exemple :

```
.*\.ibm\.com
```

Cette valeur est facultative.

Adresses IP autorisées / Masques de réseau
Liste des expressions régulières qui spécifient les adresses IP et les masques de réseau auxquels l'agent d'utilisateur peut demander l'accès. Entrez une chaîne par ligne. Par exemple :

```
10.1.1.0/24
192.168.0.10
```

Cette valeur est facultative.

Expressions régulières de nom d'hôte refusées
Liste des expressions régulières qui spécifient les noms d'hôte auxquels l'agent d'utilisateur ne peut pas demander l'accès. Entrez une chaîne par ligne. Par exemple :

```
.*\.example\.com
.*\.example2\.com
```

- Lorsque le paramètre Règles de connexion agent d'utilisateur est défini sur **Refuser l'accès aux hôtes OpenID par défaut**, cette propriété est ignorée.

- Lorsque le paramètre Règles de connexion agent d'utilisateur est défini sur **Autoriser l'accès aux hôtes OpenID par défaut**, l'usage de cette propriété est facultatif.

Adresses IP / Masques de réseau refusés
Liste des expressions régulières qui spécifient les adresses IP et les masques de réseau auxquels l'agent d'utilisateur ne peut pas demander l'accès. Entrez une chaîne par ligne. Par exemple :

```
11.12.13.0/24
192.168.0.10
```

- Lorsque le paramètre Règles de connexion agent d'utilisateur est défini sur **Refuser l'accès aux hôtes OpenID par défaut**, cette propriété est ignorée.
- Lorsque le paramètre Règles de connexion agent d'utilisateur est défini sur **Autoriser l'accès aux hôtes OpenID par défaut**, l'usage de cette propriété est facultatif.

Module d'autorisation d'accès aux noeuds finaux dynamiques
Spécifie une liste de plug-ins d'accès de point final dynamiques personnalisés. Les plug-ins peuvent vérifier les listes externes d'hôtes dignes de confiance ou non. Ce paramètre est utilisé en plus de la configuration des règles de connexion agent d'utilisateur. Si l'option est défiie sur l'approbation d'accès par défaut, les paramètres de configuration spécifiés sous les règles de connexion agent d'utilisateur sont utilisés.

Options de mappage d'identité
Vous êtes invité à sélectionner l'une des options suivantes :

- Utilisez des règles de mappage XSLT ou Javascript pour le mappage d'identité

  Sélectionnez cette option lorsque vous avez créé une règle de mappage XSLTfile ou Javascript qui fournit des règles de mappage d'identité.

  Tivoli Federated Identity Manager fournit un exemple de fichier de règles de mappage d'identité destiné aux fédérations de consommateurs OpenID :

  `/répertoire_installation/examples/sp_openid.xsl`
- Utiliser Tivoli Directory Integrator pour le mappage

  Sélectionnez cette option lorsque vous avez préalablement configuré une chaîne d'assemblage Tivoli Directory Integrator pour le mappage d'identité requis par votre fédération OpenID.
- Utiliser une instance de modèle de mappage personnalisé

  Sélectionnez cette option lorsque vous avez écrit et déployé un module de service d'accréditation personnalisé pour le mappage d'identité requis par votre fédération OpenID.

Tableau 101. Propriétés de configuration de consommateur OpenID

Propriété	Votre valeur
Nom de la fédération	
Rôle	fournisseur de services
Nom de la société	
Protocole de fédération	OpenID
URL de serveur point de contact	

Tableau 101. Propriétés de configuration de consommateur OpenID (suite)

Propriété	Votre valeur
Certificat racine digne de confiance annoncé	
Activer le protocole Yadis	
Activer des identificateurs XRI	
Proxys XRI	
Expiration des informations reconnues	
Délai de décalage de réponse de l'élément Nonce	
Protocoles serveur OpenID autorisés	HTTPS, HTTP ou les deux
Délai d'attente de connexion HTTP (secondes)	Valeur par défaut : 30 secondes
Fichier de clés	
Règles de connexion agent d'utilisateur	
Expressions régulières de nom d'hôte autorisées	
Adresses IP autorisées / Masques de réseau	
Expressions régulières de nom d'hôte refusées	
Adresses IP / Masques de réseau refusés	
Module d'autorisation d'accès aux noeuds finaux dynamiques	
Options de mappage d'identité	Sélectionnez l'une des options suivantes : • Utiliser XSL pour le mappage d'identité • Utiliser Tivoli Directory Integrator pour le mappage • Utiliser une instance de modèle de mappage personnalisé
Fichier de règles de mappage d'identité	Si vous utilisez XSL pour le mappage d'identité, spécifiez le nom de fichier de règle de mappage suivant :
Module de mappage personnalisé	Si vous utilisez un module de mappage personnalisé, notez le nom du module :

Chapitre 22. Configuration de OpenID

Vérification des dépendances OpenID

Avant de commencer

Avant d'utiliser l'assistant de création de fédération, assurez-vous que les conditions relatives aux dépendances OpenID sont satisfaites. Accomplissez les activités de planification requises en passant en revue le contenu de la section relative à la planification.

Procédure

1. Déterminez votre stratégie de mappage d'identité
   - Si vous utilisez un fichier de règles de mappage, assurez-vous que les règles de mappage XSLT ou Jacascript nécessaires ont été inclus afin de répondre aux exigences de votre déploiement.
   - Si vous utilisez une chaîne d'assemblage de Tivoli Directory Integrator, assurez-vous que celle-ci a été construite.
   - Si vous utilisez un module de mappage personnalisé, assurez-vous que ce module a été développé et testé.
2. Assurez-vous que vous avez établi les règles de l'agent d'utilisateur pour le consommateur et le fournisseur d'identité.
3. renseignez le formulaire de la fédération. Procédez à l'une des actions suivantes :
   - «Formulaire de configuration du fournisseur d'identité», à la page 312
   - «Formulaire de configuration du consommateur», à la page 318

Configuration d'une fédération OpenID

Utilisez l'assistant de fédération pour créer et configurer une fédération OpenID.

Avant de commencer

Assurez-vous que vous avez préparé les informations de configuration avant de créer la fédération au moyen de l'assistant.

Pourquoi et quand exécuter cette tâche

Pour utiliser l'assistant de fédération afin de créer et configurer une fédération OpenID, procédez comme suit :

Procédure

1. Connectez-vous à Integrated Solutions Console et cliquez sur **Tivoli Federated Identity Manager → Configurer la connexion unique fédérée → Fédérations**. Les portlets IBM Domaines en cours et Fédérations apparaissent. Le portlet Fédérations affiche plusieurs boutons d'action.
2. Cliquez sur **Créer**. L'assistant de fédération démarre. L'assistant affiche une série de panneaux de configuration.

3. Utilisez votre formulaire complété afin d'indiquer des valeurs dans chaque panneau. Indiquez les valeurs nécessaires et cliquez sur **Suivant** pour poursuivre sur le panneau suivant. Si vous avez besoin de revenir en arrière pour ajuster un paramètre de configuration, cliquez sur **Précédent**. Pour obtenir des informations sur des zones spécifiques, affichez l'aide en ligne.
   a. La première série de panneaux vous demande d'indiquer les paramètres relatifs au nom, au rôle et serveur point de contact de la fédération.
   b. Puis, le panneau de configuration OpenID vous invite à indiquer les valeurs requises pour un fournisseur d'identité ou un consommateur OpenID.
   c. La dernière série de panneaux vous invite à indiquer les paramètres de configuration du mappage d'identité.

   Lorsque vous avez terminé d'entrer les paramètres de configuration, le panneau Récapitulatif s'affiche.
4. Vérifiez que les paramètres de configuration sont corrects, puis cliquez sur **Terminer**. Le portlet Création de fédération terminée s'affiche.

Que faire ensuite

Configuration d'un serveur point de contact WebSEAL pour une fédération Open ID

Si vous envisagez d'utiliser WebSEAL en tant que serveur point de contact, vous devez le configurer pour la fédération OpenID.

Avant de commencer

Le portlet Création de fédération terminée comporte un bouton qui vous permet d'obtenir un utilitaire de configuration.

Pourquoi et quand exécuter cette tâche

Vous devez obtenir l'utilitaire, puis l'exécuter. Procédez comme suit :

Procédure

1. Cliquez sur **Télécharger l'outil de configuration Tivoli Access Manager**.
2. Enregistrez l'outil de configuration sur le système de fichiers de l'ordinateur hébergeant le serveur WebSEAL.
3. Revenez à la console de gestion et cliquez sur **Terminé** pour revenir au panneau Fédérations.
4. Démarrez l'outil de configuration depuis une ligne de commande. La syntaxe est la suivante :

   ```
   java -jar /rép_téléchargement/tfimcfg.jar -cfgfile webseald-nom_instance.conf
    -action tamconfig
   ```

   Vous aurez besoin de l'ID (par défaut : sec_master) et du mot de passe de l'utilisateur d'administration Tivoli Access Manager. L'utilitaire configure les noeuds finals sur le serveur WebSEAL, crée une jonction WebSEAL, relie les listes de contrôle d'accès adaptées et active les méthodes d'authentification adéquates.

Exemple

Par exemple, lorsque vous avez mis le fichier tfimcfg.jar dans le répertoire `/tmp` et que le nom de l'instance WebSEAL est `default`, la commande (spécifiée sur une ligne ininterrompue) est la suivante :

```
java -jar /tmp/tfimcfg.jar
   -cfgfile /<chemin_qualifié_complet>/webseald-default
   -action tamconfig
```

Pour plus d'informations, accédez à l'adresse suivante :

- Annexe A, «Référence de tfimcfg», à la page 533

Que faire ensuite

Configuration de WebSphere en tant que serveur point de contact

Tivoli Federated Identity Manager est configuré par défaut pour utiliser Tivoli Access Manager WebSEAL en tant que serveur point de contact. Pour configurer WebSphere en tant que serveur point de contact, vous devez procéder à une modification de la configuration.

Procédure

1. Connectez-vous à la console d'administration.
2. Cliquez sur Tivoli Federated Identity Manager > Gestion de la configuration > Point de contact
3. Sélectionnez **WebSphere**
4. Cliquez sur **Activer**.

Résultats

Le serveur WebSphere est désormais configuré en tant que point de contact.

Configuration des pages de connexion

Lors de la configuration d'un serveur point de contact, il convient de configurer les informations figurant sur les pages de connexion.

- Les consommateurs doivent fournir un formulaire de connexion destinés à être présentés à l'utilisateur final.

  Les administrateurs qui utilisent WebSEAL en tant que serveur point de contact peuvent choisir de modifier la page login.html par défaut de WebSEAL.
- Les fournisseurs d'identité doivent fournir des informations de reconnaissance à l'aide de la reconnaissance HTML ou Yadis. Les informations de reconnaissance sont fournies dans l'URL d'identité OpenID de l'utilisateur ou l'URL d'identificateur de fournisseur d'identité, ou les deux.

Chapitre 23. Référence OpenID

Algorithmes et modes de transport pris en charge

Tivoli Federated Identity Manager prend en charge les spécifications OpenID pour le type de session à secret partagé (association) :

- OpenID 1.1
  - Texte en clair
  - DH-SHA1

  Pour des raisons de sécurité, le support (consommateur) du fournisseur de services Tivoli Federated Identity Manager pour OpenID 1.1 émet uniquement des demandes de session de type DH-SHA1.
- OpenID 2.0
  - DH-SHA256
  - DH-SHA1
  - no-encryption

  Le consommateur Tivoli Federated Identity Manager tente le type DH-SHA256 par défaut.

  Lorsqu'un fournisseur d'identité renvoie une erreur indiquant qu'un type de session demandé est non pris en charge, le fournisseur d'identité peut établir quels types de session sont pris en charge. Dans ce cas, le consommateurTivoli Federated Identity Manager tente d'établir le type de session suggéré.

  Remarque : Le consommateur Tivoli Federated Identity Manager tente d'utiliser le type 'no-encryption' uniquement lorsque le serveur OpenID est un noeud final SSL.

Il convient que les noeuds finals de fournisseur d'identité utilisés par les consommateurs pour accéder à OpenID soient configurés en SSL.

Dans la plupart des déploiements, des noeuds finals non protégés (par exemple utilisant le protocole HTTP au lieu de HTTPS) sont utilisés pour la résolution de l'URL d'identité d'un utilisateur. Il convient que les adresses URL suivantes, renvoyées sous forme de liens à en-tête HTML, utilisent le protocole SSL :

- openid.server
- openid2.provider

Il convient que les noeuds finals de consommateur soient configurés en HTTPS (SSL).

Modèle de page pour la promotion d'un serveur OpenID

Les spécifications d'authentification OpenID établissent que lorsqu'un fournisseur d'identité utilise une URL de connexion unique, une notification doit être renvoyée en cas de réception d'une requête HTTP GET dépourvue de paramètres (conformément à la spécification OpenID 1.1). La page à renvoyer doit contenir le texte suivant :

```
Il s'agit d'un noeud final du serveur OpenID. Pour plus d'informations,
voir http://openid.net/
```

Tivoli Federated Identity Manager fournit le fichier openid_server.html. Le fichier ne contient aucune macro remplaçable.

Les administrateurs peuvent utiliser cette page sans modifications, mais peuvent dans certains cas souhaiter modifier le style du code HTML pour répondre aux exigences spécifiques de leur environnement de déploiement.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
  "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html>
  <head>
    <title>Serveur OpenID</title>
  </head>
  <body>
    Il s'agit d'un noeud final du serveur OpenID. Pour plus d'informations,
voir <a href="http://openid.net/">http://openid.net/</a>
  </body>
</html>
```

Figure 32. Modèle de fichier openid_server.html

Ce modèle n'est défini que sur le fournisseur d'identité.

Modèle de page pour le consentement d'authentification

Cette page est utilisée par le fournisseur d'identité afin de définir et enregistrer les informations de consentement de l'utilisateur, qui déterminent l'autorisation ou non de procéder à l'authentification auprès d'un consommateur particulier et indiquent quels attributs facultatifs il convient de partager avec ce consommateur.

Lors s"une opération OpenID checkid_setup, l'utilisateur est redirigé vers le fournisseur d'identité afin de valider l'état de sa connexion. A ce moment-là, le fournisseur d'identité de mander à l'utilisateur la permission de fournir les informations d'authentification et d'attribut au site de consommation. Le fournisseur d'identité de Tivoli Federated Identity Manager délivre un modèle de page HTML appelé consent.html.

Tivoli Federated Identity Manager garde en mémoire les décisions de confiance qu'un utilisateur prend à l'égard d'un site de consommation particulier, en conservant les données sous forme de `trust_root` ou de `realm`. La sauvegarde de ces connaissances permet à Tivoli Federated Identity Manager de ne pas avoir à inviter l'utilisateur à se connecter à chaque fois au même consommateur.

La page de consentement affiche la liste des attributs que la requête de connexion unique (émise par le consommateur) a indiqués comme étant *requis* ou *facultatifs*.

Comme la longueur de ces listes est indéterminée, le modèle prend en charge de multiples copies de sections répétées une fois pour chaque attribut dans la liste concernée. La prise en charge des sections répétitives est permise par la spécification d'une extension d'enregistrement simple.

Les administrateurs peuvent utiliser cette page sans modifications, mais peuvent dans certains cas souhaiter modifier le style du code HTML pour répondre aux exigences spécifiques de leur environnement de déploiement.

Ce fichier modèle prend en charge plusieurs macros de remplacement :

@OPENID_TRUSTURL@
Cette macro est remplacée par le paramètre `openid.trust_root` dans la requête checkid_setup.

@OPENID_POLICYURL@
Cette macro est remplacée par le paramètre `openid.sreg_url` dans la requête checkid_setup lorsque l'adresse URL existe. Si l'adresse URL est inexistante, les valeurs sont représentées par une chaîne vide.

@OPENID_IDENTITYURL@
Cette macro est remplacée par le paramètre `openid.identity` dans la requête checkid_setup.

@OPENID_SSOURL@
Cette macro est remplacée par le noeud final du délégué de serveur OpenID (noeud final) sur le fournisseur d'identité. Cette valeur est utilisée pour le paramètre d'action FORM afin d'envoyer par requête POST les résultats du formulaire de consentement vers le serveur OpenID.

@OPENID_RETURN_TO_VALIDATED@
Cette macro est remplacée par true ou false pour informer l'utilisateur de toute validation d'URL return_to dans le cadre de la reconnaissance de la partie de confiance.

@REQUIRED_ATTRIBUTE@
Il s'agit d'une macro à valeurs multiples contenue dans une liste de remplacement répétable `[RPT requiredAttrs]`. Les valeurs affichent la liste des attributs obligatoires spécifiés par le fournisseur de services pour l'extension d'enregistrement simple. Cette macro est remplacée par chaque valeur contenue dans le paramètre `openid.sreg.required` de la requête, précédée de la chaîne de préfixe `openid.sreg.`.

@OPTIONAL_ATTRIBUTE@
Il s'agit d'une macro à valeurs multiples contenue dans une liste de remplacement répétable `[RPT optionalAttrs]`. Les valeurs affichent la liste des attributs facultatifs spécifiés par le fournisseur de services pour l'extension d'enregistrement simple. Cette macro est remplacée par chaque valeur contenue dans le paramètre `openid.sreg.optional` de la requête, précédée de la chaîne de préfixe `openid.sreg.`.

Les attributs facultatifs nécessitent une attention particulière. Le fournisseur d'identité permet aux utilisateurs de spécifier individuellement les attributs facultatifs qu'ils consentent à envoyer à un consommateur spécifié. Les préférences utilisateur sont dénotées par les paramètres 'true' ou 'false' pour chaque attribut facultatif, comme spécifié dans le formulaire contenu dans la page HTML de consentement d'authentification. Pour permettre l'activation de cette fonctionnalité, le nom du paramètre doit *obligatoirement* commencer par le préfixe `optattr_` et se finir par le nom complet de l'attribut facultatif.

Par exemple :

```
optattr_openid.sreg.email=true&optattr_openid.sreg.nickname=false
```

La figure suivante illustre un exemple de traitement des attributs facultatifs.

```
Les attributs facultatifs suivants ont été demandés. Veuillez sélectionner
les attributs que vous vous préparer à envoyer, ou sélectionnez l'option
"Tous les attributs facultatifs" :<br /><br />
         <input id="chk_all_optional_attributes" type="checkbox"
          checked="checked" name="all_optional_attributes"
          onClick="allOptionalAttributes()" />
         <label for="chk_all_optional_attributes">Tous les attributs optionnels
         </label><br /><br />
     [RPT optionalAttrs]
             <input id="chk_@OPTIONAL_ATTRIBUTE@" type="checkbox"
name="optattr_@OPTIONAL_ATTRIBUTE@" onClick="oneOptionalAttribute()" />
             <label for="chk_@OPTIONAL_ATTRIBUTE">@OPTIONAL_ATTRIBUTE@
             </label><br />
     [ERPT optionalAttrs]
```

Figure 33. Traitement du consentement lié aux attributs facultatifs individuels

Il est à noter que le paramètre d'entrée de la case à cocher présente dans le formulaire génère le nom en utilisant le préfixe `optattr_` et le nom de l'attribut facultatif. Pour chaque attribut facultatif, contenu dans la requête émise par le fournisseur de services, le code responsable du traitement de ce formulaire au niveau du fournisseur d'identité recherche un paramètre de type `optattr_<nom_attribut>`, puis traite la valeur comme ayant la valeur 'true' ou 'false'. Une valeur 'true' indique le consentement vis-à-vis de l'attribut facultatif. Lorsqu'un paramètre est absent dans le formulaire envoyé, le consentement adopte la valeur 'false'.

L'un des scénarios de déploiement possibles consiste à déployer un *portail de données personnelles* destiné aux utilisateurs individuels. Cette solution permet à un utilisateur particulier de détenir plusieurs identités créées à son intention, chacune d'elles comportant des ensembles d'attributs différents gérés dans un magasin de données externe. Cette fonctionnalité permet à l'utilisateur final d'associer des données personnelles particulières à un consommateur OpenID particulier. Cette association permet par la suite de sélectionner ces attributs personnels particuliers lorsque l'utilisateur se connecte au consommateur spécifié.

A titre d'exemple, un fournisseur d'identité peut autoriser un utilisateur à créer, nommer et alimenter dynamiquement un ensemble d'attributs pour chaque donnée personnelle.

Ce scénario est possible grâce à l'usage d'un paramètre facultatif FORM appelé `userdata`. Le paramètre `userdata` peut être une liste (accessible par un menu) qui permet à l'utilisateur de sélectionner les données personnelles à partir desquelles les attributs doivent être spécifiés.

Lorsque le paramètre `userdata` figure dans le formulaire d'entrée, la valeur de chaîne de l'adresse URL est incluse dans les réclamations adressées au service STS lors du mappage d'identité.

L'exemple de code suivant illustre le fichier modèle HTML consent.html.

Ce modèle n'est défini que sur le fournisseur d'identité.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
    <title>OpenID Consent-to-Authenticate</title>
<script type="text/javascript">

// when "All optional attributes" is selected,
uncheck any checked individual optional attributes
function allOptionalAttributes() {
    var theForm = document.forms[0];
    for (i = 0; i < theForm.elements.length; i++) {
        if (theForm.elements[i].type == "checkbox") {
            var cbName = theForm.elements[i].name;
            if (cbName.indexOf("optattr_") == 0) {
                theForm.elements[i].checked = false;
            }
        }
    }
}

// when an individual optional attribute is selected, be sure to
uncheck "All optional attributes"
function oneOptionalAttribute() {
    document.forms[0].all_optional_attributes.checked = false;
}

// utility function to show a section
function showDiv(f) {
  if (f.style) {
    f.style.display='block';
  }
}

</script>
  </head>
  <body>
    Ce site de consommation a demandé une ouverture de session OpenID pour vous :
 <b>@OPENID_TRUSTURL@</b>
    <p />
    Vous trouverez la stratégie du site de consommation, à l'adresse : <b>@OPENID_POLICYURL@</b>
    <p />


<script type="text/javascript">
    //
    // RP-discovery information
    //
    var txtWarningReturnTo = "WARNING: The return_to URL for the site has not
been successfully validated using relying-party discovery";
    var returntoValidated = @OPENID_RETURN_TO_VALIDATED@;
    if (!returntoValidated) {
        document.write(txtWarningReturnTo);
    }
</script>


    <p />
    Votre URL d'identité est : <b>@OPENID_IDENTITYURL@</b>
<script type="text/javascript">
    //
    // Display claimed identifier if different from identity URL
(e.g. if delegation was being used)
    //
    var txtClaimedID = "Your claimed identifier is: ";
```

```
    var identityurl = "@OPENID_IDENTITYURL@";
    var claimedid = "@OPENID_CLAIMEDID@";
    if (claimedid != identityurl) {
        document.write("<p />");
        document.write(txtClaimedID);
        document.write("<b>");
        document.write(claimedid);
        document.write("</b>");
    }
</script>


    <p />
<script type="text/javascript">
    //
    // PAPE information
    //
    var txtMaxAuthnAge = "Requested Maximum Authentication Age (seconds): ";
    var txtRequestedAuthnPolicies = "Requested Authentication Policies";
    var txtRequestedAssuranceLevels = "Requested Assurance Levels";

    var nopii = false;
    var maxAuthenticationAge = @MAXIMUM_AUTHENTICATION_AGE@;
    if ( maxAuthenticationAge >= 0) {
        document.write("<p/>" + txtMaxAuthnAge + maxAuthenticationAge);
    }

    var strAuthPolicies = "";
    [RPT authenticationPolicies]
        strAuthPolicies += "@REQUESTED_AUTHENTICATION_POLICY@"+",";
    [ERPT authenticationPolicies]
    if (strAuthPolicies.length > 0) {
        // strip last comma and split into array
        strAuthPolicies =
strAuthPolicies.substring(0,strAuthPolicies.lastIndexOf(","));
        var authPolicies = strAuthPolicies.split(",");
        document.write("<p/>");
        document.write("<table border>");
        document.write("<tr><th>" + txtRequestedAuthnPolicies + "</th></tr>");
        for (var i = 0; i < authPolicies.length; i++) {
            document.write("<tr><td>"+authPolicies[i]+"</td></tr>");

            // check if this is the nopii policy
            if (authPolicies[i] ==
"http://www.idmanagement.gov/schema/2009/05/icam/no-pii.pdf") {
                nopii = true;
            }
        }
        document.write("</table>");
    }

    var strAssuranceLevels = "";
    [RPT assuranceLevels]
        strAssuranceLevels += "@REQUESTED_ASSURANCE_LEVEL@"+",";
    [ERPT assuranceLevels]

    if (strAssuranceLevels.length > 0) {
        // strip last comma and split into array
        strAssuranceLevels =
strAssuranceLevels.substring(0,strAssuranceLevels.lastIndexOf(","));
        var assuranceLevels = strAssuranceLevels.split(",");
        document.write("<p/>");
        document.write("<table border>");
        document.write("<tr><th>" + txtRequestedAssuranceLevels + "</th></tr>");
        for (var i = 0; i < assuranceLevels.length; i++) {
            document.write("<tr><td>"+assuranceLevels[i]+"</td></tr>");
        }
```

```
        document.write("</table>");
    }

</script>


    <form action="@OPENID_SSOURL@" method="post">
      <input type="hidden" name="openid.mode" value="consent_to_authenticate" />
      <div id="DIV_ATTRIBUTES" name="DIV_ATTRIBUTES" style="display: none;">
        Les attributs obligatoires suivants ont été demandés :<br />
        <ul>
        [RPT requiredAttrs]
            <li>@REQUIRED_ATTRIBUTE@</li>
        [ERPT requiredAttrs]
        </ul>
        <p />
        Les attributs facultatifs suivants ont été demandés. Veuillez sélectionner
les attributs que vous vous préparer à envoyer, ou sélectionnez l'option
"Tous les attributs facultatifs" :<br /><br />
            <input id="chk_all_optional_attributes" type="checkbox"
checked="checked" name="all_optional_attributes"
onClick="allOptionalAttributes()" />
            <label for="chk_all_optional_attributes">
All Optional Attributes</label><br /><br />
        [RPT optionalAttrs]
                <input id="chk_@OPTIONAL_ATTRIBUTE@" type="checkbox"
name="optattr_@OPTIONAL_ATTRIBUTE@" onClick="oneOptionalAttribute()" />
                <label for="chk_@OPTIONAL_ATTRIBUTE@"
>@OPTIONAL_ATTRIBUTE@</label><br />
        [ERPT optionalAttrs]
      </div>
      <p />
      Souhaitez vous ouvrir une session sur ce site, en envoyant tous les attributs
nécessaires et en sélectionnant les attributs facultatifs ?
      <div>
        <input id="rd_permit_forever" type="radio"
name="consent" value="permit_forever"
checked="checked" /><label for="rd_permit_forever">
Allow Authentication forever
(add to my trusted sites)</label><br/>
        <input id="rd_permit_once" type="radio"
name="consent" value="permit_once" />
<label for="rd_permit_once">Allow Authentication this time only</label><br />
        <input id="rd_deny_once" type="radio" name="consent"
value="deny_once" />
<label for="rd_deny_once">Do not authenticate to this
site this time only</label><br />
        <input id="rd_deny_forever" type="radio" name="consent"
value="deny_forever" />
<label for="rd_deny_forever">Do not ever authenticate to this site
(add to my untrusted sites)</label><br />
      </div>
      <p /><label for="tx_userdata">Données utilisateur ou données personnelles :</label>
<input id="tx_userdata" type="text" name="userdata" />
      <p /><input type="submit" name="submit" value="Submit" />
    </form>
<script type="text/javascript">
  //
  // if the nopii policy was requested, leave the attribute information hidden
(as we shouldn't send it), otherwise show it
  //
  if (!nopii) {
    showDiv(document.getElementById("DIV_ATTRIBUTES"));
  }
```

```
</script>

  </body>
</html>
```

Page de modèle HTML pour la gestion des sites dignes de confiance

Cette page est utilisée en fournisseur d'identité. La page HTML est utilisée pour gérer l'ensemble permanent de sites sécurisés ou non sécurisés. L'utilisateur établit les sites via la page consent.html lors des opérations de connexion.

Les fonctionnalités du fournisseur d'identité OpenID incluent la possibilité de stocker et extraire certains attributs de préférences utilisateur, tels que :

- Site de consommation particulier ou non, tel qu'identifié par la valeur `trust_root`. Les valeurs d'accréditation peuvent être `once`, `never` ou `always`.
- La liste des attributs facultatifs pouvant être envoyés à un consommateur de confiance particulier
- Les données de préférences utilisateur éventuellement choisies par le fournisseur d'identité lors de la création d'un ensemble d'attributs pour une requête de connexion unique adressée à un consommateur. Le détail optionnel peut par exemple contenir un index d'informations personnelles.

  Tivoli Federated Identity Manager est doté d'un mécanisme de stockage des attributs sous forme de cookies persistants dans le navigateur.

Le serveur Tivoli Federated Identity Manager inclut un modèle de page et le code de prise en charge. Le modèle de page et le code de prise en charge utilisent l'interface pour stocker et extraire des informations sur les sites dignes de confiance. Les utilisateurs peuvent utiliser le modèle de page pour afficher et gérer cette liste.

Le fichier modèle porte le nom sitemanager.html.

Les administrateurs peuvent utiliser cette page sans modifications, mais peuvent dans certains cas souhaiter modifier le style du code HTML pour répondre aux exigences spécifiques de leur environnement de déploiement.

Le modèle comprend les macros de remplacement suivantes :

@USERNAME@
: Cette macro est remplacée par le nom d'utilisateur Tivoli Federated Identity Manager.

@SITE_NAME@
: Cette macro à valeurs multiples est utilisée dans une liste de remplacement répétable `[RPT trustedSites]` ou `[RPT untrustedSites]`. Elle est utilisée pour afficher des informations sur les sites configurés dans un des états suivants :

  - Toujours digne de confiance
  - Refusé définitivement

  Cette macro affiche l'URL `trust_root` du site sécurisé ou non sécurisé.

@REQUIRED_ATTRIBUTES@

Cette macro à valeurs multiples est utilisée dans une liste de remplacement répétable [RPT trustedSites]. La macro est utilisée pour afficher une liste séparée par des virgules de l'ensemble spécifique d'attributs requis que l'utilisateur doit envoyer au consommateur.

@OPENID_SITEMANAGERURL@

Cette macro est remplacée par l'URL de noeud final du gestionnaire de site délégué servant à traiter l'action remove sur les sites dignes de confiance.

@ALL_OPTIONAL_ATTRIBUTES@

Cette macro à valeurs multiples est utilisée dans une liste de remplacement répétable [RPT trustedSites] pour le site digne de confiance. La macro est utilisée pour indiquer si l'utilisateur est préparé à l'envoi de tous les attributs facultatifs demandés à ce consommateur. Les valeurs admises sont true et false.

@LISTED_OPTIONAL_ATTRIBUTES@

Cette macro à valeurs multiples est utilisée dans une liste de remplacement répétable [RPT trustedSites]. La macro est utilisée pour afficher une liste séparée par des virgules de l'ensemble spécifique d'attributs facultatifs que l'utilisateur est préparé à envoyer au consommateur. Cette valeur est une chaîne non vide lorsque @ALL_OPTIONAL_ATTRIBUTES@ a la valeur false pour le site digne de confiance. Lorsque @ALL_OPTIONAL_ATTRIBUTES@ vaut true, cette valeur est une chaîne vide.

@USERDATA@

Cette macro à valeurs multiples est utilisée dans une liste de remplacement répétable [RPT trustedSites]. La macro est utilisée pour afficher les données utilisateur facultatives. Les données peuvent être spécifiées par un utilisateur lorsqu'il traite la page de consentement d'authentification pour accréditer définitivement ce site. Lorsqu'aucune donnée d'utilisateur n'est spécifiée, la valeur de la macro est une chaîne vide

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html>
 <head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
  <title>Gestionnaire de site OpenID</title>
 </head>
 <body>
  OpenID Site Manager</titleb>@USERNAME@</b>
  <p/>
  Sites de confiance<br />
  <table border="1">
   <tr><td>Site</td><td>Required Attributes</td><td>All Optional
Attributes?</td><td>Permitted Optional Attributes</td><td>User
Data</td><td>Action</td></tr>
[RPT trustedSites]
   <tr>
    <td>@SITE_NAME@</td>
    <td>@REQUIRED_ATTRIBUTES@</td>
    <td>@ALL_OPTIONAL_ATTRIBUTES@</td>
    <td>@LISTED_OPTIONAL_ATTRIBUTES@</td>
    <td>@USERDATA@</td>
    <td><a href="@OPENID_SITEMANAGERURL@?action=
remove&site=@SITE_NAME@">Remove</a></td>
   </tr>
 [ERPT trustedSites]
 </table>
 <p/>
 Sites non sécurisés<br />
 <table border="1">
 <tr><td>Site</td><td>Action</td></tr>
 [RPT untrustedSites]
 <tr>
  <td>@SITE_NAME@</td>
  <td>@OPENID_SITEMANAGERURL@?
action=remove&site=@SITE_NAME@">Remove</a></td>
 </tr>
[ERPT untrustedSites]
 </table>
</body>
</html>
```

Figure 34. Modèle de fichier HTML sitemanager.html

Ce modèle n'est défini que sur le fournisseur d'identité.

Modèle de page pour les erreurs liées à OpenID

Lorsque le traitement est interrompu par une erreur au niveau du fournisseur d'identité ou du consommateur et que cette erreur ne fait l'objet d'aucun renvoi, Tivoli Federated Identity Manager utilise un modèle de page d'erreur générique pour afficher des informations détailles sur le texte de l'erreur.

Par exemple :

- Sur un fournisseur d'identité, cette page est utilisée lorsque le traitement des pages des sites sécurisés ou d'une requête de connexion unique ce comporte aucune adresse URL `return_to` valide.
- Au niveau du consommateur, cette page est appelée lorsque des paramètres erronés sont renvoyés dans la page de connexion.

Le modèle de page porte le nom error.html.

Les administrateurs peuvent utiliser cette page sans modifications, mais peuvent dans certains cas souhaiter modifier le style du code HTML pour répondre aux exigences spécifiques de leur environnement de déploiement.

Les macros de remplacement suivantes sont prises en charge :

@REQ_ADDR@
Cette macro est remplacée par l'adresse URL du noeud final délégué en cours d'appel.

@TIMESTAMP@
Cette macro est remplacée par l'heure actuelle au format de temps universel coordonné.

@DETAIL@
Cette macro est remplacée par la version en support de langue nationale (NLS) du message d'erreur associé à l'erreur.

@EXCEPTION_STACK@
Cette macro est remplacée par la trace de pile des exceptions éventuelles qui ont provoqué l'erreur.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
    <head>
        <title>Une erreur OpenID s'est produite</title>
    </head>
    <body style="background-color:#ffffff">
        <div>
            <h2 style="color:#ff8800">Une erreur s'est produite</h2>
            <div id="infoDiv" style="background-color:#ffffff;color:#000000">
                <em>@REQ_ADDR@</em> <br />
                <em>@TIMESTAMP@</em> <br />
            </div>
            <br />
<div id="detailDiv" style="background-color:#999999; border-style:solid;
border-width:1px; border-color:#000000">
                <h4>Détails sur l'erreur</h4>
                @DETAIL@
            </div>
            <br />
            <div id="stackDiv" style="background-color:#999999;
border-style:solid; border-width:1px; border-color:#000000">
                <h4>Trace de pile</h4>
                @EXCEPTION_STACK@
            </div>
        </div>
    </body>
</html>
```

Figure 35. Modèle de fichier HTML error.html

Ce modèle est utilisé à la fois sur le fournisseur d'identité et le consommateur.

Modèle de page pour l'envoi indirect de requêtes OpenID 2.0

La norme OpenID 2.0 spécifie que des requêtes POST HTTP peuvent être utilisées à la place des redirections HTTP lors de l'envoi de messages de réacheminement entre le fournisseur d'identité et la partie de confiance (consommateur). Ces messages sont envoyés au navigateur, puis redirigés vers la cible.

Tivoli Federated Identity Manager effectue automatiquement la permutation des messages dans une requête FORM auto-émise via une requête HTTP POST (au lieu d'une redirection 302) lorsque les conditions suivantes sont vérifiées :

- OpenID 2.0 est utilisé
- La taille de message dépasse 2 Ko

Lorsqu'une requête POST est utilisée, une page est chargée. Celle-ci contient une requête FORM auto-émise (au lieu d'une redirection 302), contenant les mêmes paramètres que ceux qui auraient été autrement transmis via la chaîne de requête.

Le fichier du modèle est indirect_post.html.

Les administrateurs peuvent utiliser cette page sans modifications, mais peuvent dans certains cas souhaiter modifier le style du code HTML pour répondre aux exigences spécifiques de leur environnement de déploiement.

Le fichier prend en charge les macros de remplacement suivantes :

@OPENID_PARTNER_URL@
Cette macro est remplacée par l'adresse URL du partenaire cible. Cette valeur est utilisée pour le paramètre d'action FORM.

@PARAM_NAME@ / @PARAM_VALUE@
Il s'agit de macros à valeurs multiples spécifiées à l'intérieur d'une liste de remplacement `[RPT formFields]` répétable. Ces valeurs servent à transmettre les paramètres au destinataire concerné.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
  "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
    <title>Message OpenID</title>
  </head>
  <body>
    <form method="post" name="openid_message" action="@OPENID_PARTNER_URL@">
      [RPT formFields]
        <input type="hidden" name="@PARAM_NAME@" value="@PARAM_VALUE@" />
      [ERPT formFields]
      <noscript>
      <button type="submit">Envoyer le message OpenID</button>
<!-- inclus pour les demandeurs qui ne prennent pas en charge Javascript -->
      </noscript>
    </form>
    <script type="text/javascript">
        var signOnText = 'Envoi du message OpenID en cours...';
        document.write(signOnText);
        setTimeout('document.forms[0].submit()', 0);
    </script>
  </body>
</html>
```

Figure 36. Modèle de fichier indirect_post.html

Ce modèle n'est défini que sur le fournisseur d'identité.

Modèle de page renvoyé pour checkid_immediate

Lorsqu'une requête checkid_immediate est initiée par le fournisseur de services Tivoli Federated Identity Manager et que le fournisseur d'identité renvoie un statut selon lequel la détention de l'URL par l'utilisateur ne peut pas être confirmée, le fournisseur d'identité renvoie également l'un des éléments suivants :

- openid.user_setup_url

  Pour OpenID 1.1
- openid.mode=user_setup_needed

  Pour OpenID 2.0

Lorsque le consommateur Tivoli Federated Identity Manager reçoit ce type de réponse, il renvoie un fichier de modèle de page.

Le fichier du modèle de page porte le nom immediate.html.

Les administrateurs peuvent utiliser cette page sans modifications, mais peuvent dans certains cas souhaiter modifier le style du code HTML pour répondre aux exigences spécifiques de leur environnement de déploiement.

Le fichier comprend la macro de remplacement suivante :

@OPENID_USER_SETUP_URL@
: Cette macro est remplacée par l'adresse URL renvoyée dans le paramètre openid.user_setup_url d'une réponse à la requête checkid_immediate par le fournisseur d'identité. Lorsqu'il s'agit d'une requête OpenID 2.0, ce paramètre peut être une chaîne vide.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
  "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html>
  <head>
    <title>Résultats de checkid_immediate</title>
  </head>
  <body>
    <script type="text/javascript">
        var setup_url = "@OPENID_USER_SETUP_URL@";
        if (setup_url) {
            document.write('<a href="');
            document.write(setup_url);
            document.write('">Veuillez cliquer ici pour compléter les exigences
            du fournisseur d'identité </a>');
        } else {
            document.write('Impossible de poursuivre le traitement car une
        authentification est requise par le fournisseur d'identité OpenID.');
        }
    </script>
  </body>
</html>
```

Figure 37. Modèle de page immediate.html

Ce modèle n'est utilisé que sur le consommateur.

Modèle de page renvoyé pour les erreurs du serveur

Lorsque le consommateur Tivoli Federated Identity Manager envoie une requête checkid_immediate ou checkid_setup et que celle-ci provoque une erreur, le serveur du fournisseur d'identité renvoie `openid.mode` défini sur `error` et indique le texte de l'erreur dans le fichier `openid.error`.

Dans ce cas, le consommateur renvoie la page server_error.html.

Les administrateurs peuvent utiliser cette page sans modifications, mais peuvent dans certains cas souhaiter modifier le style du code HTML pour répondre aux exigences spécifiques de leur environnement de déploiement.

Le modèle de page prend en charge les macros de remplacement suivantes :

@OPENID_SERVER@
: Cette macro est remplacée par l'URL du serveur OpenID que le consommateur était en train de communiquer au moment où l'erreur s'est produite.

@OPENID_ERROR@
: Texte issu du fichier `openid.error`.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
  "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html>
  <head>
    <title>Erreur OpenID renvoyée par le serveur</title>
  </head>
  <body>
    Le serveur OpenID : @OPENID_SERVER@ a renvoyé
    le texte d'erreur suivant :<br />
    @OPENID_ERROR@
  </body>
</html>
```

Figure 38. Fichier modèle server_error.html

Ce modèle n'est utilisé que sur le consommateur.

Chapitre 24. Planification d'une fédération Liberty

Vous devrez, lors de la configuration d'une fédération Liberty, spécifier des valeurs pour les propriétés de la fédération.

Il convient que vous soyez familiarisé avec les documents relatifs aux normes Liberty avant de mettre en oeuvre une fédération de connexion unique. Les normes définissent les échanges de données et le traitement de messages. Vous devez déterminer les informations que vous devez fournir à vos partenaires commerciaux, ainsi que les informations que vos partenaires doivent vous remettre.

Liberty Alliance

`http://www.projectliberty.org`

L'assistant de fédération vous invite à indiquer des valeurs pour un certain nombre de propriétés. La plupart d'entre elles peuvent être modifiées ultérieurement, après la création de la fédération.

Le choix du ou des profils à utiliser dépend à la fois des décisions en matière de règles commerciales et de l'architecture du réseau du point de vue de la sécurité. Les partenaires de la fédération doivent se mettre d'accord sur le choix des profils afin de permettre la connexion unique sur l'ensemble de la fédération. Ce choix doit être fait avant la configuration de la fédération.

La norme Liberty prend en charge une gamme unique de profils de connexion unique. Les profils dépassent les spécifications pour obtenir une connexion unique fédérée et peuvent inclure d'autres fonctions, telles que la déconnexion unique, la notification de résiliation de la fédération ou l'identification du nom de registre.

Rôles du fournisseur d'identité et du fournisseur de services

Au sein d'une fédération, chaque partenaire a un rôle. Il s'agit du rôle **Fournisseur d'identité** ou **Fournisseur de services**.

- Fournisseur d'identité

  Le fournisseur d'identité est un partenaire de fédération qui garantit l'identité des utilisateurs. Il authentifie un utilisateur et transmet un jeton d'authentification au fournisseur de services.

  Le fournisseur d'identité authentifie l'utilisateur soit directement, par exemple en validant un nom d'utilisateur et un mot de passe, soit indirectement, en validant une assertion sur l'identité de l'utilisateur présentée par un autre fournisseur d'identité.

  Le fournisseur d'identité gère les identités des utilisateurs afin de dégager le fournisseur de services de cette responsabilité.

- Fournisseur de services

  Le fournisseur de services est un partenaire de fédération qui fournit des services à l'utilisateur final. En général, il n'authentifie pas les utilisateurs, mais demande à un fournisseur d'identité de prendre les décisions liées à l'authentification. Les fournisseurs de services comptent sur les fournisseurs d'identité pour affirmer l'identité d'un utilisateur et pour gérer les identités des utilisateurs pour la fédération.

Les fournisseurs de services peuvent gérer un compte local pour l'utilisateur, compte qui peut être désigné par un identificateur.

Profils de connexion unique Liberty

Liberty prend en charge plusieurs profils de connexion unique. Vous devez sélectionner au moins un profil. Vous avez également la possibilité de configurer les profils Artefact du navigateur (Browser Artifact) et POST du navigateur (Browser POST) lors de la configuration d'un fournisseur d'identité. Vous ne pouvez sélectionner qu'un seul profil lors de la configuration d'un fournisseur de services.

Artefact du navigateur (Browser Artifact)
L'artefact du navigateur utilise un canal de retour SOAP pour échanger un artefact au cours de l'établissement et de l'utilisation d'une session sécurisée entre un fournisseur d'identité, un fournisseur de services et un client (navigateur).

Vous avez également la possibilité de configurer le profil Artefact du navigateur (Browser Artifact) lors de la configuration d'un fournisseur d'identité ou d'un fournisseur de services.

Lorsque vous sélectionnez le profil Artefact du navigateur, le programme vous demandera également le nom d'une clé de chiffrement pour la session sécurisée. Vous devez spécifier une clé même si vous choisissez de rendre facultative la signature d'assertions pour les autres communications par message Liberty.

POST du navigateur (Browser POST)
Le profil du navigateur POST utilise un formulaire qui renvoie l'action à lui-même (self-posting form) pour échanger un artefact au cours de l'établissement et de l'utilisation d'une session sécurisée entre un fournisseur d'identité, un fournisseur de services et un client (navigateur).

Vous avez également la possibilité de configurer le profil POST du navigateur lors de la configuration d'un fournisseur d'identité ou d'un fournisseur de services.

Remarque : Lors de la configuration d'un fournisseur d'identité, vous pouvez sélectionner à la fois le profil Artefact du navigateur (Browser Artifact) et le profil POST du navigateur (Browser POST). Toutefois, lors de la configuration d'un fournisseur de services, vous ne pouvez sélectionner qu'un seul profil, c'est-à-dire soit l'artefact du navigateur, soir le POST du navigateur.

Profil de connexion unique LECP (Liberty-enabled client/proxy)
Un client activé pour Liberty (Liberty Enabled Client) ou un proxy activé pour Liberty (Liberty-Enabled Proxy) a ou sait comment obtenir les informations requises pour se connecter au fournisseur de services que l'utilisateur (principal) veut utiliser avec ce fournisseur de services. Un proxy activé pour Liberty est un proxy HTTP, par exemple une passerelle WAP (Wireless Application Protocol), qui émule un client activé pour Liberty.

Fournisseurs LECP
Liste séparée par des virgules de variables d'en-tête utilisées par LECP. Cette propriété se définit lors de la configuration des fournisseurs d'identité et des fournisseurs de services. Il n'existe pas de valeur par défaut.

Exemple de variable d'en-tête unique :

```
ibm_msisdn
```

Exemple de variables d'en-tête multiples :

```
ibm_msisdn,x_msisdn
```

Identificateur RNI (Register Name Identifie) pour Liberty

Ce profil met à jour l'identificateur d'un utilisateur ou principal. Liberty requiert que les fournisseurs d'identité et les fournisseurs de services échangent un alias (ou identificateur) pour chaque compte utilisateur, au lieu d'échanger le nom de compte réel de l'utilisateur. Cette fonctionnalité permet de relier des comptes entre eux tout en masquant les noms de compte utilisateur.

La configuration du profil RNI est facultative.

Lorsqu'il est sélectionné, l'administrateur doit sélectionner les liaisons de communication à utiliser entre les fournisseurs. Ces liaisons peuvent être définies séparément pour le fournisseur d'identité et pour le fournisseur de services. Les liaisons prises en charge sont les suivantes :

- Réacheminement HTTP

  Le fournisseur d'identité et le fournisseur de services communiquent en envoyant des requêtes HTTP 302 au navigateur. Les identificateurs sont mis à jour l'un après l'autre à l'aide des réacheminements. Le réacheminement HTTP est la liaison par défaut pour les fournisseurs d'identité et de services.
- SOAP/HTTP

  Les identificateurs sont mis à jour via des échanges directs entre les fournisseurs via une connexion SOAP.

Les noeuds finals sont les suivants :

URL de service RNI
Le noeud final d'URL est utilisé pour les protocoles RNI fondés sur l'agent utilisateur. Une valeur par défaut est fournie. Par exemple :

```
https://idp.exemple.com/FIM/sps/libertyfed/liberty/rni
```

URL de retour RNI
Le noeud final d'URL est utilisé à des fins de réacheminement une fois que l'enregistrement du nom HTTP a été effectué. Une valeur par défaut est fournie. Par exemple :

```
https://idp.exemple.com/FIM/sps/libertyfed/liberty/rnireturn
```

Cette valeur est requise pour RNI lors de l'utilisation des communications avec réacheminement HTTP. Elle n'est pas requise pour les communications SOAP/HTTP.

Notification FTN (Federation Termination Notification) pour Liberty

Ce profil met fin aux liaisons associées au compte d'un utilisateur dans la fédération. Par défaut, il est désactivé.

La configuration de ce profil est facultative. Lorsque ce profil est sélectionné, vous devez sélectionner les liaisons de communication à utiliser entre les fournisseurs. Ces liaisons peuvent être définies séparément pour le fournisseur d'identité et pour le fournisseur de services. Les liaisons prises en charge sont les suivantes :

- Réacheminement HTTP

  Le fournisseur d'identité et le fournisseur de services communiquent en envoyant des requêtes HTTP 302 au navigateur. Les associations de comptes à la fédération sont résiliées l'une après l'autre à l'aide des réacheminements. Le réacheminement HTTP est la liaison par défaut pour les fournisseurs d'identité et de services.
- SOAP/HTTP

  Les associations de comptes à la fédération sont résiliées l'une après l'autre à l'aide des échanges directs entre les fournisseurs via une connexion SOAP.

Les noeuds finals sont les suivants :

URL de service FTN
URL, sur le fournisseur, vers laquelle les processus FTN uniques sont envoyés. Une valeur par défaut est fournie. Par exemple :

```
https://idp.exemple.com/FIM/sps/libertyfed/liberty/ftn
```

URL de retour FTN
Adresse URL utilisée par le fournisseur d'identité ou le fournisseur de services lors du réacheminement de l'agent utilisateur à la fin du processus de notification de résiliation de la fédération basé sur l'agent utilisateur.

```
https://idp.exemple.com/FIM/sps/libertyfed/liberty/ftnreturn
```

FTN requiert cette valeur lors de l'utilisation de la communication par réacheminement HTTP.

Fermeture de session unique Liberty

Ce profil met fin à toutes les sessions de connexion associées à un utilisateur au sein de la fédération. Par défaut, il est désactivé.

La configuration de ce profil est facultative. Lorsqu'il est sélectionné, l'administrateur doit sélectionner les liaisons de communication à utiliser entre les fournisseurs. Ces liaisons peuvent être définies séparément pour le fournisseur d'identité et pour le fournisseur de services. Les liaisons prises en charge sont les suivantes :

- Réacheminement HTTP

  Le fournisseur d'identité et le fournisseur de services communiquent en envoyant des requêtes HTTP 302 au navigateur. Les sessions utilisateur sont déconnectées l'une après l'autre à l'aide des réacheminements. Le réacheminement HTTP est la liaison par défaut pour les fournisseurs d'identité et de services.
- HTTP GET

  Les fournisseurs d'identité peuvent, à l'aide des balises Image, obliger le navigateur à utiliser HTTP GET pour communiquer les demandes de déconnexion aux fournisseurs de services. Ces demandes de déconnexion sont traitées simultanément et non pas l'une après l'autre. En cas d'échec d'une demande de déconnexion, les autres demandes ne sont pas affectées et sont envoyées au fournisseur de services approprié. A l'inverse, lorsque des demandes de déconnexion sont traitées l'une après l'autre (en série, avec des réacheminements HTTP), l'échec d'une demande de déconnexion entraîne l'annulation des demandes restantes.

Remarque : Cette option n'est spécifiée que sur les fournisseurs d'identité. Les fournisseurs de services ne peuvent pas la définir.

- SOAP/HTTP

  La déconnexion des sessions utilisateur s'effectue par des échanges directs entre les fournisseurs via une connexion SOAP.

Les noeuds finals sont les suivants :

URL de service SLO
URL à laquelle le fournisseur de services envoie les demandes de déconnexion d'utilisateurs. Une valeur par défaut est fournie. Par exemple :

```
https://idp.exemple.com/FIM/sps/libertyfed/liberty/slo
```

URL de retour SLO
URL utilisée par le fournisseur de services lors du réacheminement de l'agent utilisateur vers le fournisseur d'identité à la fin du processus du profil de déconnexion unique (SLO). Une valeur par défaut est fournie. Par exemple :

```
https://idp.exemple.com/FIM/sps/libertyfed/liberty/sloreturn
```

Cette valeur est requise pour SLO lors de l'utilisation des communications avec réacheminement HTTP.

Présentation du fournisseur d'identité Liberty

Le profil IPI (Identity Provider Introduction, ou présentation du fournisseur d'identité) permet à un fournisseur de services de connaître les fournisseurs d'identité utilisés par un utilisateur (principal). Ce profil se fonde sur un cookie écrit dans un domaine commun aux fournisseurs d'identité et aux fournisseurs de services dans un réseau de fédération d'identité.

Ce profil n'est configuré que sur un fournisseur d'identité.

Domaine DNS commun

Le domaine DNS commun est un domaine virtuel dans lequel un composant est configuré pour définir ou extraire un cookie. L'utilisation de ce domaine commun permet aux fournisseurs d'identité et aux fournisseurs de services, qui se trouvent généralement dans des domaines séparés, d'accéder à un cookie. Cette propriété de configuration peut être définie avant même l'existence du domaine. Vous devrez toutefois créer ce domaine pour qu'un utilisateur puisse effectuer une connexion unique en s'appuyant sur le profil IPI. Cette propriété n'est définie que lors de la configuration d'un fournisseur d'identité. Il n'existe pas de valeur par défaut. Par exemple :

```
cot.projectliberty.org
```

La configuration IPI nécessite une valeur dans cette zone.

Nom d'hôte de domaine commun

Nom d'un système hôte dans le domaine DNS commun. Cet hôte reçoit les demandes de définition ou de lecture du cookie du domaine commun utilisé par le profil IPI. Cette propriété n'est définie que lors de la configuration d'un fournisseur d'identité. Il n'existe pas de valeur par défaut. Par exemple :

```
idp.cot.projectliberty.org
```

La partie nom de domaine de ce nom d'hôte doit correspondre à la valeur définie dans le domaine DNS commun. Par exemple, la valeur de ce système hôte doit comprendre `cot.projectliberty.org`.

La configuration IPI nécessite une valeur dans cette zone.

Sécurité des messages Liberty

Options de signature numérique

L'assistant de création de fédération vous demande si vous souhaitez signer les messages Liberty. Si vous choisissez de signer les messages Liberty, vous devez indiquer une clé ou un certificat à utiliser.

Dans certains cas, lorsque vous ne cochez pas la case Signer les messages Liberty, vous devez néanmoins entrer une clé ou un certificat. Par exemple :

- Lors de la sélection du profil Artefact du navigateur, vous devez indiquer une clé à utiliser pour signer les messages envoyés dans l'ensemble du canal de retour pour l'artefact.
- Lorsque vous sélectionnez un des profils facultatifs et que vous indiquez que les communications SOAP doivent être lancées par le fournisseur de services, vous devez spécifier une clé ou un certificat.

Si vous avez besoin d'entrer une clé ou un certificat, vous devez fournir les informations de configuration suivantes :

Nom du fichier de clés
L'assistant présente une sélection des fichiers de clés que vous avez configurés avant de commencer la configuration de la fédération de connexion unique.

Mot de passe du fichier de clés
Vous devez indiquer le mot de passe utilisé pour accéder au fichier de clés.

Nom de la clé
Vous devez spécifier la clé à utiliser.

Propriétés des communications Liberty

Durée maximale des messages Liberty

Nombre entier correspondant à la durée de validité, en secondes, d'un message Liberty. Cette propriété est définie sur le fournisseur d'identité et sur le fournisseur de services.

Valeur minimale : 60 secondes

Valeur maximale : pas de valeur maximale autre que celle, sous forme de nombre entier, prise en charge par le type de données.

Valeur par défaut : 60 secondes

Durée des artefacts Liberty

Nombre entier correspondant à la durée, en secondes, pendant laquelle un fournisseur de services peut extraire une assertion d'un fournisseur d'identité. Le fournisseur de services utilise un artefact pour extraire cette assertion. Le fournisseur d'identité conserve le mappage entre l'artefact et l'assertion en cache pendant la durée définie. Si le fournisseur de services ne récupère pas l'artefact au terme de cette durée, l'artefact est purgé du cache et la connexion du fournisseur de services échoue.

Cette propriété ne se définit que lors de la configuration d'un fournisseur d'identité à l'aide du profil de connexion unique Artefact du navigateur (Browser Artifact).

Remarque : Cette valeur n'est pas utilisée avec le profil POST du navigateur (Browser POST).

Valeur minimale : 120 secondes

Valeur par défaut : 120 secondes.

Nécessite un accord pour fédérer

Détermine si le fournisseur d'identité demande à l'utilisateur final s'il accepte de rejoindre la fédération. Cette propriété n'est définie que sur le fournisseur d'identité. Ce message s'affiche lors de la fédération du compte utilisateur. Par défaut, cette option est désactivée. Cochez cette case pour activer l'affichage de l'invite.

SOAP, noeud final

Emplacement du noeud final SOAP (Simple Object Access Protocol) sur le fournisseur de services ou le fournisseur d'identité auquel sont envoyés les messages Liberty SOAP.

Ce paramètre est requis lorsqu'au moins l'une des deux conditions suivantes se vérifie :

- Le profil de connexion unique Artefact du navigateur (Browser Artifact) est sélectionné dans la fenêtre des profils Liberty.
- Un ou plusieurs profils Liberty facultatifs sont sélectionnés, de même que la communication SOAP/HTTP initialisée par au moins un des fournisseurs de services.

Par exemple :

```
https://idp.exemple.com/FIM/sps/libertyfed/liberty/soap
```

La connexion unique est passive (pas d'interaction entre le fournisseur d'identité et l'utilisateur)

Détermine s'il peut ou non y avoir une interaction entre le fournisseur d'identité et le principal (l'utilisateur) et si ce fournisseur peut prendre le contrôle de l'interface utilisateur à la place du fournisseur d'identité. Cette propriété n'est définie que lors de la configuration d'un fournisseur de services. Cochez cette case pour activer cette option. Valeur par défaut : désactivée.

Forcer le fournisseur d'identité à authentifier l'utilisateur

Détermine si le fournisseur d'identité doit authentifier un utilisateur (principal), que ce dernier soit ou non déjà authentifié. Cette valeur ne se définit que lorsque la case **La connexion unique est passive (pas d'interaction entre le fournisseur d'identité et l'utilisateur)** est désactivée. En outre, elle ne se définit que lors de la configuration d'un fournisseur de services.

Si ce paramètre n'est pas sélectionné, le fournisseur d'identité ne doit authentifier l'utilisateur (principal) que si ce dernier ne l'a pas encore été.

- Cochez la case **Forcer le fournisseur d'identité à authentifier l'utilisateur** pour activer cette option.
- Dans le cas contraire, désactivez-la.

Modules de jetons Liberty

Lorsque vous créez une fédération de connexion unique, vous devez configurer une instance de module de jeton de sécurité pour cette fédération. Le module de jeton correspond à un type de jeton de sécurité qui définit le format du jeton chiffré contenant les données d'identification des utilisateurs.

Le jeton est échangé entre le fournisseur d'identité et le fournisseur de services dans le cadre des services d'authentification et d'autorisation pour le traitement de chaque requête d'accès d'utilisateur.

Lorsque vous utilisez l'assistant de création de fédération, un type de jeton est automatiquement sélectionné en fonction du choix du protocole de connexion unique.

La configuration du module de jeton Liberty est requise uniquement par le fournisseur d'identité. Aucune configuration n'est nécessaire lors du déploiement d'un fournisseur de services.

La propriété de configuration est identique pour les jetons Liberty v1.1 et les jetons Liberty v1.2.

Durée de validité (en secondes) de la vérification après émission
Nombre entier correspondant à la durée de validité, en secondes, de l'assertion. Il est spécifié pour les jetons Liberty. La valeur minimale est 120 secondes. La valeur maximale est 300 secondes.

Mappage d'identité Liberty

L'assistant de création de fédération vous invite à spécifier soit l'authentification par fichier de règle de mappage XSLT, soit via une instance de module de mappage personnalisée.

Le fichier de mappage XSLT ou l'instance de module de mappage personnalisée doivent être préparés avant la configuration de la fédération.

Transformation XSL pour le mappage d'identité
La sélection de ce bouton sur l'assistant indique que vous comptez fournir un fichier XSL contenant le mappage d'identité. Entrez le nom d'un fichier du système de fichiers local.

Instance de module de mappage personnalisée
La sélection de ce bouton sur l'assistant indique que vous comptez fournir une instance de module de mappage personnalisée, que vous utiliserez à la place du fichier XSL. Vous serez éventuellement invité à entrer les propriétés de configuration requises par l'instance du module de mappage personnalisée.

Mappage de données d'identification Tivoli Access Manager vers un jeton Liberty ou SAML 2

Ce scénario se produit lors de l'échange de messages entre des partenaires d'une fédération de connexion unique Liberty ou SAML 2 et lorsque des données d'identification utilisateur sont gérées par Tivoli Access Manager. Lorsqu'une demande d'utilisateur est reçue (par exemple, pour accéder à une ressource distante), le service d'accréditation prend contact avec Tivoli Access Manager et obtient des données Tivoli Access Manager relatives à l'identité de l'utilisateur.

Dans ce scénario, le module de données d'identification Tivoli Access Manager du service d'accréditation fonctionne en mode de validation. Dans ce mode, il convertit les données d'identification Tivoli Access Manager en un document d'utilisateur universel STS d'entrée (In-STSUUSER). Le document In-STSUUSER créé à partir du module d'accréditation Tivoli Access Manager contient toutes les informations issues des droits d'accès. Ces informations peuvent éventuellement être utilisées par le module de service d'accréditation qui va générer le jeton sortant.

Le service d'accréditation consulte son entrée de configuration correspondant au partenaire de la fédération (par exemple, la destination qui héberge une ressource demandée). La configuration indique le type de jeton à créer.

Le module de mappage d'identité convertit ensuite l'élément In-STSUUSER en un utilisateur universel STS de sortie (Out-STSUUSER). L'élément Out-STSUUSER doit contenir les informations requises par le module de jeton Liberty (ou SAML 2) Tivoli Federated Identity Manager pour générer un jeton Liberty (ou SAML 2).

L'élément Out-STSUUSER doit contenir les informations suivantes qui permettent au module de jeton de générer un jeton valide :

Tableau 102. Entrées Out-STSUUSER servant à générer un jeton Liberty ou SAML 2

Elément Out-STSUUSER	**Informations de jeton**	**Obligatoire/ Facultatif**
Principal Attr: Name	Nom à transmettre au service d'alias	Obligatoire
Attribute: AuthenticationMethod	Méthode d'authentification. Il est à noter que cet élément est toujours paramétré sur "password" (nom d'utilisateur/mot de passe), quelle que soit la méthode d'authentification définie dans les données d'identification Tivoli Access Manager.	Obligatoire
Liste des attributs	Attributs personnalisés supplémentaires	Facultatif

Le module de mappage est responsable des opérations suivantes :

1. Mappage de l'élément Principal Attr Name dans In-STSUUSER vers une entrée de nom Principal dans Out-STSUUSER.

   Il est à noter que lorsque le module de jeton génère le jeton, ce nom de Principal n'est pas utilisé directement. En revanche, la valeur de la zone Name est envoyée en entrée du service d'alias de Tivoli Federated Identity Manager. Le service d'alias obtient l'alias (identificateur de nom) pour le principal et place l'alias renvoyé dans le module de jeton généré.

   Pour obtenir un exemple de fichier de règles de mappage extrait du fichier de mappage d'application de démonstration, ip_liberty.xsl, voir la figure 39, à la page 352. Il est à noter que les jetons Liberty sont des extensions des jetons SAML. Par conséquent, les commentaires de l'exemple de code qui font référence aux jetons SAML sont corrects dans ce contexte.

```
</xsl:template>
<!-- Ce modèle remplace l'intégralité de l'élément Principal par un élément qui ne
     que l'adresse électronique (à partir de ivcred tagvalue_email) et le
     type de données approprié pour SAML. -->
 <xsl:template match="//stsuuser:Principal">
  <stsuuser:Principal>
   <stsuuser:Attribute name="name"
                type="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
    <stsuuser:Value>
    <xsl:value-of
    select="//stsuuser:AttributeList/stsuuser:Attribute[@name='tagvalue_email']
          [@type='urn:ibm:names:ITFIM:5.1:accessmanager']/stsuuser:Value" />
    </stsuuser:Value>
   </stsuuser:Attribute>
  </stsuuser:Principal>
 </xsl:template><!--
```

Figure 39. Exemple de code XSL présentant le mappage d'une valeur des données d'identification Tivoli Access Manager vers un nom Principal pour un jeton Liberty

2. Paramétrage de la méthode d'authentification sur "password" (mot de passe), quelle que soit la valeur obtenue des données d'identification Tivoli Access Manager. Cette action est requise par le module de jeton.

   Pour obtenir un exemple de fichier de règles de mappage extrait du fichier de mappage d'application de démonstration, ip_liberty.xsl, voir figure 40.

```
<xsl:template match="//stsuuser:AttributeList">
  <stsuuser:AttributeList>
  <!-- Tout d'abord l'attribut de la méthode d'authentification -->
   <stsuuser:Attribute name="AuthenticationMethod"
                           type="urn:oasis:names:tc:SAML:1.0:assertion">
    <stsuuser:Value>urn:oasis:names:tc:SAML:1.0:am:password</stsuuser:Value>
   </stsuuser:Attribute>
          ....
       </stsuuser:AttributeList>
</xsl:template>
```

Figure 40. Exemple de code XSL présentant l'affectation d'une méthode d'authentification sous forme d'attribut pour un jeton Liberty

3. Remplissage de l'instruction d'attribut de la vérification à l'aide des attributs de l'élément AttributeList dans In-STSUUSER. Ces informations deviennent des informations personnalisées du jeton.

   Des attributs personnalisés peuvent être requis par les applications qui utilisent les informations à transmettre entre les partenaires d'une fédération.

   Pour obtenir un exemple de fichier de règles de mappage extrait du fichier de mappage d'application de démonstration, ip_liberty.xsl, voir la figure 41, à la page 353.

```
<xsl:template match="//stsuuser:AttributeList">
  <stsuuser:AttributeList>
         ....
      <!-- Puis l'attribut commonName -->
   <stsuuser:Attribute name="commonName"
                         type="http://exemple.com/federation/v1/commonName">
    <stsuuser:Value>
     <xsl:value-of
     select="//stsuuser:AttributeList/stsuuser:Attribute[@name='tagvalue_name']
           [@type='urn:ibm:names:ITFIM:5.1:accessmanager']/stsuuser:Value" />
    </stsuuser:Value>
   </stsuuser:Attribute>
   <!-- Puis l'attribut ssn -->
   <stsuuser:Attribute name="ssn" type="http://exemple.com/federation/v1/ssn">
    <stsuuser:Value>
     <xsl:value-of
     select="//stsuuser:AttributeList/stsuuser:Attribute[@name='tagvalue_ssn']
            [@type='urn:ibm:names:ITFIM:5.1:accessmanager']/stsuuser:Value" />
    </stsuuser:Value>
   </stsuuser:Attribute>
            ....
     </stsuuser:AttributeList>
 </xsl:template>
```

Figure 41. Exemple de code XSL présentant l'affectation d'attributs facultatifs pour un jeton Liberty

4. Il est à noter que l'élément GroupList de In-STSUUSER n'est pas lu par le module de jeton. Cependant, les informations contenues dans cet élément peuvent, le cas échéant, servir à remplir les attributs personnalisés de Out-STSUUSER.

   La figure 42 présente l'affectation facultative d'une valeur GroupList à un attribut. Cet exemple de code est issu du fichier de mappage d'application de démonstration, ip_liberty.xsl.

```
<xsl:template match="//stsuuser:AttributeList">
  <stsuuser:AttributeList>
         ....
      <!-- Puis l'attribut role (peut être multiforme) -->
   <stsuuser:Attribute name="role"
                         type="http://exemple.com/federation/v1/role">
    <xsl:for-each select="//stsuuser:GroupList/stsuuser:Group">
     <stsuuser:Value>
      <xsl:value-of select="@name" />
     </stsuuser:Value>
    </xsl:for-each>
   </stsuuser:Attribute>
            ....
     </stsuuser:AttributeList>
 </xsl:template>
```

Figure 42. Exemple de code XSL présentant l'affectation facultative d'une valeur GroupList à un attribut d'un jeton Liberty

Mappage d'un jeton Liberty ou SAML 2 vers des données d'identification Tivoli Access Manager

Le fournisseur de services reçoit un jeton Liberty ou SAML 2. Le module de jeton, en mode de validation, crée un document In-STSUUSER à partir du jeton. Pour connaître les informations issues du jeton qui sont converties en un document In-STSUUSER, voir le tableau 103, à la page 354.

Tableau 103. Informations de jeton converties en document d'utilisateur universel STS

Informations de jeton	Elément In-STSUUSER	Obligatoire dans Out-STSUUSER ?
ID utilisateur obtenu à partir du service d'alias	Principal Attr: Name	Obligatoire
Attributs personnalisés supplémentaires	Liste des attributs	Facultatif

Il est à noter que le module de jeton ne remplit pas l'élément GroupList du document In-STSUUSER.

Le module de jeton lit le jeton et extrait l'élément NameIdentifier. Le module de jeton transmet l'élément NameIdentifier (alias) au service d'alias. Ce dernier convertit l'alias reçu en ID utilisateur Tivoli Access Manager local. Le module de jeton place l'ID utilisateur dans l'élément Principal du document In-STSUUSER.

Le service d'accréditation doit convertir ces informations en données d'identification Tivoli Access Manager de manière à prendre une décision d'autorisation sur la demande de l'identité utilisateur.

- L'alias NameIdentifier renvoyé sert à remplir l'attribut `name` de l'élément Principal. Il s'agit de l'ID utilisateur local.

  Pour obtenir un exemple d'affectation d'une valeur définie pour le nom de Principal, voir la figure 43. Cet exemple de code est issu du fichier de mappage d'application de démonstration, sp_liberty.xsl.

```
 <!-- Ce modèle remplace le nom de principal (correspondant à l'adresse
électronique dans la vérification SAML) par l'utilisateur "me_guest". -->
    <xsl:template match="//stsuuser:Principal/stsuuser:Attribute[@name='name']">
            <stsuuser:Attribute name="name"
                                type="urn:ibm:names:ITFIM:5.1:accessmanager">
             <stsuuser:Value>
<xsl:value-of
 select="//stsuuser:Principal/stsuuser:Attribute[@name='name']/stsuuser:Value" />
             </stsuuser:Value>
           </stsuuser:Attribute>
       </xsl:template>
```

Figure 43. Exemple de code XSL présentant l'affectation d'une valeur pour le nom de Principal d'un jeton Liberty

- D'autres informations issues du jeton servent à remplir la zone Attributes de l'élément AttributeList.

  Pour obtenir un exemple d'affectation facultative de valeurs supplémentaires aux attributs, voir la figure 44, à la page 355. Cet exemple de code est issu du fichier de mappage d'application de démonstration, sp_liberty.xsl.

```
<xsl:template match="//stsuuser:AttributeList">
  <stsuuser:AttributeList>
          ....
              ....
      <!-- Attribut tagvalue_sso -->
      <stsuuser:Attribute name="tagvalue_sso"
                           type="urn:ibm:names:ITFIM:5.1:accessmanager">
                     <stsuuser:Value>isSingleSignOn</stsuuser:Value>
      </stsuuser:Attribute>
      <!-- Attribut tagvalue_fedname -->
      <stsuuser:Attribute name="tagvalue_fedname"
                          type="urn:ibm:names:ITFIM:5.1:accessmanager">
                      <stsuuser:Value>libertyfed</stsuuser:Value>
      </stsuuser:Attribute>
              ....
              ....
     </stsuuser:AttributeList>
 </xsl:template>
```

Figure 44. Exemple de code XSL présentant l'affectation facultative d'attributs pour un jeton Liberty

Service d'alias Liberty

Les normes Liberty relatives aux protocoles de connexion unique exigent l'utilisation d'alias lorsqu'une identité d'utilisateur est envoyée dans un message échangé entre les partenaires d'une fédération de connexion unique. Les alias sont requis pour mieux garantir la confidentialité de l'utilisateur final lors de l'accès aux ressources d'un fournisseur de services.

Dans les spécifications, les alias sont appelés *identificateurs de nom*. L'identificateur du nom de tel ou tel utilisateur est enregistré lors de la fédération des comptes (liaison des comptes), puis utilisé dans tous les messages transmis entre les partenaires. Les alias sont générés au hasard et ne contiennent aucune information importante sur l'identité des utilisateurs.

Un identificateur de nom différent doit être affecté à chaque utilisateur pour les communications avec chaque partenaire. Le cas échéant, plusieurs identificateurs de nom peuvent être créés en fonction de chaque destination des messages. Par conséquent, l'alias d'un utilisateur varie selon que le fournisseur d'identité contacte le fournisseur de services ou inversement.

Le service d'alias fourni par Tivoli Federated Identity Manager gère les tâches de gestion des alias. Il rend la plupart des tâches de génération et d'échange d'alias invisibles à l'administrateur de fédération. Il assure les fonctions suivantes :

- Génération et association des alias aux utilisateurs locaux
- Recherche de l'identité d'un utilisateur local lorsqu'un alias provient d'un partenaire
- Recherche de l'alias d'un utilisateur local lorsque le fournisseur doit envoyer un message à un partenaire

Le service d'alias Tivoli Federated Identity Manager stocke les informations relatives aux alias dans un registre d'utilisateurs. Le service d'alias prend en charge les registres d'utilisateurs suivants :

- IBM Tivoli Directory Server
- Sun ONE

Pour chacun de ces serveurs LDAP, vous serez amené à définir certains paramètres de configuration après avoir créé la fédération Liberty.

Le service d'alias ne prend pas en charge les registres d'utilisateurs Lotus Domino ou Microsoft Active Directory. Vous pouvez écrire votre propre service d'alias pour l'utiliser avec ces registres.

Chapitre 25. Configuration d'une fédération Liberty

Pourquoi et quand exécuter cette tâche

Exécutez les tâches suivantes :

Procédure

1. «Création d'un fournisseur d'identité Liberty»
2. «Configuration d'un fournisseur de services Liberty», à la page 359
3. «Configuration d'un serveur point de contact WebSEAL pour la fédération Liberty», à la page 361
4. «Propriétés des propriétés de fédération Liberty», à la page 362
5. «Exportation des informations d'authentification de noeud final SOAP vers un partenaire Liberty», à la page 363
6. «Obtention des métadonnées auprès d'un partenaire de fédération Liberty», à la page 364
7. «Importation des informations d'authentification de noeud final SOAP à partir d'un partenaire Liberty», à la page 365
8. «Ajout d'un partenaire dans une fédération Liberty», à la page 367

Création d'un fournisseur d'identité Liberty

Procédure

1. Connectez-vous à la console de gestion et cliquez sur **Tivoli Federated Identity Manager → Configurer la connexion unique fédérée → Fédérations**. Les portlets IBM Domaines en cours et Fédérations apparaissent. Le portlet Fédérations affiche plusieurs boutons d'action.
2. Cliquez sur **Créer**. L'assistant de fédération démarre. Le panneau Informations générales s'affiche.
3. Indiquez le nom de la fédération et sélectionnez un rôle. Cliquez sur **Suivant**.
4. Entrez les informations sur la personne à contacter et cliquez sur **Suivant**.
5. Sélectionnez le protocole Liberty 1.1 ou Liberty 1.2 et cliquez sur **Suivant**. L'écran Serveur point de contact s'affiche.
6. Entrez les informations sur l'adresse du point de contact et cliquez sur **Suivant**.
7. Indiquez les profils à utiliser avec cette fédération. Une fois que vous avez terminé, cliquez sur **Suivant**.
   a. Sélectionnez au moins un des profils de connexion unique Liberty.

      Liberty prend en charge trois profils de connexion unique. Vous devez sélectionner au moins un profil. Vous avez également la possibilité de sélectionner les profils Artefact du navigateur (Browser Artifact) et POST du navigateur (Browser POST) lors de la configuration d'un fournisseur d'identité. Vous ne pouvez sélectionner qu'un profil lors de la configuration d'un fournisseur de services.
   b. Sélectionnez n'importe lequel des profils facultatifs à configurer :
      - **Register Name Identifier (RNI)**
      - **Federation Termination Notification (FTN)**
      - **Single Logout (SLO)**

- **Identity Provider Introduction**.

  Dans le cas de fournisseurs d'identité uniquement.

8. Le panneau Options de signature numérique s'affiche. Cochez ou décochez la case **Signer les messages Liberty**. Si vous choisissez de signer les messages Liberty, vous devez indiquer une clé ou un certificat à utiliser.

   Dans certains cas, lorsque vous ne cochez pas la case Signer les messages Liberty, vous devez néanmoins entrer une clé ou un certificat. Par exemple :

   - Lors de la sélection du profil Artefact du navigateur, vous devez indiquer une clé à utiliser pour signer les messages envoyés dans l'ensemble du canal de retour pour l'artefact.
   - Lorsque vous sélectionnez un des profils facultatifs et que vous indiquez que les communications SOAP doivent être lancées par le fournisseur de services, vous devez spécifier une clé ou un certificat.

9. Si vous avez besoin d'entrer une clé ou un certificat, sélectionnez un fichier de clés et tapez le mot de passe qui lui correspond. Cliquez sur **Liste des clés** pour afficher les clés ou les certificats contenus dans le fichier de clés sélectionné. Sélectionnez une clé et cliquez sur **Suivant**.

   - Le mot de passe correspondant au fichier de clés par défaut **DefaultKeyStore** est `testonly`.
   - Un exemple de clé est fourni à des fins de test uniquement. N'utilisez pas cette clé dans un environnement de production.

10. Configurez les propriétés des données Liberty :

    a. Une valeur par défaut est indiquée pour le **noeud final SOAP**. Utilisez cette valeur, sauf en cas de conflit de noeud final sur votre hôte.

    b. Définissez l'option **Durée maximale des messages Liberty**.

    c. Définissez l'option **Durée des artefacts Liberty**.

    d. Cochez ou décochez la case **Demander l'accord de fédération**.

    e. Lorsque le profil LECP a été sélectionné, indiquez des **fournisseurs LECP**.

    f. Lorsque le profil Identity Provider Introduction a été sélectionné, entrez les valeurs adaptées dans les zones **Domaine DNS commun** et **Nom d'hôte de domaine commun**.

    g. Cliquez sur **Suivant**.

    Le panneau de configuration du module de jeton Liberty s'affiche. Son contenu est identique pour les jetons Liberty v1.1 et les jetons Liberty v1.2.

11. Indiquez une valeur dans la zone **Durée de validité (en secondes) de la vérification après émission** et cliquez sur **Suivant**.

12. Le panneau Options de mappage d'identité s'affiche. Sélectionnez l'un des boutons d'option suivants.

    - Utiliser la transformation XSL pour le mappage d'identité

      Indique que vous comptez fournir un fichier XSL contenant le mappage d'identité requis.

      a. Lorsque vous sélectionnez cette option et cliquez sur **Suivant**, le panneau Mappage d'identité s'affiche. Dans la zone **Fichier XSLT contenant une règle de mappage d'identité**, entrez le nom d'un fichier du système de fichiers local qui contient la règle de mappage d'identité.

      Il s'agit du fichier que vous avez préparé avant de procéder à cette installation.

      Vous pouvez également localiser le fichier sur le système de fichiers local à l'aide du bouton **Parcourir**.

b. Cliquez sur **Suivant**.

   Une erreur s'affiche lorsque le fichier est introuvable ou ne contient aucune donnée XSLT (eXtensible Stylesheet Language Transform) valide.

- Utiliser l'instance de module de mappage personnalisée

  Indique que vous comptez fournir une instance de module de mappage personnalisée, que vous utiliserez à la place du fichier XSL.

  a. Lorsque vous sélectionnez l'option Utiliser l'instance de module de mappage personnalisée, un tableau des instances de module s'affiche. Cliquez sur le bouton d'option correspondant à l'instance de module à utiliser et cliquez sur **Suivant**.

  b. Le cas échéant, vous serez alors invité à indiquer des valeurs pour les propriétés de l'instance de module de mappage personnalisée. Sinon, le panneau affiche un message indiquant qu'aucune propriété ne doit être configurée pour l'instance de module indiquée.

13. Le panneau Récapitulatif s'affiche. Vérifiez que les paramètres de configuration sont corrects, puis cliquez sur **Terminer**. Le portlet Création de fédération terminée s'affiche.

Que faire ensuite

Si vous utilisez WebSEAL en tant que serveur point de contact, procédez maintenant à sa configuration. Ne quittez pas la console de gestion. Voir aussi :

- «Configuration d'un serveur point de contact WebSEAL pour la fédération Liberty», à la page 361

Configuration d'un fournisseur de services Liberty

Procédure

1. Connectez-vous à la console de gestion et cliquez sur **Tivoli Federated Identity Manager → Configurer la connexion unique fédérée → Fédérations**. Les portlets IBM Domaines en cours et Fédérations apparaissent. Le portlet Fédérations affiche plusieurs boutons d'action.
2. Cliquez sur **Créer**. L'assistant de fédération démarre. Le panneau Informations générales s'affiche.
3. Indiquez le nom de la fédération et sélectionnez un rôle. Cliquez sur **Suivant**.
4. Entrez les informations sur la personne à contacter et cliquez sur **Suivant**.
5. Sélectionnez le protocole Liberty 1.1 ou Liberty 1.2 et cliquez sur **Suivant**. L'écran Serveur point de contact s'affiche.
6. Entrez les informations sur l'adresse du point de contact et cliquez sur **Suivant**.
7. Indiquez les profils à utiliser avec cette fédération. Une fois que vous avez terminé, cliquez sur **Suivant**.

   a. Sélectionnez au moins un des profils de connexion unique Liberty.

      Liberty prend en charge trois profils de connexion unique. Vous devez sélectionner au moins un profil. Vous avez également la possibilité de sélectionner les profils Artefact du navigateur (Browser Artifact) et POST du navigateur (Browser POST) lors de la configuration d'un fournisseur d'identité. Vous ne pouvez sélectionner qu'un profil lors de la configuration d'un fournisseur de services.

   b. Sélectionnez n'importe lequel des profils facultatifs à configurer :

      - **Register Name Identifier (RNI)**

- **Federation Termination Notification (FTN)**
- **Single Logout (SLO)**
- **Identity Provider Introduction**.

  Dans le cas de fournisseurs d'identité uniquement.

8. Le panneau Options de signature numérique s'affiche. Cochez ou décochez la case **Signer les messages Liberty**. Si vous choisissez de signer les messages Liberty, vous devez indiquer une clé ou un certificat à utiliser.

   Dans certains cas, lorsque vous ne cochez pas la case Signer les messages Liberty, vous devez néanmoins entrer une clé ou un certificat. Par exemple :

   - Lors de la sélection du profil Artefact du navigateur, vous devez indiquer une clé à utiliser pour signer les messages envoyés dans l'ensemble du canal de retour pour l'artefact.
   - Lorsque vous sélectionnez un des profils facultatifs et que vous indiquez que les communications SOAP doivent être lancées par le fournisseur de services, vous devez spécifier une clé ou un certificat.
9. Si vous avez besoin d'entrer une clé ou un certificat, sélectionnez un fichier de clés et tapez le mot de passe qui lui correspond. Cliquez sur **Liste des clés** pour afficher les clés ou les certificats contenus dans le fichier de clés sélectionné. Sélectionnez une clé et cliquez sur **Suivant**.
   - Le mot de passe correspondant au fichier de clés par défaut **DefaultKeyStore** est `testonly`.
   - Un exemple de clé est fourni à des fins de test uniquement. N'utilisez pas cette clé dans un environnement de production.
10. Configurez les paramètres du fournisseur de services de profil Liberty :

    Remarque : Pour plus d'informations sur chacune des propriétés affichées dans cet écran, voir .

    a. Si vous avez sélectionné un profil Liberty facultatif (Register Name Identifier, Federation Termination Notification ou Single Logout) et que vous avez choisi SOAP/HTTP comme protocole de communication, vous devez indiquer un noeud final SOAP. Une valeur par défaut est fournie. Vous pouvez valider la valeur par défaut, sauf si vous disposez d'une configuration spécifique qui nécessite un noeud final SOAP différent.

    b. Indiquez une valeur dans la zone **Durée maximale des messages Liberty (en secondes)**.

    c. Sélectionnez ou désélectionnez l'option **La connexion unique est passive (pas d'interaction entre le fournisseur d'identité et l'utilisateur)**.

    d. Sélectionnez ou désélectionnez l'option **Forcer le fournisseur d'identité à authentifier l'utilisateur**.

    e. Si vous avez sélectionné le profil de connexion unique LECP, indiquez un **fournisseur LECP**. Cliquez sur **Suivant**.
11. Le panneau Options de mappage d'identité s'affiche. Sélectionnez l'un des boutons d'option suivants.
    - Utiliser la transformation XSL pour le mappage d'identité

      Indique que vous comptez fournir un fichier XSL contenant le mappage d'identité requis.

      a. Lorsque vous sélectionnez cette option et cliquez sur **Suivant**, le panneau Mappage d'identité s'affiche. Dans la zone **Fichier XSLT contenant une règle de mappage d'identité**, entrez le nom d'un fichier du système de fichiers local qui contient la règle de mappage d'identité.

Il s'agit du fichier que vous avez préparé avant de procéder à cette installation.

Vous pouvez également localiser le fichier sur le système de fichiers local à l'aide du bouton **Parcourir**.

b. Cliquez sur **Suivant**.

Une erreur s'affiche lorsque le fichier est introuvable ou ne contient aucune donnée XSLT (eXtensible Stylesheet Language Transform) valide.

- Utiliser l'instance de module de mappage personnalisée

  Indique que vous comptez fournir une instance de module de mappage personnalisée, que vous utiliserez à la place du fichier XSL.

  a. Lorsque vous sélectionnez l'option Utiliser l'instance de module de mappage personnalisée, un tableau des instances de module s'affiche. Cliquez sur le bouton d'option correspondant à l'instance de module à utiliser et cliquez sur **Suivant**.

  b. Le cas échéant, vous serez alors invité à indiquer des valeurs pour les propriétés de l'instance de module de mappage personnalisée. Sinon, le panneau affiche un message indiquant qu'aucune propriété ne doit être configurée pour l'instance de module indiquée.

12. Le panneau Récapitulatif s'affiche. Vérifiez que les paramètres de configuration sont corrects, puis cliquez sur **Terminer**. Le portlet Création de fédération terminée s'affiche.
13. Cliquez sur **Redémarrer WebSphere**.

Que faire ensuite

Si vous utilisez WebSEAL en tant que serveur point de contact, procédez maintenant à sa configuration. Ne quittez pas la console de gestion. Voir aussi :

- «Configuration d'un serveur point de contact WebSEAL pour la fédération Liberty»

Configuration d'un serveur point de contact WebSEAL pour la fédération Liberty

Si vous envisagez d'utiliser WebSEAL en tant que serveur point de contact, vous devez le configurer pour la fédération Liberty.

Avant de commencer

L'assistant de fédération comporte un bouton qui vous permet d'obtenir un utilitaire de configuration.

Pourquoi et quand exécuter cette tâche

Vous devez obtenir l'utilitaire, puis l'exécuter. Procédez comme suit :

Procédure

1. Sur la console de gestion, cliquez sur **Télécharger l'outil de configuration Tivoli Access Manager**.
2. Enregistrez l'outil de configuration sur le système de fichiers de l'ordinateur hébergeant le serveur WebSEAL.
3. Revenez à la console de gestion et cliquez sur **Terminé** pour revenir au panneau Fédérations.

Remarque : La console de gestion vous offre la possibilité d'ajouter immédiatement un partenaire, mais pour cette configuration initiale de la fédération, nous commencerons par exécuter d'abord les autres tâches.

4. Démarrez l'outil de configuration depuis une ligne de commande. La syntaxe est la suivante :

   ```
   java -jar /rép_téléchargement/tfimcfg.jar -cfgfile webseald-nom_instance.conf
    -action tamconfig
   ```

   Vous aurez besoin de l'ID (par défaut : sec_master) et du mot de passe de l'utilisateur d'administration Tivoli Access Manager. L'utilitaire configure les noeuds finals sur le serveur WebSEAL, crée une jonction WebSEAL, relie les listes de contrôle d'accès adaptées et active les méthodes d'authentification adéquates.

Exemple

Par exemple, lorsque vous avez mis le fichier tfimcfg.jar dans le répertoire `/tmp` et que le nom de l'instance WebSEAL est `default`, la commande est la suivante :

```
java -jar /tmp/tfimcfg.jar -cfgfile webseald-default -action tamconfig
```

Pour plus d'informations, accédez à l'adresse suivante :

- Annexe A, «Référence de tfimcfg», à la page 533

Que faire ensuite

La prochaine tâche consiste à exporter les propriétés de votre fédération Liberty dans un fichier. Voir «Propriétés des propriétés de fédération Liberty».

Configuration de WebSphere en tant que serveur point de contact

Tivoli Federated Identity Manager est configuré par défaut pour utiliser Tivoli Access Manager WebSEAL en tant que serveur point de contact. Pour configurer WebSphere en tant que serveur point de contact, vous devez procéder à une modification de la configuration.

Procédure

1. Connectez-vous à la console d'administration.
2. Cliquez sur Tivoli Federated Identity Manager > Gestion de la configuration > Point de contact
3. Sélectionnez **WebSphere**
4. Cliquez sur **Activer**.

Résultats

Le serveur WebSphere est désormais configuré en tant que point de contact.

Propriétés des propriétés de fédération Liberty

Pourquoi et quand exécuter cette tâche

Pour rejoindre une fédération hébergée par un autre partenaire commercial, vous devez fournir vos propriétés de configuration de fédération. Utilisez la console de gestion pour générer un fichier de métadonnées contenant les propriétés de votre fédération. Transmettez ce fichier à votre partenaire de fédération.

Procédure

1. Connectez-vous à la console de gestion. Cliquez sur **Tivoli Federated Identity Manager → Configurer la connexion unique fédérée → Fédérations**.
2. Le panneau Fédérations s'affiche. Sélectionnez votre fédération Liberty dans le tableau.
3. Cliquez sur **Exporter**. Le navigateur affiche une fenêtre de message qui vous invite à sauvegarder le fichier contenant les données exportées. Cliquez sur **OK**. La fenêtre de téléchargement du navigateur vous invite à entrer un emplacement de sauvegarde du fichier.
4. Sélectionnez un répertoire et un nom de fichier et cliquez sur **Sauvegarder**. Placez ce fichier dans un emplacement facilement accessible.

Que faire ensuite

Si votre partenaire commercial souhaite importer les informations de configuration correspondant à cette fédération, vous devez lui fournir ce fichier.

Exportation des informations d'authentification de noeud final SOAP vers un partenaire Liberty

fournissez à votre partenaire les clés, certificats, noms d'utilisateur ou mots de passe nécessaires pour établir des communications SSL sur les ports SOAP.

Avant de commencer

Remarque : La sécurisation des ports SOAP avec le protocole SSL, ainsi que l'usage afférent de clés, certificats, noms d'utilisateur ou mots de passe n'est pas obligatoire, mais cette pratique est généralement recommandée afin d'optimiser la sécurité des réseaux.

Pourquoi et quand exécuter cette tâche

Liberty est doté d'un canal de retour SOAP utilisé avec le profil de connexion unique Artefact du navigateur et peut éventuellement être utilisé avec d'autres profils Liberty qui prennent en charge les liaisons SOAP. Le canal de retour SOAP peut, en option, être protégé à l'aide de communications SSL (via des noeuds finals HTTPS). L'utilisation de SSL est commune à tous les noeuds finals SOAP.

Pour les fédérations Liberty, il se peut que vous ayez également besoin de fournir des informations d'authentification (certificats et informations d'authentification de base) à votre partenaire, à des fins d'accès aux noeuds finals SOAP membres de la fédération Liberty.

Cette tâche est exécutée en dehors de console de gestion.

Remarque : Si votre fédération n'utilise pas le protocole SSL pour sécuriser les ports SOAP, vous pouvez ignorer cette tâche.

Procédure

1. Fournissez à votre partenaire un certificat de validation lui permettant de valider les communications SSL que vous lui fournissez, lorsque des messages lancés par le partenaire sont reçus par son noeud final SOAP.

2. Si vous souhaitez que votre partenaire s'authentifie en tant que client, vous devez indiquer s'il est tenu de recourir à une authentification par certificat client ou à une authentification de base. Une seule forme d'authentification peut être spécifiée.

   Authentification par certificat client

   - Lorsque vous exigez une authentification par certificat client, votre partenaire et vous-même devez déterminer quel certificat doit être présenté lors de l'établissement de la session SSL. Le choix d'un certificat est une décision métier. Il peut s'agir soit d'un certificat qui est déjà en possession de votre partenaire, soit d'un certificat que vous lui fournissez.

   Authentification de base

   - Lorsque vous exigez une authentification de base, vous devez fournir un nom d'utilisateur et un mot de passe à votre partenaire afin d'établir une session authentifiée.

Obtention des métadonnées auprès d'un partenaire de fédération Liberty

Si vous souhaitez ajouter votre partenaire commercial en tant que partenaire de votre fédération de connexion unique Liberty, vous devez obtenir auprès de celui-ci les informations de configuration nécessaires relatives à sa fédération Liberty.

Avant de commencer

Une fédération Liberty doit avoir été déjà installée et configurée par votre partenaire. La fédération de votre partenaire joue le rôle opposé à celui de votre fédération. Si, par exemple, votre fédération est configurée en tant que fournisseur d'identité, la fédération de votre partenaire l'est en tant que fournisseur de services.

Pourquoi et quand exécuter cette tâche

Procédure

1. Votre partenaire doit exporter les informations de configuration sur la fédération Liberty dans un fichier de métadonnées.

   Le partenaire utilise la console de gestion Tivoli Federated Identity Manager pour exporter les paramètres de configuration vers le fichier de métadonnées. Il s'agit de la même fonctionnalité que celle utilisée pour fournir vos paramètres de configuration au partenaire.

   La fonction d'exportation définit les fichiers de métadonnées d'après une convention de dénomination reposant sur le nom de cette fédération, complété d'un horodatage. L'administrateur peut remplacer le nom par défaut du fichier de métadonnées et définir un nom arbitraire.

2. Votre partenaire vous fournit le fichier de métadonnées.

   Cette action a lieu en dehors de console de Tivoli Federated Identity Manager. Votre partenaire utilise tout processus convenu dans le cadre de l'accord d'échange préalablement négocié entre les partenaires.

3. Placez le fichier de métadonnées sur le système de fichiers local dans lequel la configuration de la fédération Liberty est conservée. Vous pouvez indiquer n'importe quel emplacement pour le fichier de métadonnées. Vous avez à présent terminé l'étape préparatoire. Vous utiliserez ultérieurement la console de gestion de Tivoli Federated Identity Manager pour ajouter le partenaire à votre fédération Liberty. La console est dotée d'un assistant d'ajout de

partenaire qui vous invite à spécifier le nom du fichier contenant les métadonnées du partenaire. La documentation vous guidera tout au long de cette tâche le moment venu.

Importation des informations d'authentification de noeud final SOAP à partir d'un partenaire Liberty

Pourquoi et quand exécuter cette tâche

Liberty est doté d'un canal de retour SOAP utilisé avec le profil de connexion unique Artefact du navigateur et peut éventuellement être utilisé avec d'autres profils Liberty qui prennent en charge les liaisons SOAP. Le canal de retour SOAP peut, en option, être protégé à l'aide de communications SSL (via des noeuds finals HTTPS). L'utilisation de SSL est commune à tous les noeuds finals SOAP.

Pour les fédérations Liberty, il se peut que vous ayez besoin d'informations d'authentification (certificats et informations d'authentification de base) de la part de votre partenaire, à des fins d'accès aux noeuds finals SOAP membres de la fédération Liberty.

Cette tâche est exécutée en dehors de console de gestion.

Remarque : Si la fédération de votre partenaire n'utilise pas le protocole SSL pour sécuriser les ports SOAP, vous pouvez ignorer cette tâche.

Procédure

1. Obtenez de la part de votre partenaire un certificat de validation permettant de valider les communications SSL provenant de votre partenaire, lorsque des messages lancés par le partenaire sont reçus par votre noeud final SOAP.
2. Obtenez de la part de votre partenaire l'exigence éventuelle pour votre client de s'authentifier lorsqu'il souhaite entrer en contact avec le noeud final SOAP de votre partenaire.

   Si votre partenaire souhaite voir votre client s'authentifier, il doit vous indiquer si vous devez recourir à une authentification par certification client ou à une authentification de base. Une seule forme d'authentification peut être spécifiée.

   Authentification par certificat client

   - Lorsque votre partenaire exige une authentification de certificat client, le partenaire et vous-même devez déterminer quel certificat doit être présenté lors de l'établissement de la session SSL. Le choix d'un certificat est une décision métier. Il doit s'agir d'un certificat qui est déjà en votre possession, ou de celui qui vous a été fourni dans ce but par votre partenaire.

   Authentification de base

   - Lorsque le partenaire exige une authentification de base, il doit vous fournir le nom d'utilisateur et le mot de passe à présenter afin d'établir une session authentifiée.
3. Lorsque votre partenaire utilise des communications SSL destinées à des ports SOAP, vous devez importer le certificat obtenu auprès de votre partenaire. Vous pouvez importer le certificat dans n'importe quel fichier de clés géré par le service de clés de Tivoli Federated Identity Manager.

   Remarque : Tivoli Federated Identity Manager fournit un fichier de clés par défaut (DefaultTrustedKeystore) qui contient quelques certificats de CA

courants que vous pouvez utiliser sous forme de certificats de validation. Cependant, vous devez dans la plupart des cas importer un certificat obtenu auprès de votre partenaire.

a. Cliquez sur **Tivoli Federated Identity Manager -> Service de clés**.

   Le panneau Fichiers de clés s'affiche.

b. Sélectionnez un fichier de clés dans le tableau des fichiers de clés. Le bouton **Afficher les clés** est activé.

c. Cliquez sur **Afficher les clés**. Le panneau Clés s'affiche. Il répertorie les éléments du fichier de clés sélectionné.

d. Cliquez sur le bouton **Importer**. L'assistant de clés démarre et affiche le panneau Format de fichier de clés.

e. Sélectionnez le **format de fichier de clés** adapté au fichier à importer.

   (PEM)
   (Privacy-Enhanced Message) Certificat public

   PKCS#12
   Public Key Cryptography Standard 12 : norme d'échange d'informations personnelles

f. Pour PKCS#12, indiquez si le fichier de clés contient plusieurs paires de clés.

   1) Sélectionnez la zone **Contient plusieurs paires de clés**, le cas échéant.
   2) Désélectionnez (supprimez la marque de sélection) la zone **Contient plusieurs paires de clés** lorsqu'une seule paire de clés est disponible. L'assistant de clé importe automatiquement la clé.

g. Cliquez sur **Suivant**. L'écran Importer la clé s'affiche.

h. Entrez un chemin d'accès complet dans la zone **Emplacement du fichier de stockage de clés**.

   Cette zone s'affiche pour tous les types de format.

   Vous pouvez également cliquer sur **Parcourir** pour localiser le fichier sur le système de fichiers.

i. Si vous y êtes invité, entrez le **mot de passe** du fichier de stockage de clés.

   Remarque : Cette zone ne s'affiche que pour le format PKCS#12.

j. Si vous y êtes invité, entrez le nom de la clé dans la zone **Entrez le nom de la clé à importer**.

   Remarque : Cette zone ne s'affiche que pour les fichiers au format PKCS#12 qui contiennent plusieurs paires de clés.

k. Entrez une chaîne désignant la nouvelle clé dans la zone **Intitulé de la nouvelle clé**.

   Cette zone s'affiche pour tous les types de format.

l. Cliquez sur **Terminer** pour quitter l'assistant.

4. Lorsque votre partenaire requiert l'authentification de base client, vous devez conserver le nom d'utilisateur et le mot de passe. Après création de votre fédération, lorsque vous utilisez la console de gestion pour ajouter un partenaire, l'assistant de partenaire vous invite à indiquer ces valeurs. Elles ne sont pas nécessaires dans les autres cas.

Ajout d'un partenaire dans une fédération Liberty

Procédure

1. Copiez le fichier de métadonnées du partenaire vers un emplacement facilement accessible sur votre ordinateur. Exemple : /tmp.

   Remarque : Lorsque le partenaire utilise également Tivoli Federated Identity Manager, ce fichier a été créé sur l'ordinateur du partenaire via la console de gestion afin d'exporter les propriétés de la fédération.
2. Connectez-vous à IBM Integrated Solutions Console et cliquez sur **Tivoli Federated Identity Manager → Configurer la connexion unique fédérée → Partenaires**. L'assistant de partenaire de fédération démarre et affiche l'écran Sélection de fédération.
3. Cliquez sur le bouton d'option en regard de la fédération Liberty et cliquez sur **Suivant**. Le panneau Entrée de métadonnées s'affiche.
4. Dans la zone Fichier de métadonnées Liberty du partenaire, entrez le chemin complet du fichier de métadonnées (sur l'ordinateur local), puis cliquez sur **Suivant**. Par exemple :

   ```
   /tmp/libertyfed11_metadata_sp.xml
   ```
5. La tâche de configuration qui suit changera selon que les métadonnées importées contiennent ou non des informations sur une clé ou un certificat.

   En général, les métadonnées importées contiennent une clé que vous devez importer vers un fichier de clés existant.

   - Lorsque les métadonnées importées contiennent des informations relatives à une clé ou un certificat, le panneau Clé partenaire s'affiche. Passez à l'étape 6.
   - Lorsque les métadonnées importées ne contiennent *aucune* information sur une clé ou un certificat, le panneau Validation de certificat serveur pour SOAP s'affiche. Passez à l'étape 7.
6. Entrez les informations requises dans la zone Clé partenaire.

   Remarque : Cette clé ou ce certificat sert à signer les messages Liberty et à signer ou valider les jetons Liberty. Cette clé ne permet pas de sécuriser les communications SOAP sur HTTPS.

   a. Sélectionnez un fichier de clés dans le tableau.
   b. Entrez le mot de passe dans la zone **Mot de passe du fichier de clés**.
   c. Entrez une valeur dans la zone **Entrez un intitulé pour la clé de votre partenaire**. Par exemple :

      ```
      benefits.exemple.com
      ```
   d. Sélectionnez ou désélectionnez la zone **Demander au partenaire de signer les messages Liberty**. Cliquez sur **Suivant**.
7. L'étape de configuration suivante changera selon que les métadonnées importées contiennent ou non un noeud final SOAP devant utiliser HTTPS. Choisissez l'une des actions suivantes :

   - Lorsque les métadonnées importées contiennent un noeud final SOAP indiqué pour l'utilisation de HTTPS, vous êtes invité à définir les clés ou certificats à utiliser. Passez à l'étape 8, à la page 368.
   - Si le noeud final SOAP n'utilise pas HTTPS, il n'est pas nécessaire de définir des clés ou certificats. Passez à l'étape 12, à la page 369.

Remarque : Dans un déploiement standard, vous devez définir des clés ou certificats à utiliser avec le noeud final SOAP. Pour optimiser la sécurité, il convient généralement de sécuriser ce noeud final via HTTPS.

8. Lorsque l'écran Validation de certificat serveur pour SOAP s'affiche, effectuez les étapes ci-dessous.
   a. Sélectionnez un élément dans le menu déroulant **Fichier de clés**.

      Tivoli Federated Identity Manager fournit un fichier de clés **DefaultTrustedKeyStore**. Si vous utilisez un des certificats de CA par défaut (en fonction du contrat que vous avez conclu avec votre partenaire), vous pouvez sélectionner ce fichier de clés. Dans le cas contraire, vous devez accéder au fichier de clés dans lequel vous avez placé le certificat obtenu du partenaire, afin de l'utiliser avec les communications SSL entre les noeuds finals SOAP.

      Dans un environnement de test ou de prototype, vous pouvez sélectionner **DefaultTrustedKeyStore**.
   b. Entrez le mot de passe dans la zone **Mot de passe du fichier de clés**.

      Le mot de passe par défaut de **DefaultTrustedKeyStore** est `testonly`.
   c. Cliquez sur **Liste des clés**.
   d. Cliquez sur le bouton d'option correspondant au certificat désiré, comme indiqué par la valeur de la colonne **Alias** dans le tableau des clés.

      Dans un environnement de test ou de prototype, vous pouvez sélectionner `testwebseal`
   e. Cliquez sur **Suivant**. Le panneau Authentification client pour SOAP s'affiche.
9. Vous êtes invité à indiquer si le partenaire requiert *l'authentification par certificat client* ou *l'authentification de base client*. Le partenaire ne peut exiger qu'une seule de ces méthodes d'authentification. Lorsqu'un des types d'authentification affiché dans l'assistant est sélectionné, les entrées correspondant à l'autre type d'authentification sont désactivées.
   - Si le partenaire requiert l'authentification par certificat client, passez à l'étape 10.
   - Si le partenaire requiert l'authentification de base client, passez à l'étape 11.
10. Indiquez les valeurs d'authentification du certificat client.
    a. Cochez la case **Le partenaire requiert l'authentification par certificat client**.
    b. Sélectionnez un élément dans le menu **Fichier de clés**.

       Il s'agit du fichier de clés dans lequel vous avez placé le certificat à utiliser lors de l'authentification par certificat client.
    c. Entrez le mot de passe dans la zone **Mot de passe du fichier de clés**.
    d. Cliquez sur **Liste des clés**.
    e. Sélectionnez le bouton d'option correspondant à la clé appropriée dans le tableau des clés. Cliquez sur **Suivant**.
    f. Passez à la section 12, à la page 369.
11. Indiquez les valeurs d'authentification de base client.
    a. Cochez la case **Le partenaire requiert l'authentification de base client**.
    b. Entrez le **nom d'utilisateur** et le **mot de passe** que vous avez obtenus de votre partenaire. Cliquez sur **Suivant**.
    c. Passez à la section 12, à la page 369.

12. Le panneau qui doit ensuite s'afficher est fonction de votre rôle de fédération (fournisseur d'identité ou fournisseur de services) et de votre version de Liberty (1.1 ou 1.2). Dans la plupart des cas, vous allez définir des propriétés pour le jeton Liberty. Sélectionnez l'instruction suivante qui correspond à votre configuration :
    - Si vous ajoutez un fournisseur de services partenaire dans une fédération de fournisseurs d'identité, passez à l'étape 13.
    - Si vous ajoutez un fournisseur d'identité partenaire dans une fédération de fournisseurs de services, passez à l'étape 14.
13. Indiquez les données de configuration du module de jeton pour l'ajout d'un fournisseur de services partenaire à une fédération de fournisseurs d'identité. Les données requises sont les mêmes pour Liberty version 1.1 et Liberty version 1.2. Le panneau de configuration du module de jeton Liberty v1.1 ou v1.2 s'affiche.
    a. Dans la zone **Entrez les types d'attributs suivants (si une étoile "*" est indiquée, tous les types sont inclus)**, définissez les types d'attributs à inclure dans le jeton Liberty.

       Vous pouvez accepter l'entrée par défaut de l'astérisque (*) pour inclure tous les types ou spécifiez des types d'attributs.
    b. Cliquez sur **Suivant**. Passez à la section 12.
14. Indiquez les données de configuration du module de jeton pour l'ajout d'un fournisseur d'identité partenaire à une fédération de fournisseurs de services. Sélectionnez une action correspondant à la version du protocole Liberty (version 1.1 ou 1.2).
    - Lors de l'ajout d'un fournisseur d'identité partenaire à une fédération de fournisseurs de services utilisant Liberty version 1.1, aucune configuration du module de jeton n'est nécessaire. Le panneau Mappage d'identité s'affiche. Passez à la section 15.
    - Pour ajouter un fournisseur d'identité partenaire à une fédération de fournisseurs de services utilisant Liberty v1.2, procédez comme suit :

    a. Vous pouvez éventuellement indiquer une valeur dans la zone **Nom d'utilisateur à employer pour les utilisateurs anonymes**. Si vous n'utilisez pas cette fonction de Liberty, vous pouvez laisser cette zone à blanc. .
    b. Cliquez sur **Suivant**. Le panneau Mappage d'identité s'affiche. Passez à l'étape 15.
15. Choisissez l'action correspondant à l'utilisation que vous faites d'une règle de mappage d'identité :
    - N'indiquez pas de règle si vous souhaitez utiliser la règle de mappage d'identité par défaut que vous avez entrée dans l'assistant de création de fédération. Cliquez sur **Suivant**.
    - Si vous disposez d'un fichier de mappage personnalisé à utiliser avec ce partenaire, entrez le chemin d'accès au fichier. Cliquez sur **Importer**. Cliquez sur **Suivant**.

    Le panneau Récapitulatif s'affiche.
16. Vérifiez que les paramètres sont corrects, puis cliquez sur **Terminer**.

    Le panneau Ajout de partenaire terminé s'affiche.
17. Cliquez sur **Activer le partenaire** pour activer ce partenaire.

    Le partenaire a été ajouté à la fédération, mais il est désactivé par défaut par mesure de sécurité. Vous devez activer le partenaire.

Configuration du service d'alias pour Liberty

Pourquoi et quand exécuter cette tâche

Le service d'alias doit être configuré pour le même registre d'utilisateurs que le service de gestion Tivoli Federated Identity Manager. Les instructions suivantes décrivent la configuration du serveur LDAP IBM Tivoli Directory Server.

Procédure

1. «Création d'un suffixe LDAP pour le service d'alias»
2. «Configuration des paramètres du serveur LDAP»

Création d'un suffixe LDAP pour le service d'alias

Pourquoi et quand exécuter cette tâche

Vous devez créer un suffixe LDAP `cn=itfim` pour permettre au service d'alias d'accéder au registre d'utilisateurs LDAP.

Procédure

1. Arrêtez le serveur LDAP d'IBM.

   UNIX

   ```
   # ibmdirctl -D cn=root -w passw0rd stop
   ```

   Windows

   Utilisez l'icône Services.

2. Ajoutez le suffixe :

   ```
   # idscfgsuf -s "cn=itfim"
   ```

3. Démarrez le serveur LDAP d'IBM.

   UNIX

   ```
   # ibmdirctl -D cn=root -w passw0rd start
   ```

   Windows

   Utilisez l'icône Services.

4. Utilisez **ldapmodify** pour mettre à jour le fichier du schéma LDAP. Par exemple, sous UNIX ou Linux :

   - IBM Tivoli Directory Server

     ```
     ldapmodify -D cn=root -w passw0rd -f
       /opt/IBM/FIM/etc/itfim-secuser.ldif
     ```

   - Serveur Sun ONE Directory :

     ```
     ldapmodify -D cn=root -w passw0rd -f
        /opt/IBM/FIM/etc/itfim-secuser-sunone.ldif
     ```

Configuration des paramètres du serveur LDAP

Pourquoi et quand exécuter cette tâche

Le service d'alias est utilisé par le protocole Liberty. Le service d'alias communique avec le serveur du registre d'utilisateurs (LDAP) pour manipuler les informations relatives aux identités utilisateur. Vous devez configurer le service d'alias avec les paramètres LDAP appropriés.

Procédure

1. Cliquez sur **Tivoli Federated Identity Manager → Gestion des domaines → Paramètres du service d'alias**. Le panneau Paramètres du service d'alias s'affiche.
2. Dans la zone Suffixe principal, sous **Paramètres de recherche LDAP**, spécifiez la propriété pour le service d'alias à utiliser lors des recherches dans le registre utilisateur LDAP.

Tableau 104. Propriétés de recherche LDAP

Propriété	Description
Suffixe principal	Indique le suffixe racine dans lequel des paramètres du service d'alias sont écrits. Cette propriété ne peut comporter qu'une seule valeur (suffixe). Par exemple : `cn=itfim`

3. Définissez les propriétés de communication du service d'alias devant être utilisées lors de la communication avec les serveurs LDAP. Utilisez les options de menu de la section **Environnement LDAP** de la fenêtre pour définir les propriétés de communication.

Tableau 105. Propriétés de l'environnement LDAP

Propriété	Description
SSL activé	Utilisez cette case à cocher pour indiquer si les communications entre le service d'alias et les serveurs LDAP doivent être sécurisées grâce au protocole SSL (Secure Socket Layer). Si les serveurs LDAP sont configurés pour utiliser SSL, le service d'alias doit également utiliser ce protocole lorsqu'il communique avec eux. Sélectionnez **SSL activé** lorsque vous utilisez le protocole SSL. Dans le cas contraire, désactivez cette case.
Fichier de clés	Lorsque que la case **SSL activé** est cochée, sélectionnez un fichier de clés dans le menu **Fichier de clés**. Il s'agit du nom du fichier de clés sécurisé contenant le certificat de CA du serveur LDAP. Les certificats de CA de tous les serveurs LDAP doivent se trouver dans le même fichier de clés.

4. Définissez les paramètres de configuration relatifs à chaque serveur LDAP. Utilisez la section **Serveurs LDAP** de la fenêtre pour configurer les propriétés des serveurs LDAP utilisés par le service d'alias.

   Vous pouvez effectuer plusieurs actions de configuration à partir de cette section de la fenêtre. Pour chaque serveur LDAP, vous pouvez définir les valeurs d'un certain nombre de propriétés de configuration.

   - Cliquez sur **Ajouter** pour activer les zones de configuration LDAP du serveur sélectionné.
   - Cliquez sur **Sauvegarder** pour sauvegarder les propriétés LDAP que vous avez entrées dans les zones de configuration d'un serveur. Lorsque vous sauvegardez ces propriétés, la console entre le nom d'hôte et le numéro de port dans la zone **Hôtes LDAP**.

Tableau 106. Propriétés du serveur LDAP

Propriété	Description
Nom d'hôte LDAP	La boîte **Hôtes LDAP** contient la liste des serveurs configurés, par ordre de préférence. Le service d'alias tente d'abord de contacter le serveur figurant au début de la liste. S'il ne parvient pas à établir le contact, il essaie avec le serveur suivant. A l'aide de la flèche vers le haut et de la flèche vers le bas situées à droite de la boîte, déplacez les serveurs LDAP vers le haut ou vers le bas, par ordre de priorité.

Port	Port sur lequel le serveur LDAP écoute.
	
	Port par défaut pour les communications non-SSL :
	`389`
	
	Port par défaut pour les communications SSL :
	`636`

Nom distinctif de la connexion	Nom distinctif utilisé par le service d'alias pour établir une liaison avec le serveur LDAP. Valeur par défaut : `cn=root`
Mot de passe BIND	Mot de passe du nom distinctif indiqué dans la zone **DN Bind**.
Nom de la clé	Nom de la clé de chiffrement à utiliser lors de l'établissement de la communication SSL. Sélectionnez un nom de clé dans la liste des noms. Ces noms proviennent du fichier de clés indiqué dans la zone **Fichier de clés** de la section **Environnement LDAP** de cette fenêtre de configuration.
Nombre minimal de connexions	Nombre de connexions (binds ou liaisons) minimal que le service d'alias peut établir avec le serveur LDAP. La plus petite valeur acceptée est zéro (0). La valeur maximale acceptée correspond à la valeur maximale prise en charge par le type de données. La valeur par défaut est 2. Utilisez-la, sauf si vous devez l'augmenter.
Nombre maximal de connexions	Nombre de connexions (binds ou liaisons) maximal que le service d'alias peut établir avec le serveur LDAP. La valeur maximale acceptée correspond à la valeur maximale prise en charge par le type de données. La valeur par défaut est 10. Utilisez-la, sauf si vous avez besoin de l'augmenter.

5. Cliquez sur **OK** pour sauvegarder les propriétés de configuration et quitter la fenêtre.

Chapitre 26. Configuration d'une fédération de connexion unique WS-Federation

Vous devrez, lors de la configuration d'une fédération WS-Federation, spécifier des valeurs pour les propriétés de la fédération.

Le protocole WS-Federation constitue une solution Web de connexion unique normalisée et multifournisseur qui repose sur un ensemble de normes de services Web intégrés (WS*), parmi lesquels WS-Security, WS-Trust et WS-Federation. Lorsque vous configure Tivoli Federated Identity Manager, vous devez sélectionner le Profil passif WS-Federation.

Il convient que vous soyez familiarisé avec les documents relatifs aux normes WS-Federation avant de mettre en oeuvre une fédération de connexion unique. Les normes définissent les échanges de données et le traitement de messages. Vous devez déterminer les informations que vous devez fournir à vos partenaires commerciaux, ainsi que les informations que vos partenaires doivent vous remettre.

Web Services Federation Language (WS-Federation) :

`http://www.ibm.com/developerworks/library/ws-fed`

L'assistant de fédération vous invite à indiquer des valeurs pour un certain nombre de propriétés. La plupart d'entre elles peuvent être modifiées ultérieurement, après la création de la fédération.

Le choix du ou des profils à utiliser dépend à la fois des décisions en matière de règles commerciales et de l'architecture du réseau du point de vue de la sécurité. Les partenaires de la fédération doivent se mettre d'accord sur le choix des profils afin de permettre la connexion unique sur l'ensemble de la fédération. Ce choix doit être fait avant la configuration de la fédération.

SAML 2 prend en charge une gamme unique de profils de connexion unique. Les profils s'étendent au-delà des spécifications, pour permettre une connexion unique fédérée, et peuvent inclure d'autres fonctions, comme la déconnexion unique et l'arrêt de la fédération.

Rôles du fournisseur d'identité et du fournisseur de services

Au sein d'une fédération, chaque partenaire a un rôle. Il s'agit du rôle **Fournisseur d'identité** ou **Fournisseur de services**.

- Fournisseur d'identité

  Le fournisseur d'identité est un partenaire de fédération qui garantit l'identité des utilisateurs. Il authentifie un utilisateur et transmet un jeton d'authentification au fournisseur de services.

  Le fournisseur d'identité authentifie l'utilisateur soit directement, par exemple en validant un nom d'utilisateur et un mot de passe, soit indirectement, en validant une assertion sur l'identité de l'utilisateur présentée par un autre fournisseur d'identité.

  Le fournisseur d'identité gère les identités des utilisateurs afin de dégager le fournisseur de services de cette responsabilité.

- Fournisseur de services

  Le fournisseur de services est un partenaire de fédération qui fournit des services à l'utilisateur final. En général, il n'authentifie pas les utilisateurs, mais demande à un fournisseur d'identité de prendre les décisions liées à l'authentification. Les fournisseurs de services comptent sur les fournisseurs d'identité pour affirmer l'identité d'un utilisateur et pour gérer les identités des utilisateurs pour la fédération.

  Les fournisseurs de services peuvent gérer un compte local pour l'utilisateur, compte qui peut être désigné par un identificateur.

Profils de connexion unique WS-Federation

Les profils de connexion unique permettent à un client utilisant un navigateur Web d'accéder aux ressources d'une fédération WS-Federation 1.0 par une connexion unique. Généralement, l'utilisateur souhaite accéder à une ressource proposée par un fournisseur de services et doit s'authentifier auprès d'un fournisseur d'identité pour bénéficier de cet accès. Le profil offre à l'utilisateur Web un profil d'obtention d'une assertion d'authentification qui permet d'établir un contexte de sécurité dans la fédération. L'établissement du contexte de sécurité permet à un utilisateur d'accéder à plusieurs ressources de la fédération sans avoir à s'authentifier plusieurs fois.

WS-Federation prend en charge deux profils utilisables avec les sessions de connexion unique :

POST du navigateur (Browser POST)
Le profil du navigateur POST utilise un formulaire qui renvoie l'action à lui-même (self-posting form) pour échanger un artefact au cours de l'établissement et de l'utilisation d'une session sécurisée entre un fournisseur d'identité, un fournisseur de services et un client (navigateur).

Par défaut, WS-Federation prend en charge le profil POST du navigateur. Aucune configuration n'est requise.

Single logout (SLO, Déconnexion unique)
Ce profil met fin à toutes les sessions de connexion associées à un utilisateur au sein de la fédération. WS-Federation prend en charge la déconnexion unique par défaut. Aucune configuration n'est requise.

Propriétés de connexion unique WS-Federation

Domaine WS-Federation
Nom du domaine WS-Federation. Ce nom est un identificateur unique pour cette instance de Tivoli Federated Identity Manager. Il figure dans les assertions envoyées aux partenaires de fédération. Les partenaires n'acceptent ces assertions que s'ils trouvent un nom de domaine connu (c'est-à-dire défini). Une valeur par défaut est fournie. Par exemple :

```
https://idp.exemple.com/FIM/sps/wsfed/wsf
```

Dans l'exemple ci-dessus, la chaîne `wsfed` correspond au nom de la fédération. Le noeud final est automatiquement créé. Vous pouvez accepter le nom par défaut.

noeud final WS-Federation
Noeud final de toutes les demandes de service WS-Federation. Une valeur par défaut est fournie. Par exemple :

```
https://idp.ibm.com/FIM/sps/wsfed/wsf
```

Dans l'exemple ci-dessus, la chaîne `wsfed` correspond au nom de la fédération. Le noeud final est automatiquement créé. Vous pouvez accepter le nom par défaut.

Propriétés des jetons WS-Federation

Lorsque vous créez une fédération de connexion unique, vous devez configurer une instance de module de jeton de sécurité pour cette fédération. Le module de jeton correspond à un type de jeton de sécurité qui définit le format du jeton chiffré contenant les données d'identification des utilisateurs.

Le jeton est échangé entre le fournisseur d'identité et le fournisseur de services dans le cadre des services d'authentification et d'autorisation pour le traitement de chaque requête d'accès d'utilisateur.

Lorsque vous utilisez l'assistant de création de fédération pour générer une fédération de connexion unique WS-Federation, le type de jeton SAML 1 est automatiquement sélectionné à votre place.

Lorsque vous configurez un fournisseur d'identité, vous êtes invité à spécifier les propriétés du module de jeton. Si vous configurez un fournisseur de services, la spécification des propriétés du module de jeton n'est pas nécessaire.

Durée de validité (en secondes) d'une vérification avant sa date d'émission.
Elle est indiquée lors de la configuration de jeton, uniquement sur le fournisseur d'identité. Valeur par défaut : 60 secondes. Aucune valeur minimale ou maximale n'est requise.

Durée de validité (en secondes) de la vérification après émission
Nombre entier correspondant à la durée de validité, en secondes, de l'assertion. La valeur par défaut est de 60 secondes. Aucune valeur minimale ou maximale n'est requise. Il est indiqué lors de la configuration de jeton, uniquement sur le fournisseur d'identité.

Mappage d'identité WS-Federation

L'assistant de création de fédération vous invite à spécifier soit l'authentification par fichier de règle de mappage XSLT, soit via une instance de module de mappage personnalisée.

Le fichier de mappage XSLT ou l'instance de module de mappage personnalisée doivent être préparés avant la configuration de la fédération.

Transformation XSL pour le mappage d'identité
La sélection de ce bouton sur l'assistant indique que vous comptez fournir un fichier XSL contenant le mappage d'identité. Entrez le nom d'un fichier du système de fichiers local.

Instance de module de mappage personnalisée
La sélection de ce bouton sur l'assistant indique que vous comptez fournir une instance de module de mappage personnalisée, que vous utiliserez à la place du fichier XSL. Vous serez éventuellement invité à entrer les propriétés de configuration requises par l'instance du module de mappage personnalisée.

Mappage de données d'identification Tivoli Access Manager vers un jeton SAML 1

Ce scénario se produit lors de l'échange de messages entre des partenaires d'une fédération de connexion unique SAML 1.0, SAML 1.1 ou WS-Federation et lorsque des données d'identification utilisateur sont gérées par Tivoli Access Manager. Lorsqu'une demande d'utilisateur est reçue (par exemple, pour accéder à une ressource distante), le service d'accréditation prend contact avec Tivoli Access Manager et obtient des données Tivoli Access Manager relatives à l'identité de l'utilisateur.

Dans ce scénario, le module de données d'identification Tivoli Access Manager du service d'accréditation fonctionne en mode de validation. Dans ce mode, il convertit les données d'identification Tivoli Access Manager en un document d'utilisateur universel STS d'entrée (In-STSUUSER). Le document In-STSUUSER créé à partir du module d'accréditation Tivoli Access Manager contient toutes les informations issues des données d'identification (voir le tableau 107). Ces informations peuvent éventuellement être utilisées par le module de service d'accréditation qui va générer le jeton sortant.

Tableau 107. Entrées In-STSUUSER générées à partir de données d'identification Tivoli Access Manager

Données d'identification Tivoli Access Manager	**Elément In-STSUUSER**
ID utilisateur	Principal Attr: name
Domaine	Principal Attr: domain
ID registre	Principal Attr: registryid
UUID de l'utilisateur	Principal Attr: uuid
Nom du groupe	Nom du groupe
ID registre du groupe	Group Attr: registryid
UUID du groupe	Group Attr: uuid
Autres entrées de données d'identification xxx	Attrlist Attr: xxx

Le service d'accréditation consulte son entrée de configuration correspondant au partenaire de la fédération (par exemple, la destination qui héberge une ressource demandée). La configuration indique le type de jeton à créer. Dans ce cas, le type de jeton est SAML.

Le module de mappage d'identité convertit ensuite l'élément In-STSUUSER en un utilisateur universel STS de sortie (Out-STSUUSER). L'élément Out-STSUUSER doit contenir les informations requises par le module de jeton SAML de Tivoli Access Manager pour générer un jeton SAML.

L'élément Out-STSUUSER doit contenir les informations suivantes qui permettent au module de jeton SAML de générer un jeton SAML valide :

Tableau 108. Entrées Out-STSUUSER servant à générer un jeton SAML

Elément Out-STSUUSER	**Informations de jeton SAML**	**Obligatoire/ facultatif**
Principal Attr: Name	AuthenticationStatement/Subject/NameIdentifier	Obligatoire
Liste des attributs	Attributs personnalisés supplémentaires	Facultatif

Le module de mappage est responsable des opérations suivantes :

1. Mappage de l'élément Principal Attr Name dans In-STSUUSER vers une entrée de nom Principal dans Out-STSUUSER.

   Le type doit être valide pour SAML. Par exemple :

   ```
   urn:oasis:names:tc:SAML:1.0:assertion#emailAddress
   ```

   Pour obtenir un exemple de fichier de règles de mappage extrait du fichier de mappage d'application de démonstration, ip_saml_10.xsl, voir la figure 45.

```
<!--
 Ce modèle remplace l'intégralité de l'élément Principal par un élément qui ne
 contient que l'adresse électronique (à partir de ivcred tagvalue_email) et le
 type de données approprié pour SAML.
-->
<xsl:template match="//stsuuser:Principal">
 <stsuuser:Principal>
  <stsuuser:Attribute name="name"
                  type="urn:oasis:names:tc:SAML:1.0:assertion#emailAddress">
   <stsuuser:Value>
    <xsl:value-of
    select="//stsuuser:AttributeList/stsuuser:Attribute[@name='tagvalue_email']
            [@type='urn:ibm:names:ITFIM:5.1:accessmanager']/stsuuser:Value" />
   </stsuuser:Value>
  </stsuuser:Attribute>
 </stsuuser:Principal>
</xsl:template>
```

Figure 45. Exemple de code XSL présentant le mappage d'une valeur des données d'identification Tivoli Access Manager vers un nom Principal pour un jeton SAML

2. Paramétrage de la méthode d'authentification sur "password" (mot de passe), quelle que soit la valeur obtenue des données d'identification Tivoli Access Manager. Cette action est requise par la norme SAML.

   Pour obtenir un exemple de fichier de règles de mappage extrait du fichier de mappage d'application de démonstration, ip_saml_10.xsl, voir la figure 46, à la page 378.

```
<xsl:template match="//stsuuser:AttributeList">
  <stsuuser:AttributeList>
                ....
   <!-- D'abord, l'attribut AuthenticationMethod -->
   <stsuuser:Attribute name="AuthenticationMethod"
                          type="urn:oasis:names:tc:SAML:1.0:assertion">
    <stsuuser:Value>urn:oasis:names:tc:SAML:1.0:am:password</stsuuser:Value>
   </stsuuser:Attribute>
                ....
                ....
     </stsuuser:AttributeList>
 </xsl:template>
```

Figure 46. Exemple de code XSL présentant l'affectation d'une méthode d'authentification sous forme d'attribut pour un jeton SAML

3. Remplissage de l'instruction d'attribut de l'assertion SAML à l'aide des attributs de l'élément AttributeList dans In-STSUUSER. Ces informations deviennent des informations personnalisées du jeton SAML.

   Des attributs personnalisés peuvent être requis par les applications qui utilisent les informations à transmettre entre les partenaires d'une fédération.

   Pour une description du mappage des attributs personnalisés de l'exemple de fichier de mappage de l'application de démonstration Tivoli Federated Identity Manager, voir la figure 47.

```
<xsl:template match="//stsuuser:AttributeList">
  <stsuuser:AttributeList>
          ....
                ....
      <!-- Puis l'attribut commonName -->
   <stsuuser:Attribute name="commonName"
                          type="http://exemple.com/federation/v1/commonName">
    <stsuuser:Value>
     <xsl:value-of
     select="//stsuuser:AttributeList/stsuuser:Attribute[@name='tagvalue_name']
             [@type='urn:ibm:names:ITFIM:5.1:accessmanager']/stsuuser:Value" />
    </stsuuser:Value>
   </stsuuser:Attribute>

   <!-- Puis l'attribut ssn -->
   <stsuuser:Attribute name="ssn"
                          type="http://exemple.com/federation/v1/namevalue">
    <stsuuser:Value>
     <xsl:value-of
      select="//stsuuser:AttributeList/stsuuser:Attribute[@name='tagvalue_ssn']
             [@type='urn:ibm:names:ITFIM:5.1:accessmanager']/stsuuser:Value" />
    </stsuuser:Value>
   </stsuuser:Attribute>
                ....
    </stsuuser:AttributeList>
 </xsl:template>
```

Figure 47. Exemple de code XSL présentant l'affectation d'attributs facultatifs pour un jeton SAML

4. Il est à noter que l'élément GroupList de In-STSUUSER n'est pas lu par le module de jeton SAML. Cependant, les informations contenues dans cet élément peuvent, le cas échéant, servir à remplir les attributs personnalisés de Out-STSUUSER.

La figure 48 présente l'affectation facultative d'une valeur GroupList à un attribut. Cet exemple de code est issu du fichier de mappage d'application de démonstration, ip_saml_10.xsl.

```
<xsl:template match="//stsuuser:AttributeList">
  <stsuuser:AttributeList>
         ....
      <!-- Puis l'attribut role (peut être multiforme) -->
   <stsuuser:Attribute name="role" type="http://exemple.com/federation/v1/role">
    <xsl:for-each select="//stsuuser:GroupList/stsuuser:Group">
     <stsuuser:Value>
      <xsl:value-of select="@name" />
     </stsuuser:Value>
    </xsl:for-each>
   </stsuuser:Attribute>
            ....
    </stsuuser:AttributeList>
 </xsl:template>
```

Figure 48. Exemple de code XSL présentant l'affectation facultative d'une valeur GroupList à un attribut d'un jeton SAML

Mappage d'un jeton SAML 1 vers des données d'identification Tivoli Access Manager

Le fournisseur de services reçoit un jeton SAML. Le module de jeton SAML, en mode de validation, crée un document In-STSUUSER à partir du jeton SAML. Pour connaître les informations issues du jeton qui sont converties en un document In-STSUUSER, voir le tableau 109.

Remarque : Cette rubrique s'applique aux jetons SAML 1.0 et SAML 1.1.

Tableau 109. Informations de jeton SAML converties en document d'utilisateur universel STS

Informations de jeton SAML	Elément In-STSUUSER	Obligatoire pour Out-STSUUSER ?
AuthenticationStatement/Subject/ NameIdentifier	Principal Attr: Name	Obligatoire
Attributs personnalisés supplémentaires	Liste des attributs	Facultatif

Il est à noter que le module de jeton SAML ne remplit pas l'élément GroupList du document In-STSUUSER.

Le service d'accréditation doit convertir ces informations en données d'identification Tivoli Access Manager de manière à prendre une décision d'autorisation sur la demande de l'identité utilisateur. Le module de mappage d'identité convertit les données In-STSUUSER en un fichier XML Out-STSUUSER.

- L'élément NameIdentifier sert à remplir l'attribut `name` de l'élément Principal.

  Pour obtenir un exemple d'affectation d'une valeur définie pour le nom de Principal, voir la figure 49, à la page 380. Cet exemple de code est issu du fichier de mappage d'application de démonstration, sp_saml_1x.xsl.

```
<!--
  Ce modèle remplace le nom de principal (correspondant à l'adresse électronique
  dans la vérification SAML) par l'utilisateur "me_chris".
 -->
 <xsl:template match="//stsuuser:Principal/stsuuser:Attribute[@name='name']">
  <stsuuser:Attribute name="name" type="urn:ibm:names:ITFIM:5.1:accessmanager">
            <stsuuser:Value>me_chris</stsuuser:Value>
            </stsuuser:Attribute>
 </xsl:template>
```

Figure 49. Exemple de code XSL présentant l'affectation d'une valeur pour le nom de Principal d'un jeton SAML

- D'autres informations issues du jeton servent à remplir la zone Attributes de l'élément AttributeList.

  Pour obtenir un exemple d'affectation facultative de valeurs supplémentaires aux attributs, voir la figure 50. Cet exemple de code est issu du fichier de mappage d'application de démonstration, sp_saml_1x.xsl.

```
<xsl:template match="//stsuuser:AttributeList">
  <stsuuser:AttributeList>
         ....
      <!-- Attribut tagvalue_name -->
   <stsuuser:Attribute name="tagvalue_name"
                         type="urn:ibm:names:ITFIM:5.1:accessmanager">
    <stsuuser:Value>
    <xsl:value-of
  select="//stsuuser:AttributeList/stsuuser:Attribute[@name='commonName']
      [@type='http://exemple.com/federation/v1/commonName']/stsuuser:Value" />
    </stsuuser:Value>
   </stsuuser:Attribute>

   <!-- Attribut tagvalue_ssn -->
   <stsuuser:Attribute name="tagvalue_ssn"
                         type="urn:ibm:names:ITFIM:5.1:accessmanager">
    <stsuuser:Value>
     <xsl:value-of
              select="//stsuuser:AttributeList/stsuuser:Attribute[@name='ssn']
          [@type='http://exemple.com/federation/v1/namevalue']/stsuuser:Value" />
    </stsuuser:Value>
   </stsuuser:Attribute>
              ....
     </stsuuser:AttributeList>
 </xsl:template>
```

Figure 50. Exemple de code XSL présentant l'affectation facultative d'attributs pour un jeton SAML

Chapitre 27. Configuration d'une fédération de connexion unique WS-Federation

Pour configurer une fédération à connexion unique WS-Federation, vous devez créer la fédération, y ajouter votre partenaire, puis fournir à celui-ci les informations de configurations issues de votre nouvelle fédération.

Pourquoi et quand exécuter cette tâche

Suivez les instructions indiquées dans chacune des sections suivantes :

Procédure

1. «Création d'une fédération de connexion unique WS-Federation»
2. «Configuration de WebSEAL en tant que serveur point de contact», à la page 382
3. «Exportation des propriétés WS-Federation», à la page 384
4. «Obtention des informations de configuration auprès d'un partenaire WS-Federation», à la page 384
5. «Ajout d'un partenaire dans une fédération de connexion unique WS-Federation», à la page 386

Création d'une fédération de connexion unique WS-Federation

Pourquoi et quand exécuter cette tâche

- Chapitre 26, «Configuration d'une fédération de connexion unique WS-Federation», à la page 373.

Procédez comme suit :

Procédure

1. Connectez-vous à Integrated Solutions Console et cliquez sur **Tivoli Federated Identity Manager → Configurer la connexion unique fédérée → Fédérations**. Les portlets IBM Domaines en cours et Fédérations apparaissent. Le portlet Fédérations affiche plusieurs boutons d'action.
2. Cliquez sur **Créer**. L'assistant de fédération démarre. Le panneau Informations générales s'affiche.
3. Indiquez le nom de la fédération et sélectionnez un rôle. Cliquez sur **Suivant**.
4. Entrez les informations sur la personne à contacter et cliquez sur **Suivant**.
5. Sélectionnez le protocole "WS-Federation Passive Protocol" et cliquez sur **Suivant**. L'écran Serveur point de contact s'affiche.
6. Entrez les informations sur l'adresse du point de contact et cliquez sur **Suivant**.
7. Choisissez-en un :
   - Si vous voulez configurer un fournisseur de services, l'étape suivante est le mappage d'identité. Passez à l'étape 8, à la page 382.
   - Lorsque vous configurez un fournisseur d'identité, le panneau Configuration du jeton de sécurité s'affiche. Spécifiez les propriétés de jeton requises, puis cliquez sur **Suivant**.

Voir Chapitre 26, «Configuration d'une fédération de connexion unique WS-Federation», à la page 373.

8. Le panneau Options de mappage d'identité s'affiche. Sélectionnez l'un des boutons d'option suivants.
   - Utiliser la transformation XSL pour le mappage d'identité

     Indique que vous comptez fournir un fichier XSL contenant le mappage d'identité requis.

     a. Lorsque vous sélectionnez cette option et cliquez sur **Suivant**, le panneau Mappage d'identité s'affiche. Dans la zone **Fichier XSLT contenant une règle de mappage d'identité**, entrez le nom d'un fichier du système de fichiers local qui contient la règle de mappage d'identité.

        Il s'agit du fichier que vous avez préparé avant de procéder à cette installation.

        Vous pouvez également localiser le fichier sur le système de fichiers local à l'aide du bouton **Parcourir**.

     b. Cliquez sur **Suivant**.

        Une erreur s'affiche lorsque le fichier est introuvable ou ne contient aucune donnée XSLT (eXtensible Stylesheet Language Transform) valide.

   - Utiliser l'instance de module de mappage personnalisée

     Indique que vous comptez fournir une instance de module de mappage personnalisée, que vous utiliserez à la place du fichier XSL.

     a. Lorsque vous sélectionnez l'option Utiliser l'instance de module de mappage personnalisée, un tableau des instances de module s'affiche. Cliquez sur le bouton d'option correspondant à l'instance de module à utiliser et cliquez sur **Suivant**.

     b. Le cas échéant, vous serez alors invité à indiquer des valeurs pour les propriétés de l'instance de module de mappage personnalisée. Sinon, le panneau affiche un message indiquant qu'aucune propriété ne doit être configurée pour l'instance de module indiquée.
9. Le panneau Récapitulatif s'affiche. Vérifiez que les paramètres de configuration sont corrects, puis cliquez sur **Terminer**. Le portlet Création de fédération terminée s'affiche.
10. Cliquez sur **Redémarrer WebSphere**.

Que faire ensuite

Si vous utilisez WebSEAL en tant que serveur point de contact, procédez maintenant à sa configuration. Ne quittez pas la console de gestion. Voir aussi :

- «Configuration de WebSEAL en tant que serveur point de contact»

Configuration de WebSEAL en tant que serveur point de contact

Si vous envisagez d'utiliser WebSEAL en tant que serveur point de contact, vous devez le configurer pour la fédération de connexion unique WS-Federation.

Avant de commencer

L'assistant de fédération comporte un bouton qui vous permet d'obtenir un utilitaire de configuration.

Pourquoi et quand exécuter cette tâche

Vous devez obtenir l'utilitaire, puis l'exécuter. Procédez comme suit :

Procédure

1. Sur la console de gestion, cliquez sur **Télécharger l'outil de configuration Tivoli Access Manager**.
2. Enregistrez l'outil de configuration sur le système de fichiers de l'ordinateur hébergeant le serveur WebSEAL.
3. Revenez à la console de gestion et cliquez sur **Terminé** pour revenir au panneau Fédérations.

   Remarque : La console de gestion vous offre la possibilité d'ajouter immédiatement un partenaire, mais pour cette configuration initiale de la fédération, nous commencerons par exécuter d'abord les autres tâches.
4. Démarrez l'outil de configuration depuis une ligne de commande. La syntaxe est la suivante :

   ```
   java -jar /rép_téléchargement/tfimcfg.jar -cfgfile webseald-nom_instance.conf
    -action tamconfig
   ```

   Vous aurez besoin de l'ID (par défaut : sec_master) et du mot de passe de l'utilisateur d'administration Tivoli Access Manager. L'utilitaire configure les noeuds finals sur le serveur WebSEAL, crée une jonction WebSEAL, relie les listes de contrôle d'accès adaptées et active les méthodes d'authentification adéquates.

Exemple

Par exemple, lorsque vous avez mis le fichier tfimcfg.jar dans le répertoire `/tmp` et que le nom de l'instance WebSEAL est `default`, la commande est la suivante :

```
java -jar /tmp/tfimcfg.jar -cfgfile webseald-default -action tamconfig
```

Pour plus d'informations, accédez à l'adresse suivante :

- Annexe A, «Référence de tfimcfg», à la page 533

Que faire ensuite

La prochaine tâche consiste à exporter les propriétés de votre fédération WS-Federation dans un fichier. Voir «Exportation des propriétés WS-Federation», à la page 384.

Configuration de WebSphere en tant que serveur point de contact

Tivoli Federated Identity Manager est configuré par défaut pour utiliser Tivoli Access Manager WebSEAL en tant que serveur point de contact. Pour configurer WebSphere en tant que serveur point de contact, vous devez procéder à une modification de la configuration.

Procédure

1. Connectez-vous à la console d'administration.
2. Cliquez sur Tivoli Federated Identity Manager > Gestion de la configuration > Point de contact
3. Sélectionnez **WebSphere**
4. Cliquez sur **Activer**.

Résultats

Le serveur WebSphere est désormais configuré en tant que point de contact.

Exportation des propriétés WS-Federation

Pourquoi et quand exécuter cette tâche

Pour rejoindre une fédération hébergée par un autre partenaire commercial, vous devez fournir vos propriétés de configuration de fédération. Dans le cas des fédérations WS-Federation, vous devez préparer manuellement un fichier contenant les propriétés de configuration. Transmettez ce fichier à votre partenaire de fédération.

Procédure

1. Connectez-vous à la console de gestion. Cliquez sur **Tivoli Federated Identity Manager → Configurer la connexion unique fédérée → Fédérations**.
2. Le panneau Fédérations s'affiche. Sélectionnez votre fédération à connexion unique WS-Federation dans le tableau.
3. Afficher les propriétés de la fédération. Obtenez les propriétés indiquées dans la liste de la rubrique «Propriétés WS-Federation à échanger avec votre partenaire», à la page 385
4. Délivrez le fichier à votre partenaire suivant la méthode convenue dans l'accord conclu entre votre société et celle de votre partenaire.

Que faire ensuite

Si votre partenaire souhaite ajouter vos informations de configuration à sa fédération de connexion unique WS-Federation, vous devez lui fournir ce fichier.

Obtention des informations de configuration auprès d'un partenaire WS-Federation

Vous devez obtenir ces informations auprès de votre partenaire WS-Federation.

Avant de commencer

Si vous souhaitez ajouter votre partenaire commercial en tant que partenaire de votre fédération de connexion unique WS-Federation, vous devez obtenir auprès de celui-ci les informations de configuration nécessaires relatives à sa fédération WS-Federation.

Une fédération WS-Federation doit avoir été déjà installée et configurée par votre partenaire. La fédération de votre partenaire joue le rôle opposé à celui de votre fédération. Si, par exemple, votre fédération est configurée en tant que fournisseur d'identité, la fédération de votre partenaire l'est en tant que fournisseur de services.

Vous pouvez obtenir ces informations en faisant en sorte que votre partenaire assemble manuellement les propriétés de configuration de sa fédération. Le partenaire doit ensuite vous fournir les informations en employant la méthode convenue dans le cadre de l'accord conclu avec votre partenaire.

Pourquoi et quand exécuter cette tâche

Exécutez les étapes suivantes :

Procédure

1. Votre partenaire doit collecter les propriétés de sa fédération via la console de gestion. Il convient que le partenaire vous fournisse les propriétés indiquées à la rubrique «Propriétés WS-Federation à échanger avec votre partenaire».
2. Il convient que votre partenaire pour délivre le fichier suivant la méthode convenue dans l'accord conclu entre votre société et celle de votre partenaire.

Propriétés WS-Federation à échanger avec votre partenaire

Propriétés de la fédération

Tableau 110. Propriétés WS-Federation

Propriété	Description
Nom de la fédération	Chaîne de caractères désignant la fédération
Rôle	Fournisseur d'identité ou fournisseur de services
Protocole	profil passif WS-Federation
Personne à contacter	
Nom de la société	Nom de la société qui a créé la fédération. Paramètre obligatoire.
Adresse URL de la société	Adresse URL de la société qui a créé la fédération. Facultatif.
Prénom et nom	Nom de la personne au sein de la fédération pouvant être contactée par d'autres sociétés. Facultatif.
Adresse électronique	Adresse électronique de la personne au sein de la fédération pouvant être contactée par d'autres sociétés. Facultatif.
Numéro de téléphone	Numéro de téléphone de la personne au sein de la fédération pouvant être contactée par d'autres sociétés. Facultatif.
Type de contact	chaîne décrivant le type de rôle dans l'entreprise, par exemple Conseiller technique ou Personnel d'assistance. Facultatif

Données relatives à la WS-Federation

Tableau 111. Données relatives à la WS-Federation

Propriété	Description
Domaine WS-Federation	Nom unique du domaine WS-Federation. Par exemple : `https://idp.exemple.com/FIM/sps/wsfed/wsf`

Tableau 111. Données relatives à la WS-Federation (suite)

Propriété	Description
noeud final WS-Federation	Noeud final du partenaire pour toutes les demandes de services WS-Federation. Par exemple : `https://idp.exemple.com/FIM/sps/wsfed/wsf`
Durée maximale d'une requête (en secondes)	Durée maximale de validité, en secondes, d'une demande ou d'un message envoyé par un partenaire WS-Federation.

Configuration du module de jeton SAML

Tableau 112. Propriétés du module de jeton SAML

En-tête	En-tête
Activer la signature des assertions	Indique si le fournisseur d'identité doit signer des assertions avant de les envoyer au fournisseur de services partenaire.
Sélectionner la clé de signature des assertions	Indiquez le nom de la clé à utiliser lors de la signature d'assertions. Cette option est spécifiée pour les partenaires des fournisseurs de services.
Entrez les types d'attributs suivants (si une étoile '*' est indiquée, tous les types sont inclus)	Types d'attributs à inclure dans le module de jeton SAML. Cette option est spécifiée pour les partenaires des fournisseurs de services.
Activer la validation des signatures	Lorsqu'elle est sélectionnée, cette option indique que le fournisseur de services validera la signature sur les assertions provenant du fournisseur d'identité partenaire. Option spécifiée pour les partenaires des fournisseurs d'identité.
Sélectionner la clé de validation	Indiquez le nom de la clé à utiliser pour la validation des signatures. Cette option est spécifiée pour les partenaires des fournisseurs d'identité.

Ajout d'un partenaire dans une fédération de connexion unique WS-Federation

Vous pouvez utiliser la console d'administration pour ajouter un partenaire dans une fédération de connexion unique WS-Federation.

Pourquoi et quand exécuter cette tâche

La procédure de configuration d'ajout est identique lors de l'ajout de tous les partenaires. Les propriétés de configuration sont différentes pour des partenaires de fournisseur d'identité et de services. L'assistant de partenaire vous demande les propriétés nécessaires.

Procédure

1. Connectez-vous à IBM Integrated Solutions Console. Cliquez sur **Tivoli Federated Identity Manager → Configurer la connexion unique fédérée → Partenaires**.

2. Le panneau Partenaires de la fédération s'affiche. Cliquez sur **Créer**. Le panneau Sélection de fédération s'affiche.
3. Sélectionnez la fédération à laquelle vous souhaitez ajouter un partenaire. Cliquez sur **Suivant**. L'écran Personnes à contacter s'affiche.
4. Spécifiez les propriétés requises, puis cliquez sur **Suivant**.

   Le nom de l'entreprise est obligatoire. Les autres zones sont facultatives. Pour plus d'informations, voir . Le panneau Données WS-Federation s'affiche.
5. Spécifiez les propriétés requises, puis cliquez sur **Suivant**.
6. Le panneau Configuration du jeton de sécurité s'affiche. Entrez les propriétés de configuration du jeton de sécurité fédéré.

   Les propriétés de configuration sont propres au rôle du partenaire :
   - Lors de l'ajout d'un fournisseur d'identité partenaire :
     a. Si les assertions doivent être signées, cliquez sur **Activer la signature des vérifications**. Si vous cochez cette case, vous devez indiquer une clé à utiliser pour la signature des assertions. Sélectionnez l'option **Fichier de clés**, tapez la valeur de la zone **Mot de passe du fichier de clés**, cliquez sur **Liste des clés** et sélectionnez une clé dans le tableau.
     b. Vous pouvez aussi indiquer des attributs dans la zone : **Entrez les types d'attributs suivants (si une étoile "*" est indiquée, tous les types sont inclus).**
     c. Cliquez sur **Suivant**.
   - Lors de l'ajout d'un fournisseur de services partenaire :
     a. Si les signatures doivent être validées, cliquez sur **Activer la validation des signatures**. Si vous cochez cette case, vous devez indiquer une clé à utiliser pour la validation des signatures. Sélectionnez l'option **Fichier de clés**, tapez la valeur de la zone **Mot de passe du fichier de clés**, cliquez sur **Liste des clés** et sélectionnez une clé dans le tableau.
     b. Cliquez sur **Suivant**.
7. Le panneau Options de mappage d'identité s'affiche. Sélectionnez l'un des boutons d'option suivants.
   - Utiliser la transformation XSL pour le mappage d'identité

     Indique que vous comptez fournir un fichier XSL contenant tous les mappages d'identité requis.
     a. Lorsque vous sélectionnez cette option et cliquez sur **Suivant**, le panneau Mappage d'identité s'affiche. Ne remplissez pas cette zone si vous souhaitez utiliser la règle de mappage d'identité par défaut que vous avez entrée dans l'assistant de création de fédération. Si vous voulez remplacer la règle de mappage par défaut par une règle spécifique au partenaire, entrez le nom d'un fichier du système de fichiers local contenant la règle de mappage d'identité concernée dans la zone **Fichier XSLT contenant une règle de mappage d'identité**.

        Pour plus d'informations sur les fichiers de règles de mappage, voir .

        Vous pouvez également localiser le fichier sur le système de fichiers local à l'aide du bouton **Parcourir**.
     b. Cliquez sur **Suivant**.
   - Utiliser l'instance de module de mappage personnalisée

     Indique que vous comptez fournir une instance de module de mappage personnalisée, que vous utiliserez à la place du fichier XSL.

a. Lorsque vous sélectionnez l'option Utiliser l'instance de module de mappage personnalisée, un tableau des instances de module s'affiche. Cliquez sur le bouton d'option correspondant à l'instance de module à utiliser et cliquez sur **Suivant**.

b. Le cas échéant, vous serez alors invité à indiquer des valeurs pour les propriétés de l'instance de module de mappage personnalisée. Sinon, le panneau affiche un message indiquant qu'aucune propriété ne doit être configurée pour l'instance de module indiquée.

Le panneau Récapitulatif s'affiche.

8. Vérifiez que les paramètres sont corrects, puis cliquez sur **Terminer**. L'écran Ajout de partenaire terminé s'affiche.
9. Cliquez sur **Activer le partenaire** pour activer ce partenaire.

   Le partenaire a été ajouté à la fédération, mais il est désactivé par défaut par mesure de sécurité. Vous devez activer le partenaire.

Partie 3. Configuration de la gestion de sécurité des services Web

Les rubriques de la section Configuration vous guident pas à pas lorsque vous configurez la gestion de sécurité des services Web pour Tivoli Federated Identity Manager.

Veuillez consulter d'abord la section suivante :

Chapitre 28, «Configuration de la gestion de sécurité des services Web», à la page 391

Chapitre 28. Configuration de la gestion de sécurité des services Web

La configuration de la gestion de sécurité des services Web commence par l'établissement d'un domaine Tivoli Federated Identity Manager. Lorsque le domaine est établir, vous pouvez configurer le composant de gestion de la sécurité des services Web.

La procédure de configuration de la gestion de sécurité des services Web est la suivante :

1. Configuration d'un domaine Tivoli Federated Identity Manager.

   Le déploiement d'un scénario Tivoli Federated Identity Manager nécessite la création d'un domaine Tivoli Federated Identity Manager.

   vous devez créer et configurer un domaine avant de pouvoir configurer le composant gestion de la sécurité des services Web.

   Voir Chapitre 1, «Configuration de domaine», à la page 3.
2. Configuration du composant gestion de la sécurité des services Web.

   La configuration du composant peut s'effectuer de différentes manières afin de refléter les scénarios de déploiement. Pour une description détaillée de la configuration, voir : *IBM Tivoli Federated Identity Manager - Guide de gestion de la sécurité des services Web*.

Partie 4. Configuration du service STS (Security Token Service)

Les rubriques de la section Configuration vous guident pas à pas lors de la configuration d'un service de jeton de sécurité (STS) dans le cadre d'une solution intégrée de gestion des identités d'utilisateur dans un environnement réseau réparti.

La présente section décrit le déploiement d'un module de service STS sur une délégation Kerberos pour les besoins de prise en charge d'une solution de jonctions Kerberos fournie par l'association entre Tivoli Federated Identity Manager et Tivoli Access Manager for e-Business WebSEAL, ainsi que des produits WebSphere et autres composants additionnels.

Veuillez d'abord consulter la présentation du scénario de déploiement :

Chapitre 29, «Présentation de la délégation contrainte Kerberos», à la page 395

Chapitre 29. Présentation de la délégation contrainte Kerberos

Tivoli Federated Identity Manager fournit un service de jeton de sécurité, ou STS (Security Token Service) qui permet d'échanger les formats des jetons de sécurité. Cette fonction sert à déplacer les données d'identification de l'utilisateur entre différents formats de jeton, suivant les besoins des différentes applications.

Le service STS fait partie intégrante des solutions de connexion unique de Tivoli Federated Identity Manager, mais est également utilisable de manière autonome. Cette autonomie d'utilisation permet d'intégrer Tivoli Federated Identity Manager dans une grande diversité de déploiements réseau hétérogènes.

L'un de ces types de déploiement est un environnement qui exploite l'authentification intégrée SPNEGO deMicrosoft Windows (SPNEGO) en association avec des tickets Kerberos. Dans cet environnement, Tivoli Federated Identity Manager peut être déployé de manière à accepter les données d'identification de l'utilisateur et à les convertir suivant le format Kerberos nécessaire.

Pour permettre cette capacité, Tivoli Federated Identity Manager inclut un module de services de jeton de sécurité destiné spécifiquement à la délégation contrainte Kerberos. Le module de la délégation Kerberos facilite l'émission des tickets du service d'application pour la délégation contrainte Kerberos, également appelé S4U2Proxy ("Service for User To Proxy").

Le module prend uniquement en charge l'*émission* des jetons et *excusivement* les tickets du service d'application Kerberos de Windows via le modèle de délégation à contrainte.

L'une des caractéristiques principales du modèle de délégation contrainte Kerberos est que le mot de passe de l'utilisateur final pour lequel le ticket de service Kerberos doit être obtenu n'a pas besoin d'être connu par l'application qui génère le ticket. Dans ce cas, l'application est WebSphere plus Tivoli Federated Identity Manager. L'application a uniquement besoin de connaître le nom de l'utilisateur final, ainsi que le nom principal (SPN) du service Kerberos cible.

Le module STS de la délégation contrainte Kerberos vise principalement à permettre à Tivoli Access Manager WebSEAL de prendre en charge la connexion unique sur les jonctions Kerberos. Il s'agit de jonctions avec un serveur Web configuré pour l'authentification intégrée SPNEGO sous Windows. WebSEAL permet de maintenir une session utilisateur au moyen de n'importe quel mécanisme d'authentification sélectionné par ses soins, puis de se connecter à un serveur Web (par exemple le serveur IIS) sur la base du flux d'authentification SPNEGO. Ce flux d'authentification exploite un ticket Kerberos.

L'utilisation de droits d'accès Kerberos pour la connexion unique sur des jonctions offre les capacités suivantes :

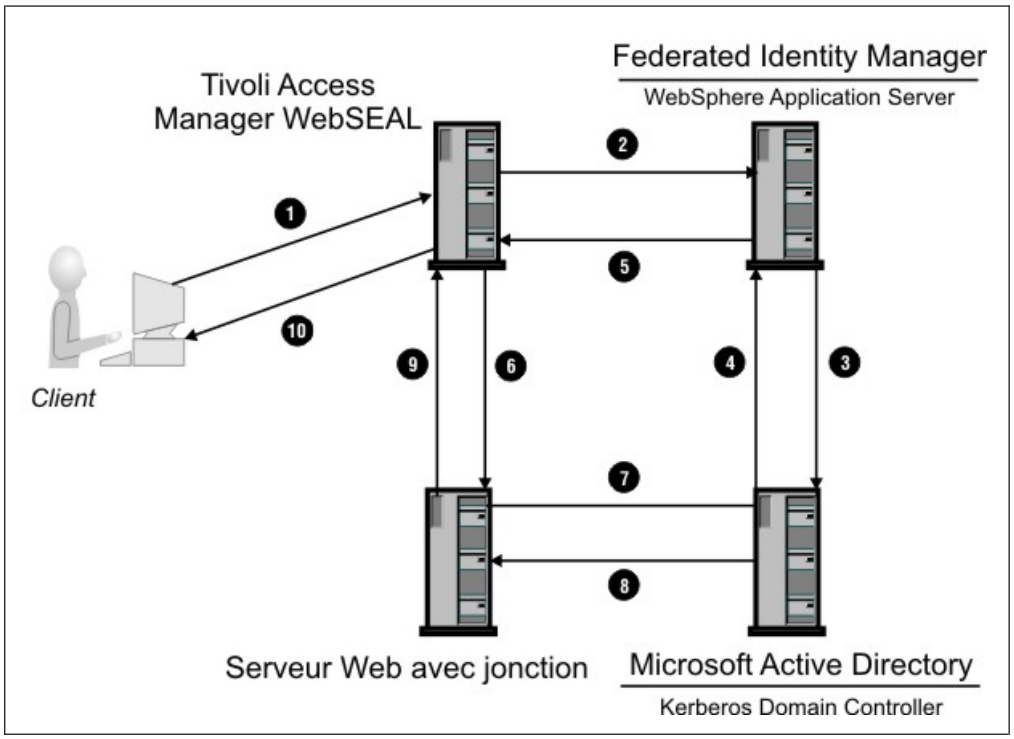
- Les droits d'accès Kerberos sont aisément utilisables par les applications Web ASP.NET sans nécessiter de déploiement de code supplémentaire.
- Les droits d'accès Kerberos peuvent être transmis d'une application à l'autre tout en maintenant une signature cryptographique, ce qui permet de renforcer la sécurité.

Remarque : ce module diffère du module STS Kerberos Java natif de Tivoli Federated Identity Manager. Le module Kerberos Java prend en charge l'émission et la validation générique des autres tickets Kerberos.

Vous trouverez plus d'informations sur les extensions Kerberos de Windows à l'emplacement suivant :

- http://technet2.microsoft.com/WindowsServer/en/Library/c312ba01-318f-46ca-990e-a597f3c294eb1033.mspx
- http://msdn2.microsoft.com/en-us/library/aa480585.aspx
- http://msdn.microsoft.com/msdnmag/issues/03/04/SecurityBriefs/

Présentation de la délégation contrainte Kerberos avec des jonctions WebSeal



Tivoli Federated Identity Manager utilise le module STS de la délégation contrainte Kerberos pour générer les jetons Kerberos. WebSEAL extrait les jetons Kerberos en déléguant la demande de jeton au module STS.

Le diagramme ci-dessus illustre un exemple de déploiement des applications lors de la réalisation de ce type de connexion unique. Le diagramme illustre également la manière dont les messages circulent entre les différents composants physiques.

1. Le client s'appuie sur le processus d'authentification standard de Tivoli Access Manager pour s'authentifier sur WebSEAL via le protocole HTTPS ou HTTP, puis demander un objet sur le serveur comportant les jonctions. WebSEAL autorise la demande émise par le client, puis détermine qu'un ticket Kerberos est requis pour accéder à l'application de la jonction.
2. WebSEAL génère un message d'émission de clé WS-Trust destiné au serveur Tivoli Federated Identity Manager. Une clé d'émission WS-Trust unique peut

être utilisée pour demander des jetons Kerberos multiples. WebSEAL ouvre une connexion auprès du serveur WebSphere exécutant Tivoli Federated Identity Manager. WebSEAL adresse la requête SOAP au serveur WebSphere.

3. Le serveur Tivoli Federated Identity Manager exécuté sur l'instance du serveur WebSphere vérifie que le serveur WebSEAL est autorisé à invoquer le service STS (Security Token Service). Le service STS appelle ensuite un module d'accréditation Tivoli Federated Identity Manager afin de demander le nombre configuré de tickets Kerberos requis pour le serveur Web de la jonction au titre du client. Le module d'accréditation communique avec le contrôleur de domaine Active Directory en utilisant Kerberos sur le port TCP ou UDP 88.
4. Le contrôleur de domaine Active Directory vérifie que le serveur Tivoli Federated Identity Manager est autorisé à demander des tickets pour le serveur Web joint, au titre de l'utilisateur concerné. Le contrôleur de domaine Active Directory renvoie le nombre de tickets Kerberos configuré vers le composant d'exécution de Tivoli Federated Identity Manager.
5. Le composant d'exécution de Tivoli Federated Identity Manager renvoie les tickets sous forme de réponse SOAP adressée au serveur WebSEAL.
6. Le serveur WebSEAL met en cache les tickets Kerberos et transmet l'un d'entre eux avec la demande client adressée au serveur Web de la jonction, via le protocole HTTP ou HTTPS.
7. Ce serveur Web de jonction demande la validation du ticket Kerberos de la part du contrôleur de domaine Kerberos (KDC). Le contrôleur KDC est décrit ici comme étant le même système que le serveur Active Directory.
8. Le contrôleur KDC vérifie que le ticket Kerberos est valide. Le ticket Kerberos est utilisé comme preuve de l'identité du client et peut également servir à d'autres contrôles d'autorisation.
9. Le serveur Web de jonction renvoie une réponse HTTP à WebSEAL.
10. WebSEAL renvoie une réponse HTTP au client.

Lors de chaque réponse ultérieure émise par le même client, au cours de la même session de connexion et sur le même serveur Web de la jonction, un nouveau ticket Kerberos est envoyé au serveur Web de la jonction en même temps que la requête. Le nouveau ticket Kerberos est soit prélevé dans le cache WebSEAL de tickets Kerberos, soit une requête est envoyée au serveur WebSphere exécutant Tivoli Federated Identity Manager, afin d'obtenir une nouvelle série de tickets Kerberos.

Présentation du déploiement

Logiciels prérequis

- Tivoli Federated Identity Manager doit être exécuté sur Windows 2003 Server Service Pack 2 ou version supérieure.

  Le module de mise à jour est requis en raison d'un problème connu de fuite de mémoire affectant le processus Windows Isass.exe sur les versions antérieures. Voir http://support.microsoft.com/kb/907524/.
- Le serveur WebSEAL peut être exécuté sur n'importe quelle plateforme prise en charge.

  Le serveur WebSEAL *ne doit pas nécessairement* faire partie du domaine Active Directory.
- Le déploiement de WebSphere peut être effectué soit en mode autonome, soit sous forme de cluster. Il convient que tous les serveurs WebSphere membres du cluster soient installé sur des systèmes Windows et fassent partie du domaine.

- Lorsque les utilisateurs de Tivoli Access Manager sont stockés dans Active Directory, le serveur de règles Tivoli Access Manager doit être hébergé sous Windows et être membre du domaine.
- Il convient que tous les contrôleurs du domaine Active Directory soient exécutés au niveau fonctionnel de Windows Server 2003.
- La prise en charge de Tivoli Federated Identity Manager support pour les modules de délégation Kerberos n'est pas incluse dans le produit Tivoli Federated Identity Manager Business Gateway.

Présentation des tâches de déploiement

1. Activez l'authentification Windows intégrée
2. Configurez Active Directory et WebSphere pour la délégation contrainte
3. Installez et configurez un domaine et un composant d'exécution Tivoli Federated Identity Manager
4. Configurez une instance de module Kerberos et une chaîne d'accréditation pour le module STS de la délégation contrainte Kerberos
5. Configurez WebSEAL pour la prise en charge d'une jonction Kerberos

Tableau 113. Exemples de noms d'hôte de serveur utilisés dans cette documentation

Rôle du serveur	**Exemple de valeur**
Serveur dorsal (serveur Web à jonctions)	mydataserver.example.com
Serveur WebSEAL	websealhost.example.com
Nom d'hôte Active Directory	activedirectoryhost.example.com

Chapitre 30. Activation de l'authentification Windows intégrée

Ces instructions expliquent comment configurer Microsoft IIS en vue de l'authentification SPNEGO.

Avant de commencer

Ces instructions supposent que vous avez déployé Windows Server 2003 avec Active Directory. Ces étapes doivent être terminées avant la configuration de la délégation contrainte.

Procédure

1. Sur le contrôleur de domaine, sélectionnez **Démarrer -> Programmes > Outils d'administration -> Utilisateurs et ordinateurs Active Directory**
2. Créez un utilisateur agissant en tant que proxy pour le serveur IIS. Par exemple, `iisuser`. Indiquez que le mot de passe de l'utilisateur `n'expire jamais`.
3. Ouvrez une invite de commande.
   a. Accédez au répertoire `C:\Program Files\Support Tools`.
   b. Exécutez la commande **ktpass** appropriée.

      Syntaxe de la commande ktpass :

      ```
      ktpass -princ HTTP/nom_serveur_IIS.nom_domaine@DOMAIN_NAME
        -mapuser nom_utilisateur_IIS -mapOp set
      ```

      où :

      - `-princ` est le nom principal, indiqué sous la forme *user@REALM*
      - `-mapuser` correspond à la valeur -princ pour ce compte d'utilisateur. Cette option est définie par défaut.
      - `-mapOp` spécifie le mode de définition de l'attribut de mappage : `set` *set_value*
4. Affichez les propriétés du compte pour `iisuser`. Vérifiez que la zone **Nom de connexion de l'utilisateur** est définie sur la valeur suivante :

   `HTTP/`*nom_serveur_IIS.nom_domaine*

   Par exemple :

   `HTTP/mydataserver.example.com`
5. Configuration de l'identité du pool d'applications
   a. Sur le système du serveur IIS, sélectionnez **Démarrer -> Programmes > Outils d'administration -> Gestionnaire IIS (Internet Information Service)**.
   b. Sélectionnez *nom_de_votre_serveur/Nom IIS* **-> Programmes > Pools d'applications -> Pool d'applications par défaut**
   c. Cliquez avec le bouton droit et sélectionnez **Propriétés**. Sélectionnez l'onglet d'identité et spécifiez l'identité de domaine de l'utilisateur IIS (exemple : `iisuser`).

   Pour obtenir des instructions détaillées sur la tâche Windows de *configuration de l'identité du pool de connexions avec IIS 6.0*, voir :

   http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/f05a7c2b-36b0-4b6e-ac7c-662700081f25.mspx?mfr=true
6. Ouvrez l'Explorateur Windows.

a. Accédez au répertoire `C:\WINNT\Microsoft.NET\Framework\v1.1.4322\Temporary ASP.NET Files`
b. Sélectionnez **Propriétés**.
c. Sélectionnez l'onglet **Sécurité**.
d. Attribuez à l'utilisateur du domaine `iisuser` le contrôle d'accès complet au répertoire

7. Accédez au système IIS et sélectionnez **Démarrer -> Programmes > Outils d'administration -> Gestion de l'ordinateur**.
   a. Ouvrez la section **Utilisateurs et groupes locaux**
   b. Ouvrez l'option **Groupes**
   c. Cliquez avec le bouton droit sur le groupe local `IIS_WPG`.
   d. Sélectionnez les propriétés.
   e. Sélectionnez Ajouter.
   f. Ajoutez l'utilisateur du domaine (soit dans le cas présent, `iisuser`) à ce groupe local.
8. Sur le système IIS, ouvrez les règles de sécurité locales du serveur. cliquez sur **Démarrer -> Exécuter** et entrez `secpol.msc`
   a. Développez les règles locales et accédez à la section Attribution des droits utilisateur.
   b. Ouvrez la stratégie intitulée **Ouverture de session en tant que service**.

      Il est à noter que n'importe quel compte ou groupe figurant dans cette liste peut ouvrir une session en tant que service.
   c. Cliquez sur **Ajouter un utilisateur ou un groupe**.
   d. Entrez (ou recherchez) le compte du nom de domaine `iisuser`.
   e. Une fois les droits accordés, réamorcez le serveur.

      Le réamorçage du système est nécessaire, car les paramètres de sécurité sont appliqués durant la phase de démarrage de toute machine Windows 2003 Server.
9. Sur le système IIS, sélectionnez **Démarrer -> Programmes > Outils d'administration -> Gestionnaire IIS (Internet Information Service)**.
   a. Ouvrez l'ordinateur local.
   b. Cliquez avec le bouton droit sur DefaultAppPool.
   c. Sélectionnez **Recycler** pour redémarrer le pool.
10. Ouvrez un navigateur et accédez à `http://`*`serveur_web`*.

    S'il s'agit d'un nouveau serveur IIS dépourvu de contenu, la page `Under Construction` du serveur doit normalement s'afficher. Lorsqu'un contenu est présent sur le serveur IIS, il convient que celui-ci soit visible.
11. Sur le système IIS, sélectionnez **Démarrer -> Programmes > Outils d'administration -> Gestionnaire IIS (Internet Information Service)**.
    a. Cliquez avec le bouton droit sur le site Web par défaut.
    b. Sélectionnez Propriétés, puis l'onglet Sécurité de répertoire.
    c. cliquez sur le bouton **Modifier** en regard de l'entrée `Permettre l'accès anonyme` et modifiez les messages d'authentification liés à cette ressource.
    d. Désactivez l'accès anonyme.
    e. Activez l'authentification Windows intégrée
    f. Cliquez sur **OK**, puis de nouveau sur **OK**.
12. Ouvrez votre navigateur et accédez à http://*serveur_web*. Vous êtes invité à ouvrir une session.

13. Entrez un utilisateur de domaine valide. Exemple : user@mydomain.com. Lorsque la connexion aboutit, vous pouvez visualiser le contenu IIS.

Chapitre 31. Configuration d'Active Directory et WebSphere pour la délégation contrainte

Pourquoi et quand exécuter cette tâche

L'agent de noeud WebSphere qui héberge le composant d'exécution de Tivoli Federated Identity Manager doit être exécuté via un compte spécial d'Active Directory pour bénéficier de la permission d'obtenir des tickets Kerberos destinés à d'autres utilisateurs, ainsi qu'une série de cibles restreintes. Vous devez créer ce compte, définir les options appropriées et modifier le service WebSphere en vue d'utiliser ce compte, avant que votre chaîne d'accréditation de délégation Kerberos puisse fonctionner. Les instructions suivantes décrivent la manière dont vous devez accomplir ces tâches.

Procédure

1. Vérifiez que le serveur DNS est correctement configuré sur le contrôleur de domaine Active Directory.

   Le serveur DNS doit être configuré à la fois en vue de permettre les recherches incursives et récursives. Chaque hôte du domaine Active Directory doit être configuré en vue d'utiliser l e serveur DNS du contrôleur de domaine.

   Pour vérifier ceci, exécutez les commandes **nslookup** à la fois sur le nom d'hôte et l'adresse IP de l'ordinateur membre du domaine. Il convient que le résultat des commandes **nslookup** indiquent que la partie correspondant au domaine dans le nom résolu est celui du contrôleur de domaine.
2. Assurez-vous que les services de synchronisation des horloges sont actifs sur toutes les machines situées dans le domaine Active Directory et que les horloges de toutes ces machines sont synchronisées.
3. Vérifiez que le système Windows Server 2003 (ou les systèmes multiples, en cas de déploiement dans un cluster WebSphere) est configuré dans le domaine Active Directory. Le serveur peut, en option, être configuré en tant que contrôleur de domaine.
4. Vérifiez que tous les contrôleurs du domaine soient exécutés au niveau fonctionnel de Windows Server 2003. Pour ce faire, procédez comme suit :
   a. Ouvrez le panneau de configuration des utilisateurs et ordinateurs d'Active Directory.
   b. Cliquez sur le nom du domaine avec le bouton droit et sélectionnez **Augmenter le niveau fonctionnel du domaine**.
   c. Sélectionnez `Windows Server 2003` et cliquez sur **OK**

   La fenêtre Augmenter le niveau fonctionnel du domaine s'affiche. Elle contient normalement les messages suivants :

   ```
   Niveau fonctionnel du domaine actuel
   Windows Server 2003

   Ce domaine fonctionne au niveau fonctionnel le plus élevé possible.
   ```
5. Sur le contrôleur de domaine, créez un utilisateur pour la délégation dans Active Directory. Le serveur WebSphere qui héberge le composant d'exécution de Tivoli Federated Identity Manager s'exécute en tant qu'identité pour cet utilisateur.

a. Créez un utilisateur. Par exemple, `tfimdeleguser` Vous pouvez indiquer une autre identité d'utilisateur. Ce nom d'utilisateur sera utilisé dans les présentes instructions.

b. Cochez la case **Le mot de passe n'expire jamais**.

Remarque : Vous pouvez, en option, définir l'expiration du mot de passe. Si tel est le cas, lorsque vous le modifierez le moment venu, vous devrez également réinitialiser le mot de passe de l'agent de noeud WebSphere dans le service Windows.

6. Sur le contrôleur de domaine, ajoutez l'utilisateur `tfimdeleguser` au groupe d'administrateurs du domaine. Pour vérifier ceci :
   a. Sélectionnez **Utilisateurs et ordinateur Active Directory**
   b. Pour le domaine, cliquez sur Utilisateurs, puis sur Administrateurs de domaine.
   c. Cliquez sur l'onglet Membres. Vérifiez que l'utilisateur tfimdeleguser figure parmi la liste des membres du groupe.
7. Assurez-vous que les outils Microsoft Support Tools sont installés sur le contrôleur de domaine. A titre d'exemple, pour obtenir les outils de support 32 bits pour Windows Server 2003 Service Pack 1 :

   http://www.microsoft.com/downloads/details.aspx?FamilyId=6EC50B78-8BE1-4E81-B3BE-4E7AC4F0912D&displaylang=en
8. Sur le contrôleur de domaine, créer un nom principal de service (SPN) pour l'utilisateur `tfimdeleguser`. Pour ce faire, procédez comme suit :
   a. Ouvrez une invite de commande sur le contrôleur de domaine sur lequel les outils de support sont installés.
   b. Exécutez la commande **setspn**

      La syntaxe de la commande est la suivante :

      `setspn -A tfim/<utilisateur_délégation_tfim> <utilisateur_délégation_tfim>`

      Par exemple :

      ```
      setspn -A tfim/tfimdeleguser tfimdeleguser
      ```
9. Sur le contrôleur de domaine, ouvrez **Utilisateurs et ordinateurs Active Directory** et accédez aux propriétés de l'utilisateur `tfimdeleguser`.
   a. Cliquez sur l'onglet Délégation.

      Remarque : Si l'onglet Délégation n'apparaît pas, revenez à l'étape précédente et assurez-vous que la commande 'setspn' a abouti.
   b. Sélectionnez l'option **N'approuver cet utilisateur que pour la délégation aux services spécifiés**.
   c. Sélectionnez le bouton d'option **Utiliser n'importe quel protocole d'authentification**.
   d. Cliquez sur le bouton **Ajouter** dans l'onglet Délégation. Ajoutez ensuite les services cibles pouvant être délégués à tfimdeleguser. Il s'agit des services cible de la délégation contrainte. Dans cet exemple, il s'agit de l'utilisateur sous le nom duquel le serveur Web IIS est exécuté.
   e. Cliquez sur le bouton **Utilisateurs ou ordinateurs** pour rechercher des services particuliers.
   f. Sélectionnez l'utilisateur du domaine (service) sous lequel le serveur IIS est exécuté pour la jonction Kerberos WebSEAL.

Lorsque vous avez terminé, il convient que l'onglet Délégation indique un service cible dans la fenêtre **Services auxquels ce compte peut présenter des données d'identification déléguées**.

La fenêtre peut, par exemple, indiquer un **Type de service** `HTTP`, tandis que la section **Utilisateur ou ordinateur** indique un nom d'hôte ou de domaine, tel que `mydataserver.example.com`

Sélectionnez l'entrée `HTTP/mydataserver.example.com`. Appuyez sur **OK** pour continuer.

10. Ajoutez tfimdeleguser aux groupes d'accès d'autorisation Windows. Pour ce faire, procédez comme suit :
    a. Ouvrez le panneau **Utilisateurs et ordinateurs Active Directory**.
    b. Sélectionnez l'objet **Builtin** sous le domaine.
    c. Recherchez l'objet **Groupes d'accès d'autorisation Windows**.
    d. Cliquez avec le bouton droit et sélectionnez **Propriétés**. Sélectionnez l'onglet **Membres**.
    e. Cliquez sur **Ajouter** et ajoutez l'utilisateur de la délégation (dans notre exemple, il s'agit de `tfimdeleguser`) en tant que membre.
11. Octroyez à l'utilisateur de la délégation (tfimdeleguser) les privilèges **Agir en tant que partie du système d'exploitation**.

    Le processus effectif qui doit être exécuté en tant que service Windows dépend de l'environnement WebSphere :

    - Le nom du service défini dans un environnement *autonome* correspond à l'instance WebSphere Application Server qui héberge le composant d'exécution de Tivoli Federated Identity Manager
    - Le nom du service défini dans un environnement *groupé* est le serveur WebSphere Application qui exécute l'agent de noeud WebSphere pour le composant d'exécution de Tivoli Federated Identity Manager.

    Remarque : Dans un environnement groupé, cette étape doit être répétée sur toutes les machines hébergeant un membre de noeud du cluster WebSphere qui exécute le composant d'exécution Tivoli Federated Identity Manager. Pour ce faire, procédez comme suit :

    a. Accédez au menu approprié suivant votre déploiement :
       - Sur le contrôleur de domaine, sélectionnez **Démarrer -> Programmes > Outils d'administration -> Stratégie de sécurité du domaine**.
       - Sur une machine autre que le contrôleur de domaine, sélectionnez **Démarrer -> Programmes > Outils d'administration -> Stratégie de sécurité locale**.
    b. Développez l'option Stratégies locales.
    c. Sélectionnez **Attribution des droits utilisateur -> Agir en tant que partie du système s'exploitation**.
    d. Cliquez avec le bouton droit et sélectionnez **Propriétés**.
    e. Cochez la case **Définir les paramètres de cette stratégie**.
    f. Cliquez sur **Ajouter un utilisateur ou un groupe** afin d'ajouter l'utilisateur de la délégation (tfimdeleguser) à la liste des utilisateurs autorisés à agir en tant que partie du système d'exploitation.
    g. Cliquez sur **OK**.

12. Octroyez à l'utilisateur de la délégation (tfimdeleguser) les privilèges nécessaires :
    - Lorsque l'application Tivoli Federated Identity Manager est exécutée sur un membre du domaine, octroyez à l'utilisateur les privilèges **Ouvrir une session en tant que service** sur la machine locale.
    - Lorsque l'application Tivoli Federated Identity Manager est exécutée sur le contrôleur de domaine, octroyez à l'utilisateur les privilèges **Ouvrir une session en tant que service** sur ce contrôleur de domaine.

    a. Revenez au menu des stratégies de sécurité ouvert à l'étape précédente.
    b. Sélectionnez **Attribution des droits utilisateur > Ouvrir une session en tant que service**.
    c. Cliquez avec le bouton droit et sélectionnez **Propriétés**.
    d. Cochez la case **Définir les paramètres de cette stratégie**.
    e. Cliquez sur **Ajouter un utilisateur ou un groupe** afin d'ajouter l'utilisateur de la délégation (tfimdeleguser) à la liste des utilisateurs autorisés à agir en tant que partie du système d'exploitation.
    f. Cliquez sur **OK**.
13. Permettez au processus WebSphere qui exécute l'application Tivoli Federated Identity Manager de s'exécuter en tant que service Windows.

    Exécutez la commande **wasservice**. Emplacement par défaut :

    ```
    C:\Program Files\IBM\WebSphere\AppServer\bin
    ```

    Exemple de commande :

    ```
    C:\Program Files\IBM\WebSphere\AppServer\bin>wasservice -add ndagentwinser
    -servername nodeagent
    -profilePath "C:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01"
    -wasHome "C:\Program Files\IBM\WebSphere\AppServer"
    -logfile "c:\Program Files\IBM\WebSphere\AppServer\profiles\
       Custom01\logs\ws_startserver.log"
    -logRoot "c:\Program Files\IBM\WebSphere\AppServer\profiles\
       Custom01\logs\nodeagent"
    -restart true
    ```

    Exemple de sortie de la commande :

    ```
    Adding Service: ndagentwinser
      Config Root:
      C:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01\config
      Server Name: nodeagent
      Profile Path: C:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01
      Was Home: C:\Program Files\IBM\WebSphere\AppServer\
      Start Args:
      Restart: 1
    IBM WebSphere Application Server V6.1
       - ndagentwinser service successfully added
    ```

    Pour obtenir un message relatif à la syntaxe de la commande **wasservice**, entrez :

    ```
    > WASService.exe
    ```

    sans spécifier d'argument.
14. Si l'exécution a lieu dans un environnement groupé, modifiez le service WebSphere depuis l'étape précédente afin qu'il démarre en tant qu'utilisateur de la délégation (tfimdeleguser)

    a. Ouvrez les **Services** dans le Panneau de configuration et recherchez le service correspondant soit au composant d'exécution Tivoli Federated Identity Manager, soit à l'agent de noeud du composant d'exécution Tivoli Federated Identity Manager dans le cas d'un environnement groupé.
    b. Cliquez sur l'onglet Connexion.

c. Spécifiez l'utilisateur de la délégation `tfimdeleguser`

d. Indiquez le mot de passe de l'utilisateur de la délégation. Cliquez sur **OK**.

15. Redémarrez l'agent de noeud WebSphere.

    Cette étape est nécessaire pour assurer que le gestionnaire de noeud Websphere démarre bien les noeuds sous la nouvelle identité.

    a. Connectez-vous à la console WebSphere.

    b. Cliquez sur **Serveurs -> Serveurs d'applications** dans le cas d'un environnement autonome, ou sur **Serveurs -> Clusters** dans le cas d'un environnement groupé.

    c. Cochez la case définissant le redémarrage du serveur ou du cluster et appuyez sur le bouton **Arrêt** pour un environnement autonome, ou sur le bouton **Démarrage en cascade** pour un environnement groupé.

    d. Dans un environnement autonome, une fois que l'arrêt du serveur a eu lieu, cochez la case définissant le redémarrage du serveur ou du cluster et appuyez sur le bouton **Démarrer**.

Que faire ensuite

Autres informations :

- Principes de configuration de Microsoft :

  http://technet2.microsoft.com/windowsserver/en/library/c312ba01-318f-46ca-990e-a597f3c294eb1033.mspx?mfr=true

- Instructions de configuration :

  http://technet2.microsoft.com/windowsserver/en/library/e5d4cdbd-f071-4a1a-b24e-92713f7fafc11033.mspx?mfr=true

- Instructions IBM pour la configuration de l'exécution de WebSphere en tant que compte autre que **Système local**

  http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/topic/com.ibm.websphere.base.doc/info/aes/ae/tsec_actwindows.html

Chapitre 32. Configuration de Tivoli Federated Identity Manager pour un scénario de jonction Kerberos

Avant de configurer la délégation Kerberos, assurez-vous d'avoir créé un domaine, tel que décrit au Chapitre 1, «Configuration de domaine», à la page 3.

Etapes de configuration :

1. «Planification de configuration de la chaîne d'accréditation»
2. Exécution de l'étape «Formulaire de configuration de chaîne d'accréditation», à la page 413
3. «Création d'une instance de module de délégation contrainte Kerberos», à la page 415
4. «Création d'une chaîne d'accréditation pour la délégation contrainte Kerberos», à la page 416

Planification de configuration de la chaîne d'accréditation

Pour déployer une chaîne d'accréditation destinée à la délégation contrainte Kerberos, vous devez accomplir les deux tâches suivantes :

1. Créez une instance du module de service d'accréditation pour la délégation contrainte Kerberos.
2. Créez une chaîne d'accréditation pour la délégation contrainte Kerberos.

Tivoli Federated Identity Manager fournit des assistants de configuration pour chaque tâche. Les assistants vous invitent à spécifier les valeurs des propriétés de configuration requises.

Instance de module de délégation Kerberos

L'ensemble des modules d'accréditation par défaut de Tivoli Federated Identity Manager n'inclut aucune instance du type de module de délégation contrainte Kerberos. Vous devez créer cette instance.

Bien que la création de plusieurs instances soit possible, il convient de n'en créer qu'une seule pour chaque domaine Tivoli Federated Identity Manager. Cette instance peut être utilisée par n'importe quelle chaîne de modules requise.

Les raisons de cette limitation à une seule instance est liée au fait que ce module de délégation contrainte Kerberos charge une bibliothèque DLL native (bibliothèque Windows chargée dynamiquement) qui est partagée par toutes les instances du module. Toutes les instances doivent par conséquent partager les mêmes paramètres de configuration.

Lorsque plusieurs instances de module sont créées, seul le *dernier* module à être initialisé détermine la taille de la mémoire cache utilisateur créée dans le code natif. Pour éviter toute confusion, la meilleure pratique consiste à ne créer qu'une seule instance de module.

Type de module
Cette propriété obligatoire est demandée dans le panneau relatif au type de module. Le type de module à utiliser est le suivant :

```
com.tivoli.am.fim.trustserver.sts.modules.KerberosDelegationSTSModule
```

Nom de l'instance de module
Cette propriété obligatoire est demandée dans le panneau relatif au nom de l'instance de module. Entrez une chaîne de votre choix. Par exemple :

```
MyKerberosDelegationInstance
```

Description de l'instance de module
Cette propriété facultative est demandée dans le panneau relatif au nom de l'instance de module. Vous pouvez entrer une chaîne qui décrit cette instance.

Taille maximale de la mémoire cache des données d'identification de l'utilisateur

Cette propriété obligatoire est demandée dans le panneau de configuration du module de délégation Kerberos. Ce nombre détermine les indicateurs de personnification et les données d'identification de l'utilisateur placées en cache dans le fichier DLL chargé par le module. La mise en cache est effectuée dans le but d'améliorer les performances. Définissez cette valeur sur le nombre approximatif attendu d'utilisateurs finals simultanés du service pour les transactions de gros volumes.

Le paramètre par défaut est 100.

Remarque : Plus ce chiffre est élevé, plus la quantité de mémoire utilisable par le module d'exécution de Tivoli Federated Identity Manager est importante.

Chaîne d'accréditation de délégation Kerberos

Nom du mappage de chaîne

Cette propriété obligatoire est demandée dans le panneau relatif à l'identification du mappage de chaîne. Vous pouvez indiquer n'importe quel nom pour la chaîne. Par exemple :

```
ivcred_to_kerberos
```

Description de chaîne
Cette propriété facultative est demandée dans le panneau relatif à l'identification du mappage de chaîne. cette description peut correspondre à n'importe quelle chaîne de caractères.

Créer une chaîne dynamique
Cette propriété est demandée dans le panneau relatif à l'identification du mappage de chaîne. Cette option n'est pas utilisée avec les chaînes d'accréditation de délégation Kerberos. Désélectionnez cette option.

Type de requête
Cette propriété obligatoire est demandée dans le panneau relatif à la recherche du mappage de chaîne. Sélectionnez **Emettre URI Oasis**

Type de recherche
Sélectionnez le bouton d'option **Utiliser les éléments WS-Trust habituels (AppliesTo, Issuer et Token)**.

(AppliesTo) Adresse
Cette propriété obligatoire est demandée dans le panneau relatif à la recherche du mappage de chaîne. Entrez une **Adresse** qui corresponde à la propriété **applies-to** définie dans la section [tfimsso:*jct_name*du fichier de configuration WebSEAL. Par exemple :

```
http://websealhost.example.com/kerbjct
```

(AppliesTo) Nom du service
Cette propriété obligatoire est demandée dans le panneau relatif à la recherche du mappage de chaîne.

Cette propriété comporte deux zones.

Dans la première zone, définissez un astérisque (*) pour que cette valeur renvoie à tous les noms de service, ou spécifiez la valeur de la propriété service-name dans la section [tfimsso:*jct name*] du fichier de configuration WebSEAL.

Dans la seconde zone, définissez toujours un astérisque (*) pour cette valeur.

(AppliesTo) Type de port
Cette propriété est demandée dans le panneau relatif à la recherche du mappage de chaîne.

Cette propriété admet deux zones.

Laissez les deux zones vides.

(Issuer) Adresse
Cette propriété obligatoire est demandée dans le panneau relatif à la recherche du mappage de chaîne. Dans la zone **Adresse**, entrez :

```
amwebrte-sts-client
```

(Issuer) Nom du service
Cette propriété est demandée dans le panneau relatif à la recherche du mappage de chaîne. Ne renseignez pas cette zone.

(Issuer) Type de port
Cette propriété est demandée dans le panneau relatif à la recherche du mappage de chaîne. Ne renseignez pas cette zone.

Type de jeton
Cette propriété obligatoire est demandée dans le panneau relatif à la recherche du mappage de chaîne. Sélectionnez **Kerberos GSS V5**.

Initialiser la chaîne au démarrage de l'exécution
Cette propriété obligatoire est demandée dans le panneau relatif à l'identification de chaîne. *Ne sélectionnez pas* cette option

Instances de modules et modes
Ces propriétés obligatoires sont demandées dans le panneau Assemblage de chaîne.

Le panneau Assemblage de chaîne vous invite à spécifier les valeurs des Instances de module dans la chaîne. Pour chaque instance de module, vous devez sélectionner un mode. Ensuite, vous cliquez sur un bouton pour ajouter la paire de valeurs instance/mode à la chaîne.

Dans le cas de la délégation contrainte Kerberos, vous pouvez configurer une séquence particulière de modules de service d'accréditation :

1. La première instance de module est **Jeton IVCred par défaut**. Choisissez un mode **validation**
2. La seconde instance est l'instance de module de la délégation que vous avez créée, et qui est nommée d'après la propriété **Nom d'instance de module** via l'assistant correspondant. Dans notre exemple, nous avons utilisé :

   ```
   MyKerberosDelegationInstance
   ```

   Sélectionnez l'onglet **Emission**.

Remarque : L'assistant vous avertira que la chaîne ne contient aucune module en mode **mappage**. Pour la délégation contrainte Kerberos, le mode mappage n'est pas obligatoire.

vous pouvez ajouter un mode de mappage si votre déploiement le nécessite. Un module de mappage est nécessaire su le nom d'utilisateur de Tivoli Access Manager doit être mappé avec un autre nom du registre Active Directory.

Dans un déploiement typique, ce mappage n'est pas obligatoire. Dans de nombreux déploiements, par exemple, Tivoli Access Manager est installé de manière à utiliser le registre Active Directory. Dans pareil cas, il n'existe qu'une identité par utilisateur.

Activer la validation des signatures
Cette propriété est demandée dans le panneau de configuration du module Access Manager Credential (IVCred). *Ne sélectionnez pas* cette option

Nom principal du service cible par défaut
Cette propriété est demandée dans le panneau de configuration du module de délégation Kerberos en tant que propriété de Partenaire.

Dans un déploiement typique, vous pouvez laisser cette zone vide.

cette valeur peut être utilisée pour les clients WS-Trust qui n'envoient pas le SPN (Service Principal Name) cible dans l'élément AppliesTo/ ServiceName du jeton RST (RequestSecurityToken). De plus, les clients ne disposent d'aucune règle de mappage pour configurer le SPN cible en tant qu'attribut de contexte pour l'utilisateur STSUU (Security Token Service Universal User).

Options permettant d'ajouter un nom d'utilisateur Tivoli Access Manager pour les besoins de l'authentification Kerberos
Ces options permettent d'indiquer si un module va automatiquement ajouter un suffixe au nom d'utilisateur STSUniversalUser. Elle sont utiles lors du déploiement du module de délégation Kerberos via un déploiement Tivoli Access Manager WebSEAL. Options :

- Ne pas ajouter de suffixe au nom d'utilisateur.

  Cette option laisse le nom d'utilisateur tel quel.
- Ajouter le domaine DNS de la machine en tant que suffixe au nom d'utilisateur.

  Cette option ajoute automatiquement le domaine DNS en tant que suffixe pour la machine d'exécution Tivoli Federated Identity Manager au nom principal dans STSUniversalUser avant d'appeler l'API Windows pour obtenir un ticket Kerberos. Le nom de domaine DNS est lu à partir de la clé de registre Windows suivante :

  `SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Domain`

  Cette option optimise le comportement du module en vue d'une utilisation dans les configurations Tivoli Access Manager utilisant les jonctions Kerberos. L'ajout du domaine DNS permet à l'API Windows d'établir une correspondance correcte entre le nom d'utilisateur et l'enregistrement utilisateur du registre d'utilisateurs Active Directory.

  Notez que ce module ajoute automatiquement le nom de domaine DNS lorsque le nom principal STSUniversalUser ne contient *pas* déjà le caractère @. Cela signifie que si une règle de mappage a été utilisée pour

ajouter un suffixe contenant le caractère @ au nom principal d'utilisateur ou si le nom d'utilisateur Tivoli Access Manager contient le caractère @, ce paramètre n'a aucun effet.

- Ajouter le suffixe configuré au nom d'utilisateur

  Cette option optimise le comportement du module en vue d'une utilisation dans les configurations Tivoli Access Manager utilisant les jonctions Kerberos.

  Cette option permet à l'administrateur d'indiquer le suffixe manuellement. Cette option est réservée aux cas particuliers où l'attribut userPrincipalName de l'utilisateur ne correspond pas au nom de domaine DNS de la machine Windows exécutant l'environnement d'exécution de Tivoli Federated Identity Manager. Cette option n'a aucun effet lorsque le nom principal contient déjà le caractère @.

  Suffixe à ajouter en cas d'utilisation d'un suffixe configuré
  Par exemple :

  ```
  @mondomaine.com
  ```

Formulaire de configuration de chaîne d'accréditation

Complétez ces formulaires avant de configurer la chaîne d'accréditation. Les propriétés des formulaires sont décrites à la rubrique «Planification de configuration de la chaîne d'accréditation», à la page 409.

Formulaire d'instance de module Kerberos

Les tableaux suivants correspondent aux panneaux présentés par l'assistant de création des instances de module.

Tableau 114. Propriétés des panneaux d'identification de module

Propriété	Valeur
Type de module	com.tivoli.am.fim.trustserver.sts.modules.KerberosDelegationSTSModule
Nom de l'instance de module	
Description de l'instance de module	

Tableau 115. Propriété du panneau pour la configuration du module de délégation Kerberos

Propriété	Votre valeur
Taille maximale des données d'identification de l'utilisateur	Valeur par défaut : 100

Formulaire de chaîne d'accréditation pour le module Kerberos

L'assistant de chaîne d'accréditation affiche une série de panneaux de configuration. Les tableaux suivants correspondent à chaque panneau.

Tableau 116. Propriétés d'identification de mappage de chaîne

Propriété	Votre valeur
Nom du mappage de chaîne	

Tableau 116. Propriétés d'identification de mappage de chaîne (suite)

Propriété	**Votre valeur**
Description de chaîne	
Créer une chaîne dynamique	*Cette option doit être désélectionnée*

Tableau 117. Propriétés de recherche de mappage de chaîne

Propriété	**Votre valeur**
Type de requête	Emettre URI Oasis
Type de recherche	Utiliser les éléments WS-Trust habituels (AppliesTo, Issuer et TokenType)
(AppliesTo) Adresse	
(AppliesTo) Nom du service	*Deux zones* Utilisez un astérisque (*) pour chaque zone
(AppliesTo) Type de port	*Deux zones* Laissez les deux zones vides
(Issuer) Adresse	
(Issuer) Nom du service	*Deux zones* Laissez les deux zones vides
(Issuer) Type de port	*Deux zones* Laissez les deux zones vides
Type de jeton	Kerberos GSS V5

Tableau 118. Panneau d'identification de chaîne

Propriété	**Votre valeur**
Initialiser la chaîne au démarrage de l'exécution	*Ne sélectionnez pas cette option*

Tableau 119. Panneau d'assemblage de chaîne

Propriété	**Votre valeur**
Première instance de module	Jeton IVCred par défaut
Premier mode de module	valider
Seconde instance de module	*Nom de l'instance de module Kerberos*:
Second mode de module	Issue (Emission)

Tableau 120. Propriété de configuration du module Tivoli Access Manager Credential

Propriété	**Votre valeur**
Activer la validation des signatures	*Désélectionnez cette option*

Tableau 121. Propriété de configuration (mode Emission) du module de délégation Kerberos

Propriété	Votre valeur
Nom principal du service cible par défaut	
Options pour l'ajout d'un nom d'utilisateur Tivoli Access Manager pour l'authentification Kerberos : • Ne pas ajouter de suffixe au nom d'utilisateur. • Ajouter le domaine DNS de la machine en tant que suffixe au nom d'utilisateur. • Ajouter le suffixe configuré au nom d'utilisateur **Suffixe à ajouter en cas d'utilisation d'un suffixe configuré** Par exemple : `@mondomaine.com`	

Création d'une instance de module de délégation contrainte Kerberos

Pourquoi et quand exécuter cette tâche

Un assistant vous guide tout au long de la création de l'instance de module. Pour plus d'informations sur chacune des propriétés requises, voir «Planification de configuration de la chaîne d'accréditation», à la page 409.

vous pouvez également consulter le document «Formulaire de configuration de chaîne d'accréditation», à la page 413.

Pour créer une instance de module, procédez comme suit :

Procédure

1. Connectez-vous à la console WebSphere.
2. cliquez sur **Tivoli Federated Identity Manager -> Configurer le service d'accréditation -> Instances de module** Le portlet Instances de module s'affiche.
3. uliquez sur **Créer**. L'assistant Instance de module démarre et le panneau Type de module s'affiche.
4. Sélectionnez **com.tivoli.am.fim.trustserver.sts.modules.KerberosDelegationSTSModule**. Cliquez sur **Suivant**. L'écran Nom d'instance de module s'affiche.
5. Entrez une valeur dans la zone Nom d'instance du module.

   Par exemple :

   `Jonction Kerberos`
6. Si vous le souhaitez, vous pouvez entrer une chaîne dans la zone Description de l'instance de module .
7. Cliquez sur **Suivant**. Le panneau Configuration du module de délégation Kerberos s'affiche.

8. Entrez une valeur dans la zone **Taille maximale de la mémoire cache des données d'identification de l'utilisateur**.
9. Cliquez sur **Terminer**. Le panneau Instances de module s'affiche. Le portlet du domaine Current s'affiche également et vous invite à spécifier les nouvelles modifications de la configuration.
10. Cliquez sur le bouton **Charger les modifications de configuration dans l'environnement d'exécution de Tivoli Federated Identity Manager**.
11. Passez à l'étape «Création d'une chaîne d'accréditation pour la délégation contrainte Kerberos».

Création d'une chaîne d'accréditation pour la délégation contrainte Kerberos

Avant de commencer

Le domaine doit contenir une instance du module de service d'accréditation pour la délégation contrainte Kerberos avant que la chaîne d'accréditation ne soit créée. Si vous n'avez pas encore créé d'instance, procédez à cette opération maintenant. Voir «Création d'une instance de module de délégation contrainte Kerberos», à la page 415.

Pourquoi et quand exécuter cette tâche

Pour configurer correctement la chaîne d'accréditation, vous devez vous assurer que les propriétés sont alignées sur les propriétés de configuration WebSEAL. Avant d'exécuter l'assistant de chaîne d'accréditation, il convient de d'accomplir les tâches suivantes :

- consultez la rubrique «Planification de configuration de la chaîne d'accréditation», à la page 409
- Exécutez la procédure indiquée à la rubrique «Formulaire de configuration de chaîne d'accréditation», à la page 413

Pour créer la chaîne d'accréditation :

Procédure

1. Connectez-vous à la console WebSphere.
2. Cliquez sur **Tivoli Federated Identity Manager -> Configurer le service d'accréditation -> Chaînes du service d'accréditation**. Le portlet Chaînes du service d'accréditation s'affiche.
3. uliquez sur **Créer**. L'assistant de configuration démarre. La page Introduction s'affiche.
4. Cliquez sur **Suivant**. Le panneau Identification du mappage de chaîne s'affiche.
5. Entrez les valeurs demandées.
   a. Entrez un nom dans la zone **Nom du mappage de chaîne**.
   b. En option, renseignez la zone Description.
   c. *Ne sélectionnez pas* la zone **Créer une chaîne dynamique**
   d. Cliquez sur **Suivant**. Le panneau **Recherche de mappage de chaîne** s'affiche.
6. Entrez les valeurs demandées.
   a. Pour l'option **Type de requête**, sélectionnez **Emettre URI Oasis**

La valeur d'URI du type de requête correspondante est automatiquement entrée par l'assistant.

b. Définissez l'option **Type de recherche** sur **Utiliser les éléments WS-Trust habituels (AppliesTo, Issuer et TokenType)**.

c. Entrez des valeurs dans la section **AppliesTo**.

Entrez des valeurs pour les zones :

- **Adresse**

  Par exemple :

  ```
  http://websealhost.example.com/krbjct
  ```

- **Nom de service**.

  Définissez par exemple les deux zones avec un astérisque (*).

- Ne renseignez pas les zones **Type de port**.

Pour obtenir de l'aide, voir «Planification de configuration de la chaîne d'accréditation», à la page 409.

d. Entrez des valeurs dans la section **Emetteur**.

- Dans la zone **Adresse**, entrez :

  ```
  amwebrte-sts-client
  ```

- N'indiquez aucune valeur dans les zones **Nom du service** et **Type de port**.

e. Pour le **Type de jeton**, sélectionnez **Kerberos GSS V5**

f. Cliquez sur **Suivant**.

Le panneau Identification de chaîne s'affiche.

7. *Ne sélectionnez pas* l'option **Initialiser la chaîne au démarrage de l'exécution**. Cliquez sur **Suivant**.

   Le panneau **Assemblage de chaîne** s'affiche.

8. Créez la chaîne d'accréditation :

   a. Pour l'instance de module, sélectionnez l'option **Jeton IVCred par défaut**

   b. Pour le mode, choisissez **validation**

   c. Cliquez sur **Ajouter l'instance de module sélectionnée à la chaîne**.

   d. Pour l'instance de module, sélectionnez le nom d'instance de module que vous avez spécifié à la rubrique «Création d'une instance de module de délégation contrainte Kerberos», à la page 415. Par exemple :

   ```
   Jonction Kerberos
   ```

   e. Pour le mode, choisissez **émission**

   f. Cliquez sur **Ajouter l'instance de module sélectionnée à la chaîne**.

9. Cliquez sur **Suivant**.

   Remarque : Un avertissement s'affiche pour vous signaler qu'un module est manquant dans votre chaîne en mode mappage. Vous pouvez ignorer cet avertissement. Pour plus d'informations, voir «Planification de configuration de la chaîne d'accréditation», à la page 409.

   L'écran Configuration du module de droits d'accès Access Manager (IVCred) s'affiche.

10. *Ne sélectionnez pas* l'option **Activer la validation des signatures**. Cliquez sur **Suivant**.

    Le panneau Configuration du module de délégation Kerberos s'affiche.

11. Si nécessaire, définissez le nom principal du service cible par défaut ou changez les options relatives à l'ajout d'un suffixe au nom d'utilisateur Tivoli Access Manager pour l'authentification Kerberos.

    Remarque : Dans la plupart des cas, vous pouvez laisser cette zone vide et conserver la sélection par défaut de ces options. Voir «Planification de configuration de la chaîne d'accréditation», à la page 409.
12. Cliquez sur **Suivant**. Le panneau Récapitulatif s'affiche.
13. Cliquez sur **Terminer**.
14. Dans le portlet Domaine en cours, cliquez sur **Charger les modifications de configuration dans l'environnement d'exécution de Tivoli Federated Identity Manager**.

Résultats

La configuration de la chaîne d'accréditation est à présent terminée.

Remarques sur la configuration de Tivoli Federated Identity Manager

Vérification de la configuration de la chaîne d'accréditation de Tivoli Federated Identity Manager

Vérification de l'aptitude du gestionnaire de déploiement WebSphere à communiquer avec l'instance WebSphere Application Server hébergeant Tivoli Federated Identity Manager.

Pour ce faire, accédez à l'adresse URL :

```
http://<serveur_IHS>/TrustServerWST13/RequestSecurityToken
```

Un modèle de réponse semblable au suivant s'affiche :

```
RequestSecurityToken ... Hi there this is an AXIS service!
 Perhaps there will be a form for invoking the service here...
```

Vérification des mappages de modules WebSphere

Assurez-vous que les mappages de module WebSphere Application Server et des hôtes virtuels ont été propagés. Pour ce faire, accédez à l'adresse URL :

```
http://<serveur_IHS>/Info/InfoService
```

Un modèle de réponse semblable au suivant s'affiche :

```
Hi there this is a Web service!
```

Haute disponibilité dans une configuration en clusters

De multiples serveurs WAS sont déployés dans un cluster WAS afin d'obtenir une haute disponibilité. Les noeuds WAS individuels membres du cluster reçoivent des instructions de configuration en provenance d'un gestionnaire de déploiement.

La plupart des tâches administratives sont accomplies en communiquant avec le gestionnaire de déploiement. Cependant, tous les flux de protocole nécessaires aux demandes de service pour le service d'accréditation TFIM sont servis par les noeuds WAS individuels. En cas de défaillance du gestionnaire de déploiement, ces flux de protocole n'en subissent aucune conséquence. En revanche, en cas de défaillance des noeuds WAS, un impact a lieu sur le flux de protocole.

Chapitre 33. Configuration de WebSEAL

Vous devez installer et configurer le serveur de règles Tivoli Access Manager avant d'installer WebSEAL. Ces instructions supposent que vous avez installé et configuré avec succès le serveur de règles.

Effectuez une installation standard de WebSEAL. La procédure exacte dépend de votre environnement de déploiement. Pour plus d'informations, voir le document *IBM Tivoli Access Manager Installation Guide*.

Présentation des tâches :

1. «Vérification d'une installation WebSEAL»
2. «Planification de la configuration des jonctions WebSEAL Kerberos», à la page 422
3. Remplissage d'un formulaire «Formulaire de configuration de jonction Kerberos», à la page 426
4. «Débogage d'une jonction WebSEAL Kerberos», à la page 427

Vérification d'une installation WebSEAL

Avant de commencer

Ces instructions supposent que vous avez installé et configuré IBM Tivoli Access Manager for e-business. Elles supposent également que vous avez installé et configuré avec succès le serveur WebSEAL. La présente rubrique explique comment vérifier que la configuration de base du serveur WebSEAL est correcte, afin que vous puissiez étendre la configuration à la prise en charge des jonctions Kerberos.

Pourquoi et quand exécuter cette tâche

Pour vérifier la configuration de base, créez une jonction WebSEAL normale et vérifiez que Tivoli Access Manager affiche correctement une invite de connexion utilisateur.

Procédez comme suit :

Procédure

1. Obtenez le nom du serveur WebSEAL.

   Le nom de serveur dépend du nom d'hôte. Si par exemple le nom d'hôte est `websealhost` :

   ```
   pdadmin sec_master> server list
     default-webseald-websealhost
   ```

2. Créez une jonction simple.

   A titre d'exemple, lorsque le serveur protégé est `mydataserver`, la commande suivante crée une jonction sur `/jct` :

   ```
   pdadmin sec_master> server task default-webseald-websealhost
    create -t tcp -h mydataserver/jct
   ```

3. Obtenez la liste de valeurs de l'objet /WebSEAL.

Cette valeur est nécessaire pour joindre correctement une liste de contrôle d'accès (ACL) :

```
pdadmin sec_master> object list /WebSEAL
  /WebSEAL/websealhost-default
```

4. Rattachez une liste de contrôle d'accès à la nouvelle jonction.

   La liste de contrôle d'accès a pour rôle de contrôler les actions pouvant être exécutées par les utilisateurs spécifiés au sein de l'espace d'objets protégés de Tivoli Access Manager. Cette étape suppose l'existence d'une liste de contrôle d'accès intitulée `testacl`.

   ```
   pdadmin sec_master> acl attach /WebSEAL/websealhost-default/testacl
   ```

5. Pour confirmer que la jonction et la liste de contrôle d'accès sont correctement configurées, procédez comme suit :

   a. Placez un fichier d'essai dans le répertoire documentRoot du serveur Web protégé.

      Par exemple, dans le répertoire documentRoot de `mydataserver`, créez un répertoire de test et ajoutez le fichier index.html pour afficher un contenu quelconque. A titre d'exemple, ajoutez le fichier suivant sous le point de jonction :

      ```
      /testdir/index.html
      ```

   b. Accédez au contenu protégé :

      ```
      https://websealhost.example.com/jct/testdir/index.html
      ```

   c. WebSEAL vous invite à vous connecter. Connectez-vous avec une identité et un mot de passe valides pour Tivoli Access Manager.

      Si l'opération aboutit, vous pouvez afficher le contenu de la page `testdir/index.html`.

Planification de la configuration des jonctions WebSEAL Kerberos

Les propriétés de configuration WebSEAL sont spécifiées dans le fichier de configuration WebSEAL. Le fichier de configuration par défaut est webseald-default.conf. Par exemple, sur les systèmes UNIX or Linux :

```
/opt/pdweb/etc/webseald-default.conf
```

Le fichier de configuration contient les propriétés qui prennent en charge le déploiement des jonctions Kerberos. Avant de pouvoir configurer WebSEAL pour les jonctions Kerberos, vous devez déterminer les valeurs requises par votre déploiement pour chaque propriété.

Les propriétés sont regroupées en deux sections :

```
[tfimsso:jct-id]
[tfim-cluster:cluster]
```

Dans certains cas, l'introduction d'une connexion unique Kerberos sur des serveurs comprenant des jonctions peut influer sur les performances. Chaque jeton Kerberos est valable uniquement pour une authentification Kerberos. WebSEAL doit donc demander un nouveau jeton Kerberos pour chaque transaction séparée. Les performances peuvent être également être réduites par le canal de communications, qui nécessite l'obtention par WebSEAL de jetons via une requête SOAP adressée à Tivoli Federated Identity Manager.

Section [tfimsso:*jct_id*]

Section [tfimsso:*jct_id*]

La section [tfimsso:<jct-id>] permet de définir les options de configuration de la connexion unique Kerberos. Cette section contient les informations de configuration de connexion unique Tivoli Federated Identity Manager pour une seule jonction.

- Pour les jonctions standard, le nom de la section doit être qualifié au moyen du nom du point de jonction, y compris la barre oblique. Par exemple :

  ```
  [tfimsso:/kerbjct]
  ```

- Pour les jonctions d'hôte virtuel, le nom de la section doit être qualifié au moyen du nom du libellé de l'hôte virtuel, par exemple :

  ```
  [tfimsso:www.example.com]
  ```

always-send-tokens

Propriété booléenne. Cette propriété peut être utilisée pour optimiser les performances lorsque le serveur dorsal (comprenant des jonctions) est capable de maintenir l'état de session. Dans ce cas, vous pouvez indiquer si WebSEAL doit envoyer un jeton Kerberos pour chaque requête HTTP ou si WebSEAL doit attendre une réponse 401 avant de demander le jeton.

Une réponse 401 signifie qu'une autorisation est requise. Lorsque l'état de sessionb est maintenu, il n'est pas nécessaire de décerner une autorisation avant chaque requête. Afin de limiter le nombre d'extractions de jetons Kerberos au nombre de fois où une autorisation est requise, définissez la valeur

```
always-send-tokens = false
```

Lorsque le serveur dorsal ne peut maintenir l'état de session et qu'un jeton de sécurité doit être envoyé pour chaque requête HTTP, définissez :

```
always-send-tokens = true
```

applies-to

Cette propriété définit les critères de recherche à appliquer pour localiser le module de service de jeton de sécurité approprié dans Tivoli Federated Identity Manager.

La valeur est généralement un chemin d'accès spécifié selon le format suivant :

```
http://hôte_serveur_webseal/nom_jonction
```

Par exemple :

```
http://websealhost.example.com/kerbjct
```

service-name

Cette propriété essentielle remplit deux objectifs :

1. Spécifier le nom principal de service utilisé lors de la génération d'un jeton Kerberos. Cette valeur est employée par Tivoli Federated Identity Manager lors de la recherche de correspondances avec la chaîne d'accréditation. La configuration de la chaîne Tivoli Federated Identity Manager inclut une section Applies-to contenant une propriété de nom de service. La valeur du paramètre service-name de WebSEAL est comparée à la propriété du nom de service.

   Pour garantir une correspondance exacte, il convient que `service-name` renvoie à la propriété Nom de service dans la configuration de Tivoli Federated Identity Manager.

Remarque : L'un des moyens permettant de trouver une correspondance consiste à utiliser, dans la configuration de Tivoli Federated Identity Manager, un caractère générique tel qu'un astérisque (*).

2. Spécifier le nom principal de service de l'utilisateur délégataire lors de la création du jeton Kerberos. Le nom principal de service (SPN) est défini sur le système Microsoft Windows.

   Pour déterminer le SPN, accédez au serveur Windows et exécutez la commande **setspn**. Par exemple :

   ```
   setspn -L nom_utilisateur
   ```

   Le serveur Web comportant des jonctions est exécuté avec l'identité *nom_utilisateur*. Par exemple, iisuser.

La syntaxe de cette propriété est la suivante :

```
service-name=nom_principal_service
```

Le format est le suivant :

```
HTTP/nom_serveur_IIS.nom_domaine
```

Par exemple :`service-name = HTTP/B16INTEL3.tamad.com`

renewal-window

Période, en secondes, pendant laquelle la durée de validité d'un jeton de sécurité est réduite. Cette entrée sert à compenser les différences ente les heures des systèmes et à permettre la mise en place de temps de transmission pour les jetons de sécurité.

```
renewal-window = 15
```

tfim-cluster-name

Nom du cluster WebSphere sur lequel le service Tivoli Federated Identity Manager est déployé. Il convient que cette valeur corresponde à une autre entrée de section [tfim-cluster:<*cluster*>], où *cluster* désigne **tfim-cluster-name**.

Par exemple :

```
tfim-cluster-name = STSCluster2
```

token-collection-size

Pour optimiser les performances, WebSEAL peut demander plusieurs jetons Kerberos à Tivoli Federated Identity Manager au sein d'une même requête SOAP. Pour cela, la spécification de service Web WS-Trust est requise. Les jetons sont mis en cache dans la session de l'utilisateur, puis réutilisés lors des requêtes ultérieures. WebSEAL ne demande des jetons de sécurité supplémentaires à Tivoli Federated Identity Manager qu'après l'utilisation complète ou l'expiration de tous les jetons placés en cache.

Vous pouvez spécifier le nombre de jetons à extraire de Tivoli Federated Identity Manager. Le nombre de requêtes envoyées à Tivoli Federated Identity Manager décroît à mesure que ce nombre augmente, mais la taille (et le temps de traitement) de chaque requête augmente également. Il peut arriver que les jetons Kerberos soient relativement volumineux. Si vous spécifiez une valeur élevée pour cette propriété, pour pouvez augmenter de façon significative la taille de la session et l'utilisation de la mémoire pour WebSEAL.

La valeur par défaut est 10 :

```
token-collection-size = 10
```

token-type
Le seul type de jeton pris en charge est le type `kerberos`. Il s'agit de la valeur par défaut. Utilisez cette valeur sans la modifier.

Section tfim-cluster

[tfim-cluster:*cluster***]**

Cette valeur définit le nom du cluster WebSphere pour le service Tivoli Federated Identity Manager. Le nom du *cluster* dans cette section doit correspondre à l'option **tfim-cluster-name** définie dans une section **[tfimsso:*jct-id*]**.

server Spécifie le niveau de priorité et l'adresse URL d'un serveur unique Tivoli Federated Identity Manager membre du cluster identifié pour cette section.

Il est possible de faire figurer plusieurs entrées **server** dans la section. Ceci vous permet de spécifier plusieurs entrées de serveur pour les besoins de la reprise en ligne et de l'équilibrage de charge entre WebSEAL et le serveur proxy de WebSphere Application Server. Lorsque le cluster Tivoli Federated Identity Manager est configuré, WebSEAL vérifie l'état du serveur Web Proxy de Tivoli Federated Identity Manager toutes les minutes.

Lorsque vous disposez de plusieurs serveurs, vous pouvez utiliser le niveau de priorité de manière à spécifier l'ordre d'accès aux serveurs lors du traitement. Le niveau de priorité est un nombre entier compris dans la plage [0-9].

Lorsqu'un seul serveur existe, vous pouvez omettre le niveau de priorité. Lorsqu'aucun niveau de priorité n'est spécifié, il est supposé égal à 9 (valeur maximale).

Syntaxe :

```
server = [0-9],URL_serveur
```

Exemple :

```
9,http://mydataserver.example.com/TrustServerWST13/services
/RequestSecurityToken
```

handle-pool-size
Définit le nombre maximal de descripteurs en cache utilisés lors de la communication avec Tivoli Federated Identity Manager.

Valeur par défaut : 10

handle-idle-timeout
Durée, en secondes, avant retrait d'un descripteur initulisé dans la mémoire cache du pool de descripteurs

Valeur par défaut : 240 secondes

timeout
Durée d'attente, en secondes, d'une réponse de la part de Tivoli Federated Identity Manager.

Valeur par défaut : 240 secondes

ssl-keyfile
Nom du fichier de la base de données de clés contenant le certificat client à utiliser.

Les entrées SSL, ainsi que les suivantes, sont facultatives. Elles ne sont requises que dans les cas suivants :

- Au moins une entrée de serveur indique que le protocole SSL (HTTPS) doit être utilisé.
- Nécessité d'un certificat autre que celui qui est utilisé par ce serveur lors des communications avec le serveur de règles.

Remarque : Cette valeur, ainsi que les valeurs d'entrée SSL suivantes, doivent être partagées par toutes les variables du serveur qui exploitent le protocole HTTPS. Lors du déploiement sur un clusterWebSphere, les valeurs doivent être les mêmes pour chaque serveur du cluster qui exploite le protocole HTTPS.

ssl-keyfile-stash
Nom du fichier de mot de passe secret pour le fichier de la base de données de clés.

ssl-keyfile-label
Libellé du certificat client dans la base de données de clés.

ssl-valid-server-dn
Cette entrée de configuration spécifie le nom distinctif du serveur (obtenu à partir du certificat SSL) qui sera accepté. Lorsqu'aucune entrée n'est configurée, tous les noms distinctifs sont considérés comme valides. Il est possible de définir plusieurs noms distinctifs en incluant des entrées de configuration multiples correspondant à ce nom.

ssl-fips-enabled
Cette entrée contrôle l'activation et la désactivation des communications FIPS avec Tivoli Federated Identity Manager. Lorsqu'aucune entrée de configuration n'est présente, le paramètre global FIPS, tel que déterminé par le serveur de règles TAM, entre en vigueur.

Remarque : Pour obtenir une description complète de chaque propriété de la section, reportez-vous au document *IBM Tivoli Access Manager WebSEAL Administration Guide*. Consultez également les commentaires contenus dans le fichier de configuration WebSEAL.

Formulaire de configuration de jonction Kerberos

Ce formulaire permet d'assembler les valeurs à ajouter au fichier de configuration WebSEAL.

Tableau 122. Propriétés des sections tfimsso et tfim-cluster

Propriété	**Votre valeur**
[tfimsso:*ID_jonction*]	
always-send-tokens	Valeur par défaut : false
applies-to	
service-name	
renewal-window	Valeur par défaut : 15
tfim-cluster-name	
token-collection-size	Valeur par défaut : 10
token-type	kerberos

Tableau 122. Propriétés des sections tfimsso et tfim-cluster (suite)

Propriété	Votre valeur
[tfim-cluster:*cluster*]	
serveur	
handle-pool-size	Valeur par défaut : 10
handle-idle-timeout	Valeur par défaut : 240
timeout	Valeur par défaut : 240
ssl-keyfile	
ssl-keyfile-stash	
ssl-keyfile-label	
ssl-valid-server-dn	
ssl-fips-enabled	

Conseils pour la configuration :

- Assurez-vous que la propriété **service-name** correspond à la configuration de la chaîne d'accréditation Tivoli Federated Identity Manager.
- Assurez-vous que la propriété **tfim-cluster-name** correspond à la propriété *cluster* de la section [tfim-cluster:*cluster*].
- Assurez-vous que la propriété *cluster* de la section [tfim-cluster:*cluster*] correspond au nom du cluster WebSphere.

Débogage d'une jonction WebSEAL Kerberos

Pourquoi et quand exécuter cette tâche

La configuration d'une jonction WebSEAL s'effectue en deux étapes :

- Edition du fichier de configuration WebSEAL

  Vous devez spécifier dans le fichier de configuration WebSEAL les propriétés qui permettent de prendre en charge les jonctions spécifiques nécessaires à la connexion unique Kerberos avant de pouvoir créer la jonction via la commande 'pdadmin'.
- Utilisez la commande 'pdadmin' pour créer la jonction et joindre les listes de contrôle d'accès requises.

  Pour créer une jonction standard activée pour la connexion unique Kerberos, exécutez la commande de création de jonction ('server task create') en spécifiant l'option -Y. L'option -Y spécifie que la connexion unique SPNEGO/Kerberos est requise pour la jonction.

  Pour créer une jonction d'hôte virtuel activée pour la connexion unique Kerberos, exécutez la commande de création d'hôte virtuel ('server task create') en spécifiant l'option -Y.

  WebSEAL prend en charge de nombreuses options pour la création de jonctions. vous pouvez associer l'option -Y à d'autres options, suivant les besoins de votre déploiement. Pour obtenir des informations complètes sur les options liées aux jonctions WebSEAL, reportez-vous au document *IBM Tivoli Access Manager WebSEAL Administration Guide*.

Pour configurer une jonction WebSEAL Kerberos :

Procédure

1. Utilisez un éditeur de texte pour éditer le fichier de configuration WebSEAL.

   Spécifiez les valeurs regroupées dans le formulaire pour le support de jonction Kerberos.

   Pour plus d'informations, voir : «Planification de la configuration des jonctions WebSEAL Kerberos», à la page 422
2. Utilisez la commande 'pdadmin' pour créer la jonction Kerberos et joindre les listes de contrôle d'accès (ACL) requises.

   Vous pouvez créer soir des jonctions Kerberos classiques, soit des jonctions Kerberos d'hôte virtuel.

   Remarque :

   - Le nom de la jonction doit correspondre à la valeur *jct_id* définie dans la section [tfimsso:*jct_id*] du fichier de configuration WebSEAL.
   - Assurez-vous que vous avez bien configuré le fichier de configuration WebSEAL conformément au type de jonction que vous prévoyez d'utiliser. Si vous n'avez pas édité le fichier de configuration WebSEAL, la commande d'administration échoue et renvoie un message d'erreur.

   Jonctions Kerberos classiques

   a. Créez la jonction :

   ```
   pdadmin sec_master>  server task default-webseald-websealhost
     create -t tcp -h mydataserver.example.com -Y /kerbjct
   ```

   L'hôte mydataserver.example.com correspond au serveur d'arrière plan IIS.

   b. Rattachez la liste de contrôle d'accès :

   ```
   pdadmin sec_master> acl attach /WebSEAL/websealhost-default/kerbjct testacl
   ```

   Jonctions Kerberos d'hôte virtuel

   a. Créez la jonction :

   ```
   pdadmin sec_master> server task default-webseald-websealhost virtualhost
     create -t tcp -h mydataserver.example.com -v website.example.com
     -Y kerbvirtjct
   ```

   b. Rattachez la liste de contrôle d'accès :

   ```
   pdadmin sec_master> acl attach /WebSEAL/websealhost-default/kerbvirtjct
     testacl
   ```

Résultats

Les messages d'erreur sont consignés dans le fichier journal de configuration WebSEAL. Par exemple, sous UNIX ou Linux :

```
/opt/pdweb/log/msg__webseald-default.log
```

Remarques sur la configuration de WebSEAL

Remarques concernant la configuration entre WebSEAL et le client

- La haute disponibilité pour le serveur WebSEAL s'obtient généralement en plaçant un équilibreur de charge en amont du serveur WebSEAL. Consultez l'article du document IBM Developer Works intitulé *Load Balancers for Tivoli Access Manager* :

  http://www-128.ibm.com/developerworks/tivoli/library/t-tlb/index.html

- La sécurité des canaux de communication entre le client et WebSEAL est généralement assurée grâce à l'acquisition d'un certificat SSL destiné au serveur WebSEAL.
- Les clients peuvent s'authentifier à WebSEAL via n'importe quelle méthode prise en charge.
- Aucune modification de ces configurations standard n'est nécessaire pour prendre en charge les jonctions Kerberos.

Remarques concernant la configuration des communications entre WebSEAL et la jonction

- La haute disponibilité pour le serveur de la jonction s'obtient généralement en configurant des serveurs de jonctions multiples pour le point de jonction. Consultez l'article du document IBM Developer Works intitulé *Load Balancers for Tivoli Access Manager* :

  http://www-128.ibm.com/developerworks/tivoli/library/t-tlb/index.html
- La sécurité des canaux de communication entre WebSEAL et la jonction est généralement assurée via l'authentification mutuelle de certificats SSL.
- Aucune modification de ces configurations standard n'est nécessaire pour prendre en charge les jonctions Kerberos.

Synchronisation temporelle entre WebSphere et WebSEAL

Vérifiez que les paramètres temporels sont synchronisés entre le système hébergeant l'instance WebSphere Application Server qui exécute Tivoli Federated Identity Manager et le système hébergeant l'instance Tivoli Access Manager WebSEAL.

Pour afficher les paramètres, procédez comme suit :

1. Sur le système WebSphere, accédez aux options Default Domain Security Settings, puis Account Policies et Kerberos Policy.
2. Examinez la tolérance maximale définie pour la synchronisation de l'horloge système.

Si l'écart horaire entre l'instance WebSphere Application Server et le serveur WebSEAL est importante, il se peut que les jetons de sécurité générés par Tivoli Federated Identity Manager expirent avant de pouvoir être utilisés.

Messages d'erreur de configuration

Les messages d'erreur suivants s'affichent lorsqu'une ou plusieurs des conditions suivantes sont vérifiées :

- La propriété service-name ne correspond pas à la configuration de la chaîne d'accréditation de Tivoli Federated Identity Manager
- WebSEAL extrait des jetons de Tivoli Federated Identity Manager, mais ceux-ci ont expiré. Cette situation peut par exemple se produire lorsque les paramètres temporels des serveurs ne sont pas synchronisés.
- Le navigateur renvoie une erreur. Par exemple :

```
Erreur du serveur
Access Manager WebSEAL could not complete your request due to an
unexpected error.
Diagnostic Information
Method: GET
URL: /kjct/index.html
Error Code: 0x38cf027c
Error Text: DPWWA0636E No TFIM single sign-on tokens were available.
```

- Le fichier journal WebSEAL contient des erreurs. Par exemple (certaines lignes sont scindées pour d es raisons de mise en forme) :

```
DPWWA2852E   An error occurred when attempting to communicate with the SOAP
  server URL
http://d06win13.testlab.example.com/TrustServerWST13/services/
  RequestSecurityToken: +JNI:
Error running InitializeSecurityContext for HTTP/d02jlnx.testlab.example.com:
-2146893042 (No credentials are available in the security package).
File h:\fim620\src\kerberoswin32\KerbUserState.cpp,
 line 641  (error code: 71/0x47).
2008-03-04-13:08:10.080-06:00I----- 0x38CF027C
webseald ERROR wwa sso ThirdPartyJunction.cpp 4124 0x00000070
DPWWA0636E   No TFIM single sign-on tokens were available.
```

Débogage d'une jonction Kerberos

Pour effectuer le débogage d'un déploiement de jonction Kerberos, activez la fonction de trace sur Tivoli Federated Identity Manager et Tivoli Access Manager. Un point de trace approprié pour Tivoli Access Manager et WebSEAL est : pdweb.sso.tfim.

Par exemple, dans un environnement Linux ou UNIX :

```
pdadmin> server task default-webseald-c1sun1 trace set pdweb.sso.tfim 9
  file path=/var/pdweb/log/debug.log
```

Pour désactiver la fonction de trace, définissez la valeur du niveau de trace sur 0.

Configuration de WebSEAL pour gérer les cookies

Par défaut, WebSEAL ne supprime aucun cookie à la déconnexion. Si vous comptez configurer WebSEAL pour gérer les cookies, la liste des cookies gérés ne doit pas inclure le cookie de session WebSphere.

Chapitre 34. Tâche de configuration SSL pour un déploiement de jonctions Kerberos

Pour une sécurité optimale, configurez les communications SSL entre serveurs dans un déploiement de jonctions Kerberos.

Cette rubrique présente les étapes de configuration d'un environnement groupé WebSphere en vue d'utiliser des communications SSL entre les instances WebSEAL, IBM HTTP Server (IHS), WebSphere Application Server Plug-in, WebSphere Application Server et Tivoli Federated Identity Manager. Ces procédures ne concernent pas les communications SSL entre le client et WebSEAL, ni avec le serveur Web d'arrière-plan. Aucune modification de ces configurations SSL standard n'est nécessaire pour prendre en charge les jonctions Kerberos.

Conseil : Envisagez le déploiement d'une configuration opérationnelle sans SSL, avant d'ajouter le protocole SSL.

Pour chaque composant, créez une paire de clés publique/privée et extrayez la clé publique vers un emplacement connu.

Sur le serveur WebSEAL :

1. Copiez la clé publique IHS sur le système WebSEAL
2. Exécutez l'utilitaire **ikeyman** pour ajouter la clé publique IHS. Lorsque l'environnement comprend plusieurs instances Proxy IHS, accomplissez cette procédure pour chaque serveur IHS.
3. Configurez les valeurs appropriées pour les variables `[tfim-cluster:cluster]` suivantes : server, ssl-keyfile, ssl-keyfile-stash. En option, configurez la variable ssl-valid-server-dn le cas échéant.

   Pour plus d'informations, voir «Planification de la configuration des jonctions WebSEAL Kerberos», à la page 422.
4. Redémarrez WebSEAL pour activer les modifications apportées au fichier de configuration WebSEAL.

Sur le serveur IBM HTTP Server :

1. Copiez la clé publique WebSEAL sur le système IHS.
2. Exécutez l'utilitaire ikeyman sur IHS pour ajouter la clé publique WebSEAL.
3. Copiez la clé publique WebSphere du système WebSphere Deployment Manager (dmgr) vers le système IHS.
4. Exécutez l'utilitaire ikeyman sur IHS pour ajouter la clé publique WebSphere.
5. Mettez à jour le fichier httpd.conf pour configurer ou ajouter un hôte virtuel prenant en charge les connexions SSL.
6. Redémarrez l'instance IHS pour activer les modifications.
7. Lorsque votre déploiement comprend des instances de proxy IHS multiples, répétez la procédure ci-dessus pour chaque proxy IHS.

Dans le module d'extension WebSphere situé sur le serveur IHS :

1. Copiez la clé publique WebSphere sur le système hébergeant le module d'extension.
2. Exécutez l'utilitaire ikeyman pour le module d'extension afin d'ajouter la clé publique WebSphere.
3. Copiez la clé publique WebSphere du noeud WebSphere vers le serveur hébergeant le module d'extension.
4. Exécutez l'utilitaire ikeyman pour le module d'extension afin d'ajouter la clé publique du noeud WebSphere.
5. Lorsque votre déploiement comprend de multiples modules d'extension, répétez la procédure ci-dessus pour chaque module d'extension.

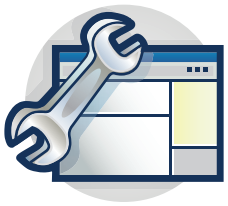
Sur l'instance WebSphere Network Deployment Manager (dmgr) :

1. Assurez-vous que la clé publique du module d'extension est référencée sous un chemin accessible via la console d'administration WebSphere.
2. Utilisez la console WebSphere pour ajouter la clé publique du module d'extension à CellDefaultTrustStore.
3. Lorsque votre déploiement comprend de multiples modules d'extension, répétez la procédure ci-dessus pour chaque module d'extension.
4. Assurez-vous que la clé publique du noeud est référencée sous un chemin accessible via la console d'administration WebSphere.
5. Utilisez la console WebSphere pour ajouter la clé publique du noeud à CellDefaultTrustStore.
6. Lorsque votre déploiement comprend de multiples noeuds, répétez la procédure ci-dessus pour chaque noeud.
7. Si nécessaire, configurez l'authentification client pour votre déploiement.

Sur le noeud WebSphere :

1. Assurez-vous que la clé publique du gestionnaire de déploiement (DMGR) est référencée sous un chemin accessible via la console d'administration WebSphere.
2. Utilisez la console WebSphere pour ajouter la clé publique du gestionnaire de déploiement à NodeDefaultTrustStore.
3. Lorsque votre déploiement comprend de multiples noeuds, répétez la procédure ci-dessus pour chaque noeud.

Partie 5. Configuration de User Self Care



Les rubriques de la section Configuration vous guident pas à pas lors de la configuration de User Self Care.

Cette section présente le déploiement de User Self Care. Veuillez d'abord consulter la présentation de la fonction User Self Care :

Chapitre 35, «Découverte de User Self Care», à la page 435

Chapitre 35. Découverte de User Self Care

User Self Care fournit une méthode grâce à laquelle les utilisateurs peuvent être mis à disposition dans des environnements entreprise à client. User Self Care effectue cette mise à disposition en fournissant un ensemble d'opérations que les utilisateurs peuvent utiliser pour créer et gérer leurs propres comptes. Ces opérations incluent :

- Création d'un compte
- Création et mise à jour des attributs associés au compte
- Modification des mots de passe
- Récupération des mots de passe et ID utilisateur oubliés
- Suppression de comptes

User Self Care est basé sur la technologie STS Tivoli Federated Identity Manager. Avec l'infrastructure STS, les administrateurs peuvent brancher leurs modules de consommation et de création de jeton. User Self Care utilise l'infrastructure STS et les composants HTTP de Tivoli Federated Identity Manager, mais il n'est pas utilisé pour la consommation et création de jeton.

Les utilisateurs accèdent aux opérations de User Self Care via une interface HTTP. Les utilisateur interagissent avec les pages Web qui demandent des entrées, collectent des données et fournissent du feedback. User Self Care fournit un petit ensemble d'URL servant de noeuds finaux pour accéder aux opérations.

Vous pouvez personnaliser User Self Care. Les plug-ins de modules STS démarrés de manière séquentielle dans une chaîne implémentent la logique commerciale. Pour d'autres fonctions pour chaque chaîne, vous pouvez remplacer des modules individuels ou en ajouter de nouveaux. Vous pouvez modifier ou remplacer des formulaires HTML selon nécessaire.

User Self Care utilise les fonctions de cluster, de distribution, de mise à l'échelle et de configuration fournies par WebSphere. User Self Care utilise également le composant WebSphere Federated Repositories pour rendre les adaptateurs de registre disponibles à l'environnement d'exploitation. Les administrateurs peuvent ajouter ou remplacer des registres.

User Self Care s'intègre à Tivoli Access Manager WebSEAL. WebSEAL fournit une authentification et une autorisation pour les transactions entreprise à client.

L'illustration montre les parties logicielles composant la solution User Self Care.

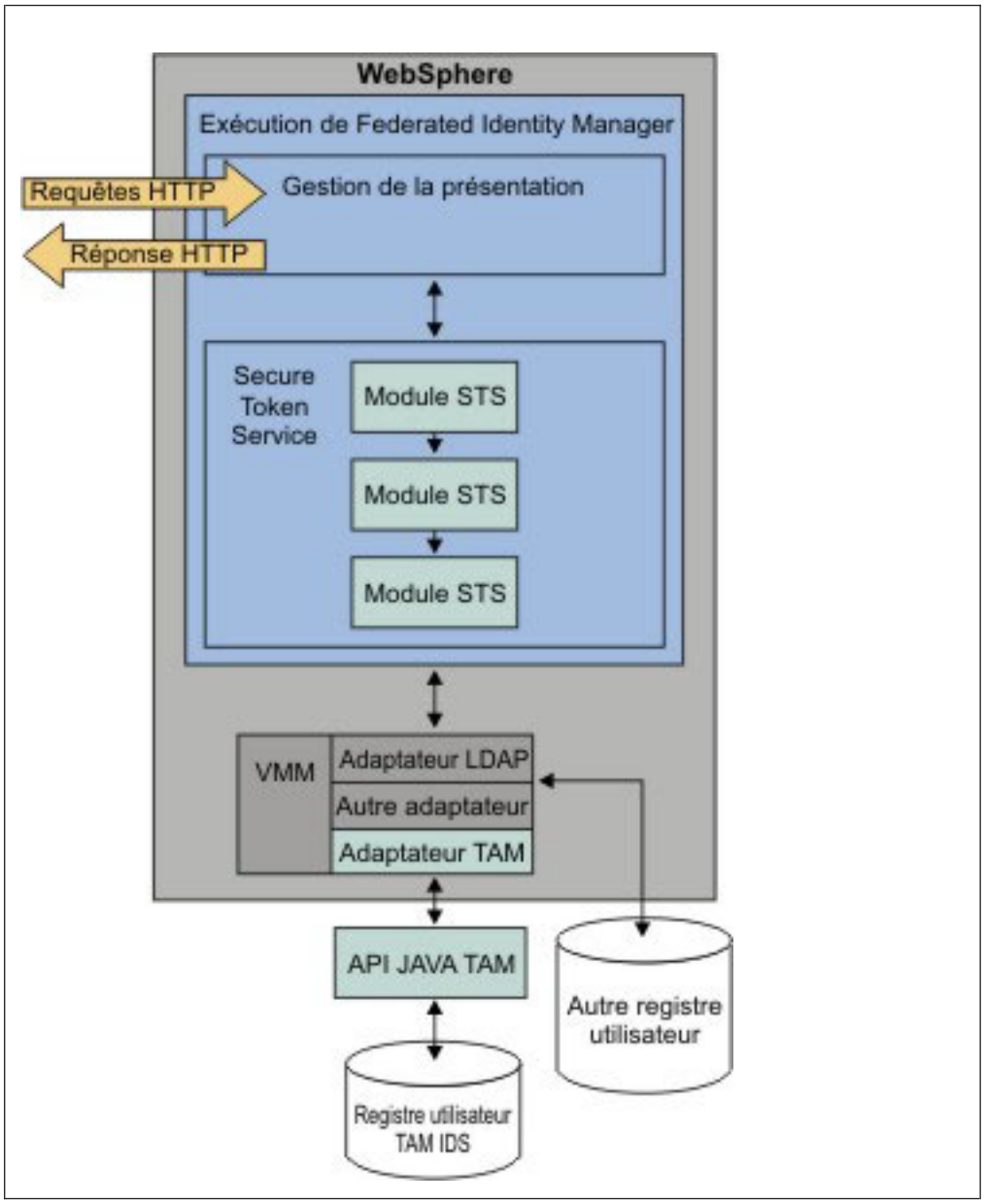


Figure 51. Solution User Self Care

- WebSphere fournit l'infrastructure pour la plupart des parties logicielles.
- L'exécution de Tivoli Federated Identity Manager fournit deux composants qui prennent en charge User Self Care :

  Gestion de la présentation User Self Care
  Fournit un ensemble de pages par défaut. Les utilisateurs interagissent avec ces pages en demandant des URL User Self Care. L'infrastructure de gestion prend en charge la personnalisation et le remplacement de ces pages. Cette prise en charge inclut la capacité à substituer (personnaliser) les macros des pages.

Chaînes d'accréditation STS (Secure Token Service)
Prend en charge la création des chaînes dynamiques des modules de plug-in pour effectuer la logique commerciale. La prise en charge User Self Care inclut un nombre de chaînes STS. Chaque chaîne se mappe sur une opération User Self Care. Vous pouvez étendre ces chaînes. Vous pouvez remplacer ou modifier les modules de composant de chaque chaîne. La validation de l'entrée utilisateur et l'envoi d'un e-mail de confirmation est un exemple d'opération de chaîne User Self Care.

- Les modules STS utilisent WebSphere Federated Repository pour communiquer avec le registre utilisateur. Lorsque le registre utilisateur cible est Tivoli Access Manager, User Self Care utilise un adaptateur Tivoli Access Manager pour communiquer avec le registre Tivoli Access Manager via l'API Tivoli Access Manager Registry Direct Java.

User Self Care fonctionne avec plusieurs registres utilisateur. Chaque registre a une syntaxe unique pour la réalisation des opérations de gestion. Le composant WebSphere Federated Repositories permet à User Self Care d'émettre une commande de gestion, telle que **user create**, à l'aide d'une syntaxe cohérente. Le composant Federated Repositories transmet alors la requête à l'adaptateur de registre approprié, qui traduit la commande en syntaxe spécifique au registre. Etant donné que WebSphere Federated Repositories fournit une interface de plug-in pour les adaptateurs, vous pouvez ajouter de nouveaux registres sans modifier User Self Care.

Personnalisation efficace de User Self Care

Les déploiements de User Self Care sont en général personnalisés selon les besoins spécifiques de la société. Vous pouvez personnaliser votre déploiement de la manière la plus efficace possible seulement si vous comprenez bien comment les différentes parties de User Self Care fonctionnent ensemble.

1. Découvrez la technologie User Self Care.
   - User Self Care est basé sur une série d'opérations. Voir «Découverte des opérations User Self Care», à la page 438.
   - Les utilisateurs interagissent avec les fonctions de User Self Care via des échanges de demandes et réponses HTTP. Les pages HTML en URL dirigent les échanges. Les pages HTML sont des modèles pour les informations que vous souhaitez échanger avec vos utilisateurs. Vous puvez (et devez) personnaliser les pages HTML de sorte à refléter les besoins de votre société. Pour plus d'informations sur les pages HTML par défaut, voir «URL User Self Care», à la page 446.
   - Un grand nombre de sites Internet utilise des tests de réponse Captcha (Completely Automated Public Turing test to tell Computers and Humans Apart) pour se protéger des attaques informatiques. Cette technologie fait partie des nombreux déploiements User Self Care. Le produit User Self Care fournit un module Captcha de démonstration. Voir «Démonstration Captcha» , à la page 450.
2. Déployez Tivoli Federated Identity Manager et configurez User Self Care.

   Ce document présente les étapes de configuration que vous devez faire dans un ordre spécifique. Voir Chapitre 36, «Déploiement de User Self Care», à la page 453.
3. Découvrez les méthodes de réglage des caches distribués pour optimiser les performances. Voir Chapitre 37, «Réglage de User Self Care», à la page 473.

Découverte des opérations User Self Care

Une *opération* User Self Care représente une série d'étapes nécessaires pour qu'un utilisateur accomplisse une tâche, telle que la récupération d'un mot de passe oublié. Pour exécuter cette tâche, l'utiliateur doit procéder aux étapes suivantes :

1. Soumettre un formulaire Web avec son ID utilisateur
2. Soumettre un second formulaire qui l'invite à répondre à sa question secrète et à entrer un nouveau mot de passe
3. Cliquer sur un lien compris dans un e-mail qui lui est envoyé.

La combinaison des étapes forment une *opération*.

Chaque action lancée par un utilisateur effectuée dans le cadre de User Self Care se trouve sous la forme d'une requête HTTP. Par exemple, la demande d'une page, la soumission d'un formulaire ou le clic sur un lien d'un e-mail. Chaque requête HTTP a une réponse HTTP correspondante. Des exemples de réponses fournissent à l'utilisateur le formulaire d'entrée ou bien l'informent de l'envoi d'un e-mail. Chaque opération User Self Care est composée d'un ou plusieurs échanges requête-réponse.

La plupart du temps, chaque échange requête-réponse est un événement atomique. Par exemple, lorsqu'un utilisateur demande la page Gestion des profils, User Self Care termine une opération discrète en renvoyant la page. User Self Care ne conserve pas d'état ni aucun signe indiquant que l'utilisateur a lancé la requête initiale. Il existe des exceptions à ce comportement d'état utilisateur ; elles sont décrites dans les rubriques liées aux opérations individuelles de cette documentation.

Cette documentation regroupe les échanges requête-réponse selon leur association à une opération. Chaque opération est associée à une chaîne d'accréditation de service de jeton sécurisé particulier. Les chaînes d'accréditation STS réalisent la base du travail en traitant une opération User Self Care.

Echange requête-réponse typique

Le flux typique lorsqu'un utilisateur soumet une requête dans User Self Care est le suivant :

1. L'utilisateur demande une URL User Self Care indiquant un formulaire HTML.
2. Le composant de gestion de présentation User Self Care renvoie le formulaire HTML approprié.

   Si le module Captcha est utilisé, la chaîne STS Captcha est démarrée afin d'obtenir l'image affichée à l'utilisateur à des fins de validation.
3. L'utilisateur fournit des données pour le formulaire et procède à la soumission.
4. Le composant de gestion de présentation envoie la requête HTTP qui en résulte à la chaîne d'accréditation STS.
5. Les modules d'accréditation STS User Self Care de la chaîne sont démarrés dans un ordre particulier, pour réaliser des tâches telles que :
   - Validation des données
   - Mappage des attributs
   - Interaction avec les registres
   - Envoi d'e-mail

6. Les modules STS renvoient les résultats de traitement au composant de gestion de présentation.
7. Le composant de gestion de présentation renvoie une réponse HTTP à l'utilisateur. La réponse est en général l'une des suivantes :
   - Un autre formulaire
   - Le même formulaire avec un message
   - Une page d'erreur
   - Une page d'informations

   Selon l'opération, la tâche de l'utilisateur est finie ou bien elle nécessite un autre étape. Si une autre étape est nécessaire, la séquence précédente ou identique est répétée.

Opérations et chaînes STS

Chaque opération de User Self Care se mappe à une chaîne STS unique. Lors de l'opération, la chaîne STS peut être démarrée plusieurs fois. User Self Care détermine la phase de l'opération en cours et contrôle le comportement en conséquence.

Par exemple, la validation Captcha peut être réalisée lorsqu'un utilisateur soumet le formulaire d'inscription initial. Toutefois, elle n'est pas réalisée lorsque l'utilisateur clique sur le lien de l'e-mail. Dans les deux cas, la même chaîne STS est démarrée et le module STS Captcha est présent au début de la chaîne. Dans le second cas, le module Captcha n'est pas censé effectuer d'action et transmet la requête au module STS suivant dans la chaîne.

Vous pouvez utiliser la console d'administration pour afficher chaque chaîne d'accréditation. Les chaînes d'accréditation correspondent à une ou plusieurs opérations User Self Care. Lorsque vous affichez les chaînes d'accréditation, vous voyez les modules STS accomplissant l'opération. Vous pouvez alors personnaliser les modules et chaînes pour votre déploiement.

Remarque : Pour des informations sur la personnalisation de User Self Care, voir le Wiki Tivoli Federated Identity Manager :

http://www.ibm.com/developerworks/wikis/display/tivolifederatedidentitymanager/Home

Opération de vérification d'existence d'ID utilisateur

A la plage d'inscription initiale, l'utilisateur entre un ID utilisateur dans une zone spécifique. User Self Care fournit une icône sur laquelle l'utilisateur peut cliquer si l'ID existe dans le registre. L'opération d'existence d'ID utilisateur est une exception à la règle d'unicité de chaîne STS par opération. Cette opération se mappe sur la même chaîne d'accréditation STS en opération d'inscription. Toutefois, elle est conceptuellement différente et elle utilise une URL différente.

Flot de tâches d'opération :

1. L'utilisateur entre son ID utilisateur demandé dans une zone de formulaire.
2. L'utilisateur clique sur l'icône.
3. La chaîne STS de création de compte démarre.
   - Le registre est interrogé pour déterminer si l'ID utilisateur existe.
   - Le cache interne est également interrogé.

La vérification du cache interne est décrite à la rubrique «Opération d'inscription».

Opération d'inscription

L'opération d'inscription prend place en deux échanges requêtes-réponses :

1. Obtention des informations utilisateur en préparation pour l'envoi d'un message électronique de validation.
2. L'utilisateur valide l'opération en cliquant sur une lien dans le message électronique.

Demande d'inscription initiale

Flot de tâches d'opération :

1. L'utilisateur demande et reçoit un formulaire de demande d'inscription. L'utilisateur renseigne les zones du formulaire avec des détails d'inscription comme :
   - ID utilisateur
   - Adresse électronique
   - Mot de passe
   - Choix d'attribut de profil, y compris l'attribut de question secrète.
2. L'utilisateur soumet le formulaire de demande d'inscription.
3. La chaîne STS de création de compte démarre.
   - Si des erreurs surviennent, elles sont renvoyées à l'utilisateur. Les erreurs s'affichent en tant que message du formulaire que l'utilisateur a traité.
   - Si aucune erreur ne se produit, un message électronique est envoyé à l'utilisateur pour validation. User Self Care affiche une page à l'utilisateur, l'informant du message électronique.
4. Une entrée est créée dans un cache interne qui conserve les informations d'inscription de l'utilisateur lors de la validation. Ce cache interne conserve également l'ID utilisateur de sorte qu'aucun autre utilisateur ne puisse l'utiliser pour l'inscription. Vous pouvez configurer les limites de temps concernant la période pendant laquelle les données sont conservées dans le cache interne.

Validation de l'inscription

Le message électronique envoyé lors de la demande d'inscription initiale contient un lien auquel s'ajoute une chaîne de requête. La chaîne de requête contient une clé dans l'entrée de cache interne pour que les données soumises initialement par l'utilisateur puissent être récupérées et que l'inscription se finalise.

Flot de tâches :

1. L'utilisateur clique sur un lien du message électronique de validation.
2. La chaîne STS de création de compte démarre.
3. Si des erreurs se produisent, elles s'affichent dans une page envoyée à l'utilisateur. Si aucune erreur ne se produit, User Self Care :
   a. Crée une entrée dans le registre pour le nouveau compte utilisateur
   b. Supprime l'entrée de cache interne
   c. Envoie un message indiquant une réussite à l'utilisateur.

Opérations de gestion du mot de passe

Il existe deux opérations de gestion du mot de passe :

- Une modification du mot de passe lancée par l'utilisateur
- Une modification du mot de passe requise après expiration du mot de passe existant

Modification du mot de passe lancée par l'utilisateur

Flot de tâches :

1. L'utilisateur demande l'URL de formulaire Modifier le mot de passe.
2. User Self Care fournit à l'utilisateur un formulaire dans lequel il entre son ancien mot de passe, puis il entre deux fois son nouveau mot de passe.
3. L'utilisateur soumet le formulaire dans l'URL Modifier le mot de passe.
4. User Self Care démarre la chaîne STS Modifier le mot de passe.
   - En cas d'erreur, User Self Care envoie à l'utilisateur une page d'informations contenant lesdites erreurs.
   - Si aucune erreur ne se produit, le mot de passe est modifié.User Self Care envoie alors à l'utilisateur une page indiquant la réussite de l'opération.

Modification du mot de passe après son expiration

Le flux de tâches est identique que celui de la rubrique de modification de mot de passe lancée par l'utilisateur, sauf :

- L'utilisateur fait une requête initiale pour une ressource protégée
- Le serveur point de contact demande à l'utilisateur de modifier son mot de passe.

La requête initiale de l'utilisateur est interceptée par le serveur point de contact d'authentification, tel que WebSEAL ou WebSphere Application Server. Le serveur point de contact gère le flux de communications et doit diriger l'utilisateur vers User Self Care de sorte qu'il modifie son mot de passe. User Self Care indique des suggestions et améliorations de déploiement pour ce faire à l'aide de WebSEAL en serveur point de contact. Pour plus d'informations, voir «Intégration de User Self Care à WebSEAL», à la page 467.

User Self Care peut fonctionner en tant que composant à appeler pour une fonction telle que Tivoli Access Manager Local Response Redirect. Cette fonction redirige l'utilisateur vers le gestionnaire de User Self Care pour réaliser une opération de modification de mot de passe. L'utilisateur est alors redirigé à la fin de l'opération.

Opérations de gestion de profil

La gestion des profils permet à un utilisateur de gérer les informations étendues spécifiques à son compte. Voici des exemples de ces informations :

- Adresse
- Numéro de téléphone
- Question secrète

Requête de gestion des profils initiale

Flot de tâches :

1. L'utilisateur soumet des requêtes pour l'URL de formulaire de gestion des profils. Cette adresse URL doit être une ressource protégée.
2. L'identité de l'utilisateur est obtenue à partir du contexte authentifié
3. User Self Care démarre la chaîne STS de gestion des profils et fournit l'identité de l'utilisateur.
   - Si des erreurs se produisent, elles s'affichent dans une page d'informations envoyée à l'utilisateur.
   - Si aucune erreur ne se produit, le module STS extrait les attributs à partir du registre.
4. User Self Care présente à l'utilisateur le formulaire de gestion des profils contenant ses attributs existants. L'utilisateur peut alors mettre à jour les informations de profil, y compris sa question secrète.

Soumission de la mise à jour de profil

Flot de tâches :

1. L'utilisateur modifie les zones de son choix et soumet la forme.
2. L'identité de l'utilisateur est obtenue à partir du contexte authentifié.
3. User Self Care démarre la chaîne STS de gestion des profils.
   - Si des erreurs se produisent, elles s'affichent dans une page d'informations envoyée à l'utilisateur.
   - Si aucune erreur ne se produit, le registre est mis à jour.User Self Care envoie une page indiquant une réussite à l'utilisateur.

Opération d'ID utilisateur oublié

Flot de tâches d'opération :

1. L'utilisateur clique sur l'URL ID oublié. Cette URL ne doit pas être une ressource protégée.
2. Le formulaire d'ID oublié est renvoyé à l'utilisateur.
3. L'utilisateur entre son adresse e-mail.

   Une solution personnalisée peut utiliser un attribut de registre différent, tel qu'un numéro de compte client, par exemple. Le formulaire User Self Care par défaut utilise l'adresse e-mail.
4. L'utilisateur soumet le formulaire.
5. User Self Care transmet le contenu du formulaire à la chaîne STS ID oublié. Les modules de cette chaîne extraient du registre tous les ID utilisateur associés à l'adresse e-mail, et les envoie par messagerie électronique à l'utilisateur.
   - Si des erreurs se produisent, elles s'affichent dans une page d'informations envoyée à l'utilisateur.
   - Si aucune erreur ne se produit, User Self Care envoie la page d'informations d'accusé de l'ID oublié à l'utilisateur. La page informe l'utilisateur que les ID utilisateur ont été envoyés à son adresse e-mail.

Opération de mot de passe oublié

L'opération liée au mot de passe oublié a lieu dans le cadre de plusieurs échanges questions-réponses.

Flot de tâches :

1. L'utilisateur demande l'URL de mot de passe oublié. Cette URL ne doit pas être une ressource protégée
2. User Self Care envoie le formulaire de mot de passe oublié à l'utilisateur.
3. L'utilisateur envoie son ID utilisateut et soumet le formulaire.
4. User Self Care transmet le contenu du formulaire à la chaîne STS ID oubliée de sorte à extraire la question secrète.
5. Le module STS envoie le formulaire de question secrète du mot de passe oublié à l'utilisateur. Le formulaire contient une question secrète et une zone dans laquelle l'utilisateur doit entrer la réponse. Le formulaire fournit également deux zones de capture du nouveau mot de passe.
6. L'utilisateur édite et soumet le formulaire Question secrète.
7. User Self Care transmet le contenu du formulaire à la chaîne STS ID oublié de sorte à procéder à la validation de la question secrète.
   a. Le module STS assure le suivi des tentatives infructueuses dans un cache interne. Si le nombre dépasse la limite configurée, le module STS envoie une erreur à l'utilisateur.
   b. Le module STS stocke la demande de modification de mot de passe dans un cache interne.
   c. Le module STS envoie à l'utilisateur un e-mail contenant un lien vers l'URL de formulaire de validation de mot de passe oublié. L'e-mail contient un lien auquel s'ajoute une chaîne de requête. La chaîne de requête contient une clé vers l'entrée de cache interne. La clé est utilisée de sorte que l'utilisateur soumis puisse être récupéré et la modification du mot de passe achevée.
8. L'utilisateur demande le lien dans l'e-mail.
9. User Self Care transmet la requête à la chaîne STS ID oublié. Les modules de chaînes récupèrent les données à partir du cache interne et tentent de modifier le mot de passe.
   - Si des erreurs se produisent, elles s'affichent dans une page d'informations envoyée à l'utilisateur.
   - Si aucune erreur ne survient, User Self Care envoie à l'utilisateur la page d'informations d'accusé de mot de passe oublié. Cette page lui indique que le mot de passe a été modifié.

Opération de suppression de compte

Flot de tâches d'opération :

- L'utilisateur demande la page de suppression de compte. Cette page doit être une ressource protégée.
- L'utilisateur clique sur un lien de la page.
- L'identité de l'utilisateur est obtenue à partir du contexte authentifié.
- La chaîne STS de suppression de compte est démarrée.
- La chaîne STS de suppression de compte finalise la suppression du compte utilisateur.
- User Self Care renvoie à l'utilisateur la page d'informations de réussite de suppression de compte.

Opération Captcha

Captcha ne représente pas une opération User Self Care distincte. En effet, l'opération Captcha est implémentée en tant que module STS Captcha. Vous pouvez placer le module d'abord dans des chaînes d'accréditation de service de jeton sécurisé utilisées par User Self Care. Lorsque le module Captcha est présent, la validation Captcha est effectuée avant l'exécution de toute autre opération.

Pour plus d'informations, voir «Démonstration Captcha», à la page 450.

Opérations d'attributs de registre

User Self Care ne donne pas la possibilité de modifier le schéma de registre utilisateur. Vous devez modifier votre schéma de registre selon nécessaire pour créer les attributs de registre requis pour la prise en charge de vos profils. Vous devez également modifier le schéma pour prendre en charge l'attribut *question secrète*.

User Self Care fournit un exemple de fonction. User Self Care utilise l'attribut LDAP `businessCategory` pour stocker l'attribut de profil de question secrète. L'exemple d'implémentation utilise également l'attribut LDAP `mobile` pour stocker un numéro de téléphone portable pour l'utilisateur.

Lorsque vous déployez User Self Care, vous devez créer un schéma qui peut contenir les attributs de profil que vous devez fourni à vos utilisateurs. Dès que vous avez identifié et défini ces attributs, vous pouvez personnaliser les formulaires HTML et modules STS de sorte à les utiliser.

Dans le cadre d'un déploiement complet, il est nécessaire de créer un schéma qui peut contenir les attributs de profil que vous devez fourni à vos utilisateurs. Lorsque ces attributs sont sélectionnés, vous devez personnaliser les formulaires HTML et les modules STS afin d'utiliser les nouveaux attributs.

Pour plus d'informations, voir le Wiki Tivoli Federated Identity Manager :

http://www.ibm.com/developerworks/wikis%2Fdisplay%2Ftivolifederatedidentitymanager%2Fhome.

Opération relative à la question secrète

La *question secrète* représente un mot de passe et un conseil secondaires stockés dans le registre utilisateur en attribut utilisateur. User Self Care considère la gestion de la question secrète comme un autre élément de profil.

User Self Care fournit un exemple d'implémentation de la question secrète question en utilisant l'attribut LDAP businessCategory pour stocker le profil de question secrète. Vous pouvez personnaliser cette implémentation de sorte qu'elle corresponde au mieux à vos besoins.

Les rubriques suivantes décrivent le fonctionnement de l'exemple d'implémentation.

Sélection de question secrète durant l'inscription

Un formulaire d'inscription User Self Care fournit un menu qui permet à un utilisateur de sélectionner une des questions suivantes :

- Nom de jeune fille de la mère
- Lieu de naissance
- Nom du premier animal animal domestique

La sélection d'un ou plusieurs éléments renseigne une zone de formulaire avec des valeurs numériques correspondant à l'index de l'entrée dans la liste. Le nom de cette zone sur les formulaires HTML fourni avec User Self Care est `usc.form.profile.secret.question`.

Une zone de formulaire distinct est utilisé pour spécifier la réponse à la question du texte. Le nom de cet attribut sur les formulaires HTML fourni avec User Self Care est `usc.form.profile.secret.question.answer`.

Lorsque l'utilisateur soumet le formulaire d'inscription, chacun de ces paramètres est transmis à la chaîne d'accréditation STS d'inscription. L'index et la réponse sont concaténés ensemble et stockés dans l'attribut LDAP `businessCategory`.

Affichage de la question secrète durant la gestion des profils

Lorsque l'utilisateur demande le formulaire de gestion des profils, User Self Care extrait les attributs, y compris la question secrète, à partir du registre. Le module STS de gestion des profils analyse l'attribut et détermine l'index spécifiant la question secrète que l'utilisateur a précédemment sélectionnée. User Self Care utilise alors cette valeur d'index pour afficher la valeur appropriée du menu du formulaire de gestion des profils.

Utilisation de la question secrète pour valider l'identité utilisateur

Lorsque l'utilisateur soumet le formulaire de mot de passe oublié, User Self Care utilise l'ID utilisateur pour extraire l'attribut de registre `businessCategory`. Le module STS Mot de passe oublié analyse alors la valeur de l'attribut et renvoie l'index au composant de gestion de présentation. Ce composant utilise l'index pour effectuer une substitution de macro. La substitution fournit une valeur à JavaScript qui mène la sélection de la question secrète correspondante.

Astuce d'implémentation de question secrète

La sécurité de l'approche de la question secrète est améliorée si les utilisateurs peuvent créer leur propre question secrète. Une liste de menu peut s'avérer pratique, mais il existe un risque de fournir des informations d'identification. Les informations sont souvent réutilisées sur plusieurs sites Internet.

Les valeurs par défaut fournies par User Self Care servent d'exemples uniquement. Elles incluent les valeurs souvent utilisées, telles que le nom de jeune fille de la mère, le couleur préférée et le nom du premier animal domestique. Il est recommandé de ne pas utiliser ces valeurs dans un déploiement d'entreprise.

URL User Self Care

User Self Care fournit un ensemble de pages HTML par défaut pour communiquer avec l'utilisateur. Les pages HTML facilitent l'échange de demandes HTTP et réponses.

Requêtes HTTP User Self Care

La table suivante répertorie les URL demandées par les utilisateurs lors de leur interaction avec User Self Care. Certaines URL sont présentées pour plusieurs requêtes. Chaque URL est unique à une opération User Self Care et est mappée à une chaîne STS. User Self Care détermine la phase de l'opération effectuée en examinant le contenu de la requête.

Remarque : L'authentification utilisateur est requise pour certaines URL. Si la description ne mentionne pas d'authentification utilisateur, cette dernière n'est pas nécessaire.

Tableau 123. Requêtes HTTP

Nom	Méthode HTTP	URI et description de la requête
Page principale	GET	Page personnalisée facultative non hébergée par User Self Care. Vous pouvez décider de créer une page contenant des liens vers les opérations User Self Care, mais qui n'est pas hébergée par User Self Care.
Formulaire de demande d'inscription	GET	/sps/*federation_name*/usc/self/account/create Demande le formulaire d'inscription.
Soumettre la demande d'inscription	POST	/sps/*federation_name*/usc/self/account/create Soumet le formulaire d'inscription.
Extraire l'ID utilisateur	POST	/sps/*federation_name*/usc/global/userid/search Se mappe sur une opération User Self Care distincte qui détermine si un ID utilisateur existe. Cette page apparaît une fois que vous avez cliqué sur un lien du formulaire de demande d'inscription.
Validation de l'inscription	POST	/sps/*federation_name*/usc/self/account/create/validate Indique l'URL de base dans l'e-mail envoyé à l'utilisateur durant la validation de l'inscription. Une chaîne de requête est ajoutée à l'URL finale.
Formulaire Modifier le mot de passe	GET	/sps/*federation_name*/usc/self/password/update Authentification requise Demande le formulaire de modification du mot de passe.
Soumettre la modification du mot de passe	POST	/sps/*federation_name*/usc/self/password/update Authentification requise Soumet le formulaire de modification du mot de passe.
Formulaire ID oublié	GET	/sps/*federation_name*/usc/self/account/recover/userid Demande le formulaire d'ID oublié.
Soumettre ID oublié	POST	/sps/*federation_name*/usc/self/account/recover/userid Soumet le formulaire d'ID oublié.
Formulaire Mot de passe oublié	GET	/sps/*federation_name*/usc/self/account/recover/password Demande le formulaire de mot de passe oublié.

Tableau 123. Requêtes HTTP (suite)

Nom	Méthode HTTP	URI et description de la requête
Formulaire Mot de passe oublié	POST	/sps/*federation_name*/usc/self/account/recover/password Soumet le formulaire de mot de passe oublié.
Formulaire de question secrète du mot de passe oublié	POST	/sps/*federation_name*/usc/self/account/recover/password/secretquestion Soumet le formulaire de validation de la question secrète. Ce formulaire est présenté à l'utilisateur après soumission du formulaire de mot de passe oublié.
Formulaire de validation du mot de passe oublié	POST	/sps/*federation_name*/usc/self/account/recover/password/validate Indique l'URL de base dans l'e-mail envoyé à l'utilisateur durant la validation du mot de passe oublié. Une chaîne de requête est ajoutée à l'URL finale.
Formulaire de mise à jour de profil	GET	/sps/*federation_name*/usc/self/profile/update Authentification requise Demande le formulaire de mise à jour de profil.
Soumettre la mise à jour du profil	POST	/sps/*federation_name*/usc/self/profile/update Authentification requise Soumet le formulaire de mise à jour de profil.
Formulaire Suppression de compte	GET	/sps/*federation_name*/usc/self/account/delete Authentification requise Demande le formulaire de suppression de compte.
Soumettre la suppression de compte	POST	/sps/*federation_name*/usc/self/account/delete Authentification requise Soumet le formulaire de suppression de compte.

Réponses HTTP User Self Care

Cette rubrique répertorie l'ensemble de pages que User Self Care présente à l'utilisateur. Cet ensemble entre dans les catégories suivantes :

Info
Page d'informations présentant des instructions, des erreurs ou une indication de réussite.

Formulaire
Un formulaire HTML dans lequel l'utilisateur entre des données.

Réacheminement
Un réacheminement HTTP.

Tableau 124. Réponses HTTP

Nom	Type	Description
Formulaire de demande d'inscription	Formulaire	Rassemble les informations suivantes : • ID utilisateur requis • Adresse électronique • Mot de passe • Confirmation du mot de passe • Attributs du profil • Entrée Captcha (facultatif)
Validation de l'inscription	Formulaire	Informe l'utilisateur qu'un e-mail a été envoyé à des fins de validation ou qu'une erreur est survenue.
Résultat de l'inscription	Info	Informe l'utilisateur que son compte a été créé ou qu'une erreur est survenue.
Modifier le mot de passe	Formulaire	Rassemble les informations suivantes : • Ancien mot de passe • Nouveau mot de passe • Confirmation du nouveau mot de passe
Résultat de modification du mot de passe	Info	Informe l'utilisateur que son mot de passe a été modifié ou qu'une erreur est survenue.
ID oublié	Formulaire	Rassemble les éléments suivants pour aider à utilisateur à récupérer un ID utilisateur oublié : • Adresse électronique • Entrée Captcha. Cette valeur est facultative.
Mot de passe oublié	Formulaire	Rassemble les informations suivantes : • ID utilisateur • Entrée Captcha Cette valeur est facultative.
Question secrète du mot de passe oublié	Formulaire	Affiche la question secrète. Rassemble les informations suivantes : • Réponse à la question secrète • Nouveau mot de passe • Confirmation du nouveau mot de passe • Entrée Captcha Cette valeur est facultative.
Post ID oublié	Info	Présente une erreur ou une indication de réussite après une tentative de récupération d'un ID oublié.
Mettre à jour le profil	Formulaire	Présente à l'utilisateur ses détails de profil actuels et rassemble les modifications dans les zones.
Post gestion des profils	Info	Présente une erreur ou une indication de réussite après des opérations de gestion des profils.
Suppression de compte	Formulaire	Présente une icône que l'utilisateur peut utiliser pour supprimer son compte.
Post suppression de compte	Info	Présente une erreur ou une indication de réussite après une suppression de compte

Validation de contenu du formulaire

Considérez l'utilisation d'une validation d'entrée côté client pour vérifier que les zones du formulaire contiennent les données appropriées pour leur type. Les pages HTML de User Self Care contiennent plusieurs exemples.

Démonstration Captcha

Le module STS de démonstration Captcha fournit un exemple d'intégration de Captcha à User Self Care.

User Self Care fournit des pages HTML qui prend en charge les opérations User Self Care. Plusieurs de ces pages sont bonnes pour le type de validation d'entrée fournie par Captcha. Vous pouvez configurer ces pages pour inclure une macro pour Captcha. L'application User Self Care peut remplacer la valeur de la macro par la source HTML nécessaire de sorte à prendre en charge la démonstration Captcha. Lorsque Captcha n'est pas configuré, la macro n'est pas substituée et les éléments Captcha ne s'affichent pas sur la page.

Lorsqu'un utilisateur demande initialement une page contenant un challenge Captcha, le module STS Captcha est contacté. Le module sélectionne de manière aléatoire une image de l'ensemble des images configurées. Cette image construit la macro sur la page HTML affichée à l'utilisateur.

Après la substitution de la macro, une bloc de code tel que l'exemple ci-dessous s'affiche sur la page.

```
<label for="demo_captcha">
Veuillez entrer le ou les mots de vérification affichés ci-dessous (obligatoire)
            </label>
<br />
<img src="http://myserver/public/captcha_test/hello.jpg" border="0" />
<br />
<input type="hidden"
       name="usc.demo.captcha.challenge.field"
       id="usc.demo.captcha.challenge.field"
       value="http://myserver/public/captcha_test/hello.jpg" />
<input style="background-color:#F8F8C8;"
       type="text"
       name="usc.demo.captcha.response.field"
       id="usc.demo.captcha.response.field" />
```

Figure 52. Exemple Captcha

Ce bloc fournit une balise `src` et deux zones d'entrée. La balise `src` affiche l'image à l'utiliateur. La première zone d'entrée fournit le nom de l'image. La seconde rassemble l'entrée utilisateur, à savoir le texte situé dans l'image.

Lorsque le formulaire est soumis, les deux zones d'entrée sont fournies dans le module STS Captcha de démonstration. Ce module compare la réponse de l'utilisateur avec la chaîne associée à cet image. Si une correspondance est correcte, la validation est terminée.

Remarque : La première zone d'entrée spécifie une valeur qui est l'URL d'un serveur hébergeant les images s'affichant à l'utilisateur.

Le module de démonstration Captcha est situé dans le répertoire :
Federated_Identity_Manager_installation_directory/examples/demo/captcha

Ce répertoire contient :

- Un fichier readme
- Un fichier com.tivoli.am.fim.demo.sts.captcha.jar contenant à la fois le code compilé et le code source pour le module de démonstration STS Captcha.
- Un répertoire captchaTestImages contenant :
  - Un ensemble de six images JPEG
  - Un fichier DemoCaptchaImagesInfo.txt qui affiche le mappage entre les noms de fichiers d'images et la chaîne de texte que l'utilisateur doit entrer lorsqu'il voir l'image associée.

Pour des instructions concernant la configuration, voir «Configuration de la démonstration Captcha», à la page 464.

Chapitre 36. Déploiement de User Self Care

Tivoli Federated Identity Manager installe automatiquement User Self Care dans le cadre de l'exécution. Vous n'avez pas besoin d'installer d'autres logiciels, à moins que vous ne comptiez utiliser Tivoli Access Manager en registre utilisateur cible.

Les administrations qui souhaitent déployer User Self doivent maîtriser la gestion de :

- WebSphere Application Server, y compris l'interface d'administration **wsadmin**.
- Les modules STS Tivoli Federated Identity Manager et chaînes d'accréditation.
- Tivoli Directory Server LDAP.

Les administrations qui souhaitent utiliser Tivoli Access Manager en registre utilisateur cible ou WebSEAL en serveur point de contact doivent maîtriser l'administration de Tivoli Access Manager for e-business.

La liste suivante récapitule les tâches de déploiement de User Self Care et l'ordre dans lequel les effectuer. Avant de commencer une tâche, vérifiez que vous avez procédé aux tâches préalables requises.

1. Configurez un domaine Tivoli Federated Identity Manager. Les étapes de configuration incluent la configuration de la gestion de l'exécution.

   Les étapes de cette tâche sont identiques pour tous les scénarios Tivoli Federated Identity Manager. Aucune tâche de cette rubrique n'est unique à User Self Care. Les liens associés aux tâches vous transfèrent vers les rubriques des tâches courantes du guide de configuration de *Tivoli Federated Identity Manager.*

   «Configuration d'un domaine Tivoli Federated Identity Manager», à la page 454
2. Intégrez User Self Care au registre utilisateur pour votre déploiement. User Self Care prend en charge les registres Tivoli Directory Server et Tivoli Access Manager. Vous êtes dirigé vers les instructions correspondant au type de votre registre.

   «Configuration d'un registre utilisateur», à la page 454
3. La configuration User Self Care est basée sur des valeurs obtenues d'un fichier de réponse. Dans cette tâche, vous renseignez un fichier de réponses avec des valeurs applicables à votre déploiement.

   «Configuration d'un fichier de réponses», à la page 461
4. Vous utilisez le fichier de réponses créé lors de la tâche précédente pour configurer votre déploiement User Self Care. Cette étape décrit comment afficher les chaînes d'accréditation préconfigurées à partir de l'interface d'administration. Cette étape décrit également comment utiliser l'interface de ligne de commande Tivoli Federated Identity Manager pour déployer votre environnement User Self Care. Eventuellement, vous pouvez configurer la démonstration Captcha.

   «Configuration de User Self Care», à la page 463
5. Lorsque votre déploiement inclut le serveur WebSEAL Tivoli Access Manager en serveur point de contact, vous devez intégrer des fonctions User Self Care à WebSEAL. Cet ensemble de tâches vous explique comment procéder à l'intégration.

   «Intégration de User Self Care à WebSEAL», à la page 467

Configuration d'un domaine Tivoli Federated Identity Manager

Vous devez configurer un domaine Tivoli Federated Identity Manager.

Avant de commencer

Installez les composants Tivoli Federated Identity Manager suivants :

- Gestion de l'environnement d'exécution
- Console d'administration

Procédure

1. Connectez-vous à la console d'administration.
2. Créez un domaine. Pour plus d'informations, voir Chapitre 1, «Configuration de domaine», à la page 3.

Que faire ensuite

Poursuivez avec la rubrique «Configuration d'un registre utilisateur».

Configuration d'un registre utilisateur

Intégrez User Self Care au registre utilisateur défini pour votre déploiement.

User Self Care prend en charge ces registres via la configuration de WebSphere Federated Repositories :

- IBM Tivoli Directory Server. Voir «Configuration de Tivoli Directory Server».
- IBM Tivoli Access Manager. Voir «Configuration d'un adaptateur Tivoli Access Manager», à la page 455.
- Microsoft Active Directory. Voir «Configuration d'un serveur Active Directory», à la page 460.

Configuration de Tivoli Directory Server

Configurez WebSphere Federated Repository pour Tivoli Directory Server LDAP.

Pourquoi et quand exécuter cette tâche

N'utilisez pas cette tâche si vous utilisez Tivoli Access Manager en registre utilisateur. Voir «Configuration d'un adaptateur Tivoli Access Manager», à la page 455.

Procédure

1. Connectez-vous à la console d'administration.
2. Sélectionnez l'onglet Sécurité, puis sélectionnez **Sécurité globale**.
3. Cliquez sur **Configurer**.
   L'icône est située à la droite du menu des référentiels fédérés.
4. Cliquez sur l'option d'**ajout d'une entrée de base au domaine**.
5. Cliquez sur **Ajouter le référentiel**.
6. Entrez un nom d'**identificateur de référentiel**
   Vous pouvez indiquer un nom d'identificateur.
7. Entrez les valeurs dans les zones suivantes :

- **Type de répertoire**
- **Nom d'hôte principal**
- **Port**
- **Nom distinctif Bind**
- **Mot de passe Bind**

Vous pouvez fournir en option des valeurs pour les zones supplémentaires.

8. Cliquez sur **OK** et sauvegardez. Vous pouvez maintenant voir une page qui demande le **nom distinctif d'une entrée de base qui identifie de manière unique cet ensemble d'entrées dans le domaine**.
9. Entrez un nom d'entrée de base. Cliquez sur **OK** et sauvegardez.

   Si nécessaire, voir la documentation WebSphere Application Server relative à WebSphere Federated Repository.

   Remarque : Mémorisez le nom de l'entrée de base. Vous devez l'utiliser lors de la configuration de User Self Care.
   La page de configuration pour **defaultWIMFileBasedRealm** s'affiche.
10. Examinez la table intitulée **Référentiels du domaine**. Vérifiez que le nouveau domaine s'affiche, et que l'**entrée de base** est définie sur la valeur que vous entrez. Cliquez sur **OK** et sauvegardez. La console d'administration revient à la page **Sécurité globale**.
11. Cochez la case d'**activation de la sécurité d'application**.
12. Cliquez sur **OK** et sauvegardez.

Que faire ensuite

Passez à la section «Configuration d'un fichier de réponses», à la page 461.

Configuration d'un adaptateur Tivoli Access Manager pour WebSphere Federated Repository

Pour configurer un adaptateur Tivoli Access Manager pour User Self Care, vous devez configurer l'adaptateur et l'ajouter à WebSphere Federated Repository en registre personnalisé.

Exécutez les tâches suivantes :

1. «Configuration d'un adaptateur Tivoli Access Manager».
2. «Configuration d'un adaptateur en registre personnalisé WebSphere Application Server», à la page 457.

Si nécessaire, consultez les informations de dépannage dans «Identification et résolution des incidents de connexion à WebSphere Application Server», à la page 459.

Configuration d'un adaptateur Tivoli Access Manager

Configurez cet adaptateur lorsque User Self Care gère le registre Tivoli Access Manager.

Pourquoi et quand exécuter cette tâche

Cet adaptateur utilise l'API Tivoli Access Manager Registry Direct Java API pour effectuer des commandes d'administration telles que la création d'utilisateurs et de groupes. L'installation de Tivoli Access Manager fournit cet adaptateur.

Remarque : Si vous n'utilisez pas d'adaptateur Tivoli Access Manager, ne prenez pas ces instructions en compte. Voir «Configuration de Tivoli Directory Server», à la page 454.

Procédure

1. Vérifiez que vous avez installé Tivoli Access Manager.
2. Vérifiez que vous avez installé et configuré Tivoli Access Manager à l'aide de Tivoli Directory Server en registre utilisateur.
3. Vérifiez que vous avez installé le composant d'exécution Tivoli Access Manager 6.1.1 Java.
4. Copiez *TAM_installation_directory*/java/export/rgy/com.tivoli.pd.rgy.jar dans *WebSphere_installation_directory*/lib.
5. Créez une identité utilisateur Tivoli Access Manager exécutant l'API Java.

   Par exemple :

   ```
   pdadmin -a sec_master -p sec_master_password
   pdadmin sec_master> user create -no-password-policy user_name
   cn=user_name,registry_suffix user_name user_name password
   ( SecurityGroup ivacld-servers remote-acl-users )
   pdadmin sec_master> user modify user_name account-valid yes
   ```

   Dans cet exemple, *user_name* est le nom que vous avez choisi pour l'utilisateur. Il est recommandé d'utiliser les conventions de dénomination suivantes :

   ```
   tamVMMAdapter-machine_name
   ```

   La valeur *registry_suffix* est le suffixe du registre où l'utilisateur doit être stocké. Par exemple :

   ```
   o=ibm,c=us
   ```

6. Accédez à l'ordinateur sur lequel l'adaptateur Tivoli Access Manager doit être configuré. Modifiez le répertoire sur *WebSphere_installation_directory*/lib . Exécutez l'outil **com.tivoli.pd.rgy.until.RgyConfig**.

   Utilisez l'environnement d'exécution IBM Java pour exécuter cet outil. Par exemple :

   ```
   <WebSphere install>/AppServer/java/jre/bin/java
   ```

Tableau 125. Utilisation de l'utilitaire com.tivoli.pd.rgy.util.RgyConfig

Syntaxe :

```
java com.tivoli.pd.rgy.util.RgyConfig properties_file_destination create Default
Default "ldaphostname:389:readwrite:5" "DN" DN_password
```

properties_file_destination
Spécifie le chemin complet vers un répertoire existant et le nom d'un fichier créé à l'exécution de cette commande. Placez le fichier dans un répertoire correspondant à votre déploiement WebSphere Application Server :

- Pour un serveur WebSphere Application Server qui n'est pas en cluster :

  WebSphere_application_server/profiles/*server_name*/config/itfim

- Pour un environnement WebSphere Application Server en cluster (répliqué), créez le fichier sur le DMgr :

  WebSphere_application_server/profiles/*DMgr_server_name*/config/itfim

ldaphostname
Le nom d'hôte du serveur LDAP sur lequel Tivoli Access Manager est configuré. Le nom d'hôte est spécifié dans le fichier de configuration d'exécution Tivoli Access Manager :

Tivoli Access Manager_installation_directory/etc/ldap.conf

389
Le port LDAP par défaut. A modifier selon nécessaire pour votre déploiement.

"DN"
Le nom distinctif (DN) spécifié dans la commande de création d'utilisateur **pdadmin**. Vérifiez que la valeur est entourée de guillemets simples.

DN_password
Le mot de passe pour le nom DN.

Exemple de commande :

```
java com.tivoli.pd.rgy.util.RgyConfig
WebSphere_application/profiles/<server>/config/itfim/tamVMMAdapter.properties
 create Default Default "myldapsystem:389:readwrite:5"
"cn=tamVMMAdapter-myhost,o=ibm,c=us" mypasswordmypassword
```

7. Mettez à jour la configuration selon nécessaire pour votre déploiement WebSphere Application Server :
   - Pour un serveur WebSphere Application Server qui n'est pas en cluster, rechargez la configuration Tivoli Federated Identity Manager.
   - Pour un environnement WebSphere Application Server en cluster (répliqué), effectuez une nouvelle synchronisation complète de WebSphere Application Server et rechargez la configuration Tivoli Federated Identity Manager.

Que faire ensuite

Passez à la section «Configuration d'un adaptateur en registre personnalisé WebSphere Application Server».

Configuration d'un adaptateur en registre personnalisé WebSphere Application Server

Pour procéder à l'intégration à WebSphere, configurez le registre personnalisé Tivoli Access Manager adapter as a WebSphere Application Server.

Avant de commencer

Réalisez la tâche «Configuration d'un adaptateur Tivoli Access Manager», à la page 455.

Pourquoi et quand exécuter cette tâche

Après la configuration de l'adaptateur Tivoli Access Manager avec l'environnement d'exécution Tivoli Access Manager, vous devez configurer l'adaptateur Tivoli Access Manager VMM (Virtual Member Manager) dans WebSphere Application Server en registre personnalisé.

Remarque : Pour des informations sur la configuration des registres personnalisés WebSphere Federated Repository, consultez la documentation liée à WebSphere Application Server. Pour WebSphere Application Server Network Deployment 6.1, consultez le centre de documentation WebSphere.

Procédure

1. Arrêtez WebSphere Application Server.
2. Placez-vous dans le répertoire suivant :

   WebSphere_Installation_directory/profiles/*profile_name*/config/cells/*cell_name*/wim/config
3. Utilisez un éditeur de texte pour ouvrir `wimconfig.xml`.

   Remarque : Sauvegardez `wimconfig.xml` avant de le modifier.
4. Ajoutez un nouvel élément `config:repositories` au fichier. Placez cet élément avant l'élément `config:realmConfiguration`.

   Cette entrée spécifie le nom de classe de l'adaptateur et elle définit un identificateur pour le référentiel. Par exemple, pour spécifier un nom de classe de `com.tivoli.pd.vmm.adapter.tam.TAMRegistryAdapter` et pour définir le référentiel `TAMRegistryAdapter` en tant qu'identificateur :

   ```
   <config:repositories
   adapterClassName="com.tivoli.pd.vmm.adapter.tam.TAMRegistryAdapter"
   id="TAMRegistryAdapter"/>
   ```
5. Sauvegardez le fichier wimconfig.xml, et fermez l'éditeur de texte.
6. Copiez le fichier *TAM_installation_directory*/java/export/vmm_tam_adapter/VMMTamAdapter.jar dans *WebSphere_install_directory*/lib.
7. Démarrez **wsadmin** en mode hors **connexion** :

   ```
   wsadmin -conntype none
   ```
8. Désactivez la pagination dans la configuration de référentiel commun. Définissez le paramètre `supportPaging` pour la commande `updateIdMgrRepository` sur `false` pour désactiver le pagination.

   ```
   $AdminTask updateIdMgrRepository {-id TAMRegistryAdapter
    -supportPaging false }
   ```

   Remarque : Un avertissement s'affiche jusqu'à la fin de la configuration de l'exemple de référentiel.
9. Ajoutez une propriété personnalisée à `TAMRegistryAdapter`.

   ```
   $AdminTask setIdMgrCustomProperty {-id TAMRegistryAdapter
   -name tamConfFile -value "properties_file_destination"}
   ```

   properties_file_destination
   : Le fichier de propriétés créé suite à l'exécution de **com.tivoli.pd.rgy.util.RgyConfig** dans le cadre de la tâche prérequise «Configuration d'un adaptateur Tivoli Access Manager», à la page 455.
10. Ajoutez une entrée de base à la configuration de l'adaptateur à l'aide de la commande **addIdMgrRepositoryBaseEntry** pour indiquer le nom de l'entrée de base pour le référentiel spécifié :

```
$AdminTask addIdMgrRepositoryBaseEntry {-id TAMRegistryAdapter
base-name base_entry_name }
```

base_entry_name
Ce nom doit correspondre au suffixe utilisé par le registre utilisateur Tivoli Access Manager.

11. Utilisez la commande **addIdMgrRealmBaseEntry** pour ajouter l'entrée de base au domaine. Cette action relie le domaine au référentiel.

```
$AdminTask addIdMgrRealmBaseEntry {-name defaultWIMFileBasedRealm
-baseEntry base_entry_name }
```

base_entry_name
Ce nom doit correspondre à la valeur spécifiée dans la commande précédente.

defaultWIMFileBasedRealm
Le nom de domaine par défaut est `defaultWIMFileBasedRealm`. Si le nom de domaine a été modifié, utilisez le vrai nom de domaine plutôt que `defaultWIMFileBasedRealm`.

12. Sauvegardez les modifications apportées à votre configuration. Entrez les commandes suivantes pour sauvegarder la nouvelle configuration et fermer l'outil **wsadmin** :

```
$AdminConfig save
exit
```

13. Redémarrez WebSphere Application Server.

Que faire ensuite

Sélectionnez l'une des options suivantes :

- Si vous pouvez vous connecter à WebSphere Application Server, poursuivez avec «Configuration d'un fichier de réponses», à la page 461
- Si vous ne pouvez pas vous connecter à WebSphere Application Server, voir «Identification et résolution des incidents de connexion à WebSphere Application Server»

Identification et résolution des incidents de connexion à WebSphere Application Server

Si vous ne pouvez pas vous connecter à la configuration WebSphere Application Server suivante de l'adaptateur, revoyez ces astuces d'identification et résolution des problèmes.

Pourquoi et quand exécuter cette tâche

S'il est impossible de contacter un registre, WebSphere Application Server vous empêche de vous connecter. Cette limitation survient même si le compte d'administration WebSphere Application Server est situé dans un registre différent. Une configuration incorrecte ou le manque de disponibilité d'un registre requis peut impliquer que WebSphere Application Server vous empêche de vous connecter en administrateur.

Si vous rencontrez ce problème après la configuration de l'adaptateur Tivoli Access Manager, essayez les opérations suivantes :

Procédure

1. Vérifiez que le registre Tivoli Access Manager est disponible. Etant donné que l'adaptateur de Tivoli Access Manager Registry ne maintient pas de cache

d'authentification, une erreur indiquant qu'il est impossible de vous connecter s'affiche dès l'indisponibilité du registre.

a. Utilisez **pdadmin** pour vous connecter au registre et effectuez une création de test pour confirmer.
b. Redémarrez le registre et corrigez tout problème de connexion si nécessaire.
c. Si le problème persiste, passez à l'étape suivante.

2. Ouvrez le fichier `wimconfig.xml` et vérifiez les paramètres du nouveau code que vous créez.

```
<config:repositories adapterClassName="com.tivoli.pd.vmm.adapter.tam.TAMRegistryAdapter"
id="TAMRegistryAdapter" supportPaging="false">
<config:baseEntries name="o=ibm,c=us"/>
<config:CustomProperties
name="tamConfFile"
value="/opt/IBM/WebSphere/AppServer/profiles/dmgr/config/itfim/tamVMMAdapter.properties"/>
</config:repositories>
```

Figure 53. Exemples de paramètres wimconfig.xml

- Confirmez que l'emplacement ou le nom du fichier de propriétés est correct.
- Confirmez que le suffixe est correct pour le registre Tivoli Access Manager.

Remarque : Si vous modifiez le fichier de configuration, vous devez redémarrer WebSphere Application Server. WebSphere Application Server nécessite que vous vous connectiez en administrateur pour arrêter WebSphere Application Server. Toutefois, si vous ne pouvez pas vous connecter, vous devez arrêter le processus WebSphere Application Server. Vous pouvez alors redémarrer WebSphere Application Server sans connexion.

3. Si vous n'avez pas identifié de problèmes liés au fichier de configuration lors de l'étape suivante, revenez à la copie de sauvegarde de wimconfig.xml.
   a. Faites une copie de sauvegarde de votre nouveau fichier wimconfig.xml.
   b. Restaurez la sauvegarde du fichier wimconfig.xml original.
   c. Redémarrez WebSphere Application Server.

      Remarque : WebSphere Application Server nécessite que vous vous connectiez en administrateur pour arrêter WebSphere Application Server. Toutefois, si vous ne pouvez pas vous connecter, vous devez arrêter le processus WebSphere Application Server. Vous pouvez alors redémarrer WebSphere Application Server sans connexion.

   Si vous pouvez vous connecter après la restauration du fichier sauvegardé, le problème se situe au niveau de la configuration de l'adaptateur Tivoli Access Manager. Revoyez la configuration et corrigez les erreurs.

Configuration d'un serveur Active Directory

Configurez WebSphere Federated Repository pour Microsoft Active Directory.

Pourquoi et quand exécuter cette tâche

N'utilisez pas cette tâche si vous utilisez Tivoli Access Manager en registre utilisateur. Voir «Configuration d'un adaptateur Tivoli Access Manager», à la page 455.

Procédure

1. Connectez-vous à la console d'administration.
2. Sélectionnez l'onglet Sécurité, puis sélectionnez Sécurité globale.
3. Cliquez sur **Configurer**.
   L'icône est située à la droite du menu des référentiels fédérés.
4. Cliquez sur l'option d'**ajout d'une entrée de base au domaine**.
5. Cliquez sur **Ajouter le référentiel**.
6. Entrez un nom d'**identificateur de référentiel**
   Vous pouvez indiquer un nom d'identificateur.
7. Entrez les valeurs dans les zones suivantes :
   - **Type de répertoire**
   - **Nom d'hôte principal**
   - **Port**
   - **Nom distinctif Bind**
   - **Mot de passe Bind**

   Vous pouvez fournir en option des valeurs pour les zones supplémentaires.
8. Dans la console WebSphere Application Server, sélectionnez **Require SSL communications** (Demander aux communications SSL).

   Remarque : La configuration de communications SSL entre un WebSphere Application Server et un registre utilisateur tel qu'Active Directory exige d'autres étapes. Voir la documentation pour votre version de WebSphere Application Server pour des instructions sur la configuration des connexions SSL avec WebSphere Application Server.
9. Cliquez sur **OK** et sauvegardez. Vous pouvez maintenant voir une page qui demande le **nom distinctif d'une entrée de base qui identifie de manière unique cet ensemble d'entrées dans le domaine**.
10. Entrez un nom d'entrée de base. Cliquez sur **OK** et sauvegardez.
    Si nécessaire, voir la documentation WebSphere Application Server relative à WebSphere Federated Repository.

    Remarque : Mémorisez le nom de l'entrée de base. Vous devez l'utiliser lors de la configuration de User Self Care.
    La page de configuration pour **defaultWIMFileBasedRealm** s'affiche.
11. Examinez la table intitulée **Référentiels du domaine**. Vérifiez que le nouveau domaine s'affiche, et que l'**entrée de base** est définie sur la valeur que vous entrez. Cliquez sur **OK** et sauvegardez. La console d'administration revient à la page **Sécurité globale**.
12. Cochez la case d'**activation de la sécurité d'application**.
13. Cliquez sur **OK** et sauvegardez.

Que faire ensuite

Passez à la section «Configuration d'un fichier de réponses».

Configuration d'un fichier de réponses

Créez un fichier de réponses et remplissez-le avec les valeurs spécifiques à votre déploiement.

Pourquoi et quand exécuter cette tâche

User Self Care charge la configuration à partir d'un fichier de propriétés XML appelé *fichier de réponses*. Ce fichier contient les réponses aux options de configuration. Dans la plupart des cas, le contenu du fichier de réponse est généré par les choix de l'administrateur lors du déploiement initial. Pour User Self Care, le chargement d'un fichier de propriétés est requis dans le cadre de la configuration initiale.

Procédure

1. Créez un fichier de réponses selon nécessaire pour votre déploiement. Utilisez **wsadmin**:

   ```
   $AdminTask manageItfimUserSelfCare {-operation createResponseFile
   -fileId target_location }
   ```

   La valeur *emplacement_cible* représente le chemin complet vers un fichier créé. La valeur *emplacement_cible* représente le chemin complet vers un fichier créé.
2. Déterminez la valeur de chaque paramètre dans le fichier de réponses, tel que requis par votre déploiement.

   Eventuellement, utilisez la feuille de travail suivante pour planifier votre fichier de réponses. La feuille de travail identifie les paramètres requis. Dans le fichier de réponses, vous pouvez rechercher la chaîne `REQUIRED` pour trouver ces paramètres.

   Pour plus d'informations sur chaque paramètre de cette feuille de travail, voir Chapitre 38, «Paramètres de fichier de réponses», à la page 477

Tableau 126. Paramètres du fichier de réponses User Self Care

Paramètre du fichier de réponses	Obligatoire/ facultatif	Valeur par défaut	Votre valeur
AccountCreateLifetime	oui	86400	
AccountRecoveryFailureLifetime	non	86400	
AccountRecoveryFailureLimit	non	3	
AccountRecoveryFailureLockoutTime	non	86400	
AccountRecoveryLookupAttribute	non	mail	
AccountRecoveryLookupField	non	aucun	Cette zone est dépréciée.
AccountRecoveryValidationAttributes	non	mail	
AccountRecoveryValidationLifetime	non	86400	
AttributeMappingFilename	oui	aucun	
BaseURL	oui	aucun	
CaptchaSTSModuleId	oui	default-usc-captcha-noop	
DemoCaptchaImageAndKeyList	Oui, en cas d'utilisation de Captcha	Contenu fixe.	Ne pas modifier.
DemoCaptchaImageRootURL	Oui, en cas d'utilisation de Captcha	aucun	
EnrollmentEmailSender	oui	aucun	
EntitySuffix	oui	o=ibm,c=us	
GroupMembershipGroups	non	aucun	

Tableau 126. Paramètres du fichier de réponses User Self Care (suite)

Paramètre du fichier de réponses	Obligatoire/ facultatif	Valeur par défaut	Votre valeur
PasswordRecoveryEmailSender	oui	aucun	
ProfileManagementAttributes	oui	businessCategory roomNumber mobile mail	
SMTPAuthenticatePassword	Non, à moins que votre serveur SMTP ne l'exige	aucun	
SMTPAuthenticateUsername	Non, à moins que votre serveur SMTP ne l'exige	aucun	
SMTPServerName	oui	aucun	

3. Mettez à jour votre fichier de réponses avec les valeurs, puis sauvegardez le fichier.

Que faire ensuite

Poursuivez avec la rubrique : «Configuration de User Self Care».

Configuration de User Self Care

Procédez aux étapes de cette rubrique pour configurer User Self Care avec le déploiement Tivoli Federated Identity Manager.

Avant de commencer

Vérifiez que vous avez réalisé les tâches de configuration prérequises :

1. «Configuration d'un domaine Tivoli Federated Identity Manager», à la page 454
2. «Configuration d'un registre utilisateur», à la page 454
3. «Configuration d'un fichier de réponses», à la page 461

Pourquoi et quand exécuter cette tâche

Réalisez les étapes suivantes dans l'ordre. Les instructions pour chaque tâche fournissent un lien vers la tâche suivante. La liste des tâches s'affiche ici en présentation générale.

Procédure

1. «Affichage des chaînes d'accréditation», à la page 464
2. «Configuration de la démonstration Captcha», à la page 464

   Ignorez cette étape si vous n'avez pas l'intention d'utiliser la démonstration Captcha.
3. «Utilisation d'un fichier de réponses pour configurer User Self Care», à la page 465
4. «Configuration d'un serveur point de contact», à la page 466
5. «Intégration de User Self Care à WebSEAL», à la page 467

Ignorez cette étape si vous utilisez WebSphere Application Server en serveur point de contact

Affichage des chaînes d'accréditation

Vous pouvez configurer Tivoli Federated Identity Manager de sorte à afficher les chaînes d'accréditation créées par défaut pour User Self Care.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la console d'administration pour afficher chaque chaîne d'accréditation. Les chaînes d'accréditation correspondent à une ou plusieurs opérations User Self Care. Lorsque vous affichez les chaînes d'accréditation, vous voyez les modules STS accomplissant l'opération. Vous pouvez alors personnaliser les modules et chaînes selon votre déploiement.

Remarque : Pour des informations sur la personnalisation de User Self Care, voir le wiki Tivoli Federated Identity Manager :

http://www.ibm.com/developerworks/wikis/display/tivolifederatedidentitymanager/Home

Procédure

1. Connectez-vous à la console d'administration.
2. Accédez au panneau Gestion des noeuds d'exécution.
3. Dans la partie de propriété personnalisée du panneau, sélectionnez l'entrée de menu pour `STS.showUSCChains`.
4. Définissez la valeur sur `true`.
5. Sauvegardez la configuration.
6. A l'invite, chargez les modifications de configuration.
7. Redémarrez WebSphere Application Server pour actualiser les commandes de gestion disponibles à **wsadmin**.

Que faire ensuite

Sélectionnez une des étapes suivantes :

- Si vous souhaitez utiliser la démonstration Captcha, poursuivez avec «Configuration de la démonstration Captcha».
- Si vous ne souhaitez pas utiliser la démonstration Captcha, poursuivez avec «Utilisation d'un fichier de réponses pour configurer User Self Care», à la page 465.

Configuration de la démonstration Captcha

Vous pouvez éventuellement configurer la démonstration Captcha dans le cadre de votre déploiement User Self Care.

Avant de commencer

Vérifiez que vous avez réalisé toutes les tâches de configuration prérequises :

- «Configuration d'un domaine Tivoli Federated Identity Manager», à la page 454
- «Configuration d'un registre utilisateur», à la page 454
- «Configuration d'un fichier de réponses», à la page 461
- «Affichage des chaînes d'accréditation»

Procédure

1. Hébergez les fichiers d'images fournis sur un serveur Web accessible à vos utilisateurs.

   Assurez-vous que vous connaissez l'emplacement de l'URL racine des images utilisé lors de la configuration du module STS Captcha. La valeur est stockée dans le paramètre DemoCaptchaImageRootURL du fichier de réponses.
2. Activez le plug-in :
   a. Copiez le fichier jar Captcha dans le répertoire de plug-ins de Tivoli Federated Identity Manager. Par exemple, copiez :

      FIM_install_dir/examples/demo/captcha/com.tivoli.am.fim.demo.sts.captcha.jar

      dans le répertoire :

      TFIM_install_dir/plugins
   b. A l'aide du panneau Gestion des noeuds d'exécution, cliquez sur l'icône **Publier les plug-ins**.
   c. Cliquez sur **Charger les modifications de configuration**.
3. Utilisez le panneau d'instances du module pour créer une instance de DemoCaptchaSTSModule. Définissez le nom de l'instance du module sur la valeur `usc-captcha-demo`.

Que faire ensuite

Passez à la section «Utilisation d'un fichier de réponses pour configurer User Self Care».

Utilisation d'un fichier de réponses pour configurer User Self Care

Utilisez le fichier de réponses que vous avez créé précédemment pour fournir les propriétés nécessaires à la commande de configuration pour User Self Care.

Avant de commencer

Vérifiez que vous avez réalisé les tâches de configuration prérequises :

- «Configuration d'un domaine Tivoli Federated Identity Manager», à la page 454
- «Configuration d'un registre utilisateur», à la page 454
- «Configuration d'un fichier de réponses», à la page 461
- «Affichage des chaînes d'accréditation», à la page 464
- Si vous utilisez la démonstration Captcha, assurez-vous qu'elle est configurée. Voir «Configuration de la démonstration Captcha», à la page 464.

Procédure

1. Obtenez votre fichier de réponses configuré.
2. Exécutez **wsadmin**

   ```
   wsadmin.sh -username WebSphere_adminstrator_name -password password
   ```
3. Chargez le fichier de réponses :

   ```
   $AdminTask manageItfimUserSelfCare {-operation configure -fimDomainName
   domain_name -federationName federation_name
    -fileId response_file_path }
   ```

   Fournissez ces valeurs :

domain_name
Le nom du domaine Tivoli Federated Identity Manager que vous avez créé.

federation_name
Le nom de la fédération Tivoli Federated Identity Manager que vous avez créée.

response_file_path
Emplacement de votre fichier de réponses User Self Care.

4. Rechargez la configuration Tivoli Federated Identity Manager.

```
$AdminTask reloadItfimRuntime {-fimDomainName domain_name }
```

Fournissez cette valeur :

domain_name
Le nom du domaine Tivoli Federated Identity Manager que vous avez créé.

Que faire ensuite

Poursuivez avec la rubrique : «Configuration d'un serveur point de contact».

Configuration d'un serveur point de contact

Vous devez configurer un serveur point de contact pour User Self Care.

Sélectionnez les instructions pour le type de serveur point de contact utilisé par votre déploiement :

- «Configuration de WebSphere Application Server en tant que serveur point de contact»
- «Configuration de WebSEAL en tant que serveur point de contact», à la page 467

Configuration de WebSphere Application Server en tant que serveur point de contact

Vous pouvez configurer WebSphere Application Server en tant que serveur point de contact pour User Self Care.

Procédure

1. Utilisez **wsadmin** pour activer le type de point de contact **WebSphere**.

   Utilisez les commandes **wsadmin** :

```
$AdminTask manageItfimPointOfContact {-operation activate
-uuid uuid4f3d17d-0106-w412-r36b-a0d5ecc604ba
-fimDomainName your_domain_name}

$AdminTask reloadItfimRuntime {-fimDomainName your_domain_name}
```

2. Connectez-vous à la console d'administration.
3. Sélectionnez **Enterprise Applications > ITFIMRuntime > Rôle de sécurité pour le mappage utilisateur/groupe**.
4. Mettez à jour le rôle d'application **FIMUserSelfCareAnyAuthenticated** avec **AnyAuthenticated**.
5. Sauvegardez la configuration WebSphere Application Server.
6. Redémarrez WebSphere Application Server.

Que faire ensuite

Consultez les instructions liées au réglage des performances dans le Chapitre 37, «Réglage de User Self Care», à la page 473.

Configuration de WebSEAL en tant que serveur point de contact

Vous pouvez configurer WebSEAL en serveur point de contact pour User Self Care.

Procédure

1. Déterminez l'emplacement de votre fichier tfimcfg.jar.

   Ce fichier est situé dans la hiérarchie sous le répertoire d'installation Tivoli Federated Identity Manager. Sous UNIX, le chemin est le suivant :

   ```
   /opt/IBM/FIM/tools/tamcfg/tfimcfg.jar
   ```

2. Exécutez l'outil **tfimcfg**.

   ```
   java -jar tfimcfg.jar -cfgfile /opt/pdweb/etc/webseald-default.conf
   -action tamconfig
   ```

   Remarques sur l'utilisation :

   - Les chemins de fichier peuvent varier selon votre installation et votre instance WebSEAL
   - Le port HTTP par défaut de Tivoli Federated Identity Manager est 9080. Ce port est également le port WC_defaulthost pour WebSphere Application Server.
   - Ne spécifiez pas d'ID utilisateur administrateur ni de mot de passe Tivoli Federated Identity Manager facultatif
   - Répondez `non` à la question `Utiliser la connexion SSL au serveur ITFIM`.
   - Sélectionnez `uscfed` dans la liste des fédérations à configurer.

Que faire ensuite

Poursuivez avec la rubrique : «Intégration de User Self Care à WebSEAL».

Intégration de User Self Care à WebSEAL

Les déploiements User Self Care ayant un registre Tivoli Access Manager utilisent la plupart du temps WebSEAL en serveur point de contact. Dans ce cas, vous devez intégrer les interactions entre deux composants qui accomplissent la tâche de suppression de compte et de gestion de mot de passe.

- Suppression de compte

  Lorsqu'un utilisateur supprime son compte du registre Tivoli Access Manager dans le cadre d'un déploiement User Self Care, vérifiez que sa session en cours est terminée. Cette restriction est requise dans la cadre des recommandations de sécurité

  La suppression de la session utilisateur inclut sa session WebSEAL. User Self Care arrête par défaut la session WebSEAL lorsque le compte est supprimé. Toutefois, cet arrêt dépend de votre utilisation antérieure de l'outil tfimcfg pour configurer WebSEAL en serveur point de contact. Si vous avez exécuté cet outil tel que décrit précédemment, aucune configuration spéciale n'est requise.

  Si vous n'avez pas configuré WebSEAL en serveur point de contact, procédez à cette opération maintenant. Voir «Configuration de WebSEAL en tant que serveur point de contact».

- Gestion de mot de passe

  Deux opérations de gestion de mot de passe sont affectées lorsque WebSEAL est le serveur point de contact. Il s'agit des opérations suivantes : Modifier le mot de passe et Mot de passe expiré. Ces deux intégrations nécessitent que vous autorisiez l'accès non authentifié à la page de modification du mot de passe et que vous utilisiez un formulaire Modifier le mot de passe User Self Care.

Intégration de l'opération de modification de mot de passe à WebSEAL

Lorsque WebSEAL est le serveur point de contact et qu'un utilisateur souhaite modifier un mot de passe, l'utilisateur doit fournir les données. Il existe plusieurs méthodes pour ce faire.

Les voici :

- L'utilisateur peut accéder directement à l'URL Modifier le mot de passe User Self Care
- Le formulaire de modification de mot de passe WebSEAL peut rediriger l'utilisateur vers le même formulaire de User Self Care. Vous pouvez ajouter un réacheminement de balise meta dans la page de modification de mot de passe WebSEAL pour prendre en charge cette action.

Intégration de l'opération de mot de passe expiré à WebSEAL

WebSEAL, en tant que serveur point de contact, gère l'authentification, y compris les mots de passe expirés. Toutefois, lorsque User Self Care est intégré à WebSEAL, il doit gérer la gestion des mots de passe expirés.

Dans ce cas, les étapes suivantes se produisent :

1. WebSEAL indique la session authentifié sur `expired` (expirée).
2. L'utilisateur voit une version modifiée du formulaire de mot de passe expiré WebSEAL
3. L'utilisateur entre des données et soumet le formulaire de mot de passe expiré. Cette action envoie les données de mot de passe à l'URI de modification de mot de passe User Self Care.

   Remarque : Les données de mot de passe peuvent être présentées par toute sorte d'éléments. Elles doivent répondre à certains critères et POST de l'URI cible User Self Care. Lorsque l'utilisateur a soumis le formulaire, User Self Care traite le contenu du formulaire et gère les erreurs. Ce traitement peut inclure l'affichage du formulaire de modification de mot de passe User Self Care à l'utilisateur avec les détails concernant les erreurs.
4. User Self Care gère la modification du mot de passe.
5. La session WebSEAL s'arrête.

   Remarque : La session WebSEAL s'arrête car l'entrée de session gérée par WebSEAL est indiquée `expired` (expirée). Jusqu'à la modification de cet indicateur, l'utilisateur voit toujours le formulaire de modification de mot de passe WebSEAL. L'utilisateur ne peut pas continuer, même après avoir modifié son mot de passe à l'aide de User Self Care. L'arrêt de la session est également recommandé pour des raisons de sécurité, car il est nécessaire que l'utilisateur se connecte avec son nouveau mot de passe afin de poursuivre.
6. La page de réussite de modification de mot de passe User Self Care s'affiche à l'utilisateur. Cette page peut être modifiée en vue d'un réacheminement vers WebSEAL si vous le souhaitez.

Etapes de configuration

Effectuez chacune des étapes suivantes pour l'opération à intégrer à WebSEAL :

- Pour intégrer l'opération de modification de mot de passe à WebSEAL :

1. «Autorisation d'accès non authentifié au formulaire de modification de mot de passe de User Self Care»
2. «Modification du formulaire de modification de mot de passe WebSEAL User Self Care»

- Pour intégrer l'opération de mot de passe expiré à WebSEAL :
  1. «Autorisation d'accès non authentifié au formulaire de modification de mot de passe de User Self Care»
  2. «Modification du formulaire de modification de mot de passe WebSEAL User Self Care»
  3. «Modification d'un formulaire de mot de passe expiré WebSEAL», à la page 470
  4. «Prise en charge du réacheminement vers WebSEAL», à la page 471

Autorisation d'accès non authentifié au formulaire de modification de mot de passe de User Self Care

Pour prendre en charge l'intégration de l'opération de mot de passe WebSEAL, les utilisateurs non authentifiés doivent pouvoir accéder à l'URI de modification de mot de passe via une jonction WebSEAL. La jonction doit être configurée avec SSL pour la confidentialité.

Utilisez pdadmin pour autoriser l'accès non authentifié au formulaire de modification de mot de passe de User Self Care situé à l'emplacement suivant :

WebSEAL_server/*fim_junction*/sps/uscfed/usc/self/password/update

Consultez la documentation Tivoli Access Manager pour des informations concernant la commande **pdadmin**.

Lorsque vous modifiez cet accès, vous devez utiliser un nouveau formulaire de modification de mot de passe User Self Care. Poursuivez avec la rubrique «Modification du formulaire de modification de mot de passe WebSEAL User Self Care».

Modification du formulaire de modification de mot de passe WebSEAL User Self Care

L'ID utilisateur doit être fourni dans le formulaire Modifier le mot de passe lors de l'intégration des opérations de modification de mot de passe User Self Care à WebSEAL.

Pourquoi et quand exécuter cette tâche

L'autorisation de l'accès non authentifié signifie qu'il est possible aux utilisateurs d'accéder au formulaire de modification du mot de passe. D'une perspective de sécurité, cette action utilisateur est acceptable car l'utilisateur doit entrer son ancien mot de passe dans ce formulaire avant qu'il ne procède à sa modification. Toutefois, vous devez modifier modify to the default User Self Care form to activate this function.

Par défaut, User Self Care n'exigent pas que les utilisateurs entrent leur ID utilisateur dans le formulaire de modification de mot de passe. A la place, User Self Care rassemble les informations d'un contexte authentifié. Ce mécanisme ne fonctionne pas si l'utilisateur ne s'authentifie pas avant de demander le formulaire.

Si l'utilisateur demande le formulaire sans authentification, User Self Care renvoie un message d'erreur indiquant qu'aucune identité utilisateur authentifiée n'est disponible.

Pour éviter cette erreur, l'ID utilisateur doit être fourni dans le formulaire Modifier le mot de passe lors de l'intégration des opérations de modification de mot de passe User Self Care à WebSEAL.

Procédure

1. Faites une copie de sauvegarde de *FIM_install_dir*/pages/C/usc/password/changepassword.html
2. Copiez le fichier d'exemple changepassword.html dans le référentiel de pages User Self Care.
   - Le fichier d'exemple est :
     FIM_install_dir/examples/examples/html/usc/password/changepassword.html
   - L'emplacement de destination est :
     FIM_install_dir/pages/C/usc/password/changepassword.html
3. Connectez-vous à la console d'administration.
4. Accédez au panneau **Gestion des noeuds d'exécution**. Cliquez sur l'option d'**actualisation des pages**.
5. Sauvegardez les modifications de configuration.

Que faire ensuite

- Si vous intégrez l'opération de modification de mot de passe, vous avez terminé la tâche.
- Si vous intégrez l'opération de mot de passe expiré, poursuivez avec «Modification d'un formulaire de mot de passe expiré WebSEAL»

Modification d'un formulaire de mot de passe expiré WebSEAL

Modifiez le formulaire de mot de passe expiré WebSEAL pour vous assurer une bonne gestion des mots de passe dans User Self Care.

Avant de commencer

Vérifiez que vous avez réalisé les tâches prérequises :

1. «Autorisation d'accès non authentifié au formulaire de modification de mot de passe de User Self Care», à la page 469
2. «Modification du formulaire de modification de mot de passe WebSEAL User Self Care», à la page 469

Pourquoi et quand exécuter cette tâche

Il existe plusieurs moyens de modifier le formulaire. La méthode suivante est la plus simple.

Procédure

1. Copiez le fichier User Self Care changepassword.html dans le répertoire WebSEAL dans lequel sont situés les pages de gestion. Renommez-le en usc_changepassword.html.

Par exemple :

```
/opt/pdweb/www-default/lib/html/C/usc_changepassword.html
```

2. Editez le formulaire `usc_changepassword.html` comme suit :
   a. Ajoutez une nouvelle zone masquée :

      ```
      <input type="hidden" name="usc.form.password.expired.flag" value="true" />
      ```

   b. Ajoutez une autre nouvelle zone masquée :

      ```
      <input type="hidden" name="usc.form.userid" value="%USERNAME%" />
      ```

   c. Supprimez ou commentez les deux lignes :

      ```
      <div class="hidden" id="errorDiv"> </div>
      <div class="hidden" id="errorAttrDiv"> </div>
      ```

   d. Remplacez la macro du formulaire `ACTION` par l'URL de la cible de modification de mot de passe User Self Care.

      Par exemple :

      ```
      https://webseal.example.com/fimjct/sps/uscfed/usc/self/password/update
      ```

3. Définissez les droits et appartenance de fichier de `usc_changepassword.html` de sorte à faire correspondre les droits des autres fichiers de gestion WebSEAL.
4. Editez le fichier de configuration WebSEAL. Accédez à la section `acnt-mgt` et modifiez la valeur `passwd-expired = passwd_exp.html` en `passwd-expired = usc_changepassword.html`
5. Redémarrez WebSEAL.

Que faire ensuite

Eventuellement, vous pouvez poursuivre avec «Prise en charge du réacheminement vers WebSEAL»

Prise en charge du réacheminement vers WebSEAL

Eventuellement, vous pouvez rediriger les utilisateurs vers WebSEAL une fois qu'ils ont modifié leur mot de passe.

Pourquoi et quand exécuter cette tâche

Parfois, vous pouvez décider d'héberger une *page d'atterrissage* avec des liens vers des destinations à partir du système WebSEAL plutôt que le système User Self Care.

Procédure

1. Créez une page de *réussite de modification de mot de passe* dans le répertoire docs WebSEAL.

   Cette page est la page d'atterrissage de WebSEAL. Elle peut par exemple indiquer que `votre mot de passe a été correctement modifié et que vous devez vous connecter à nouveau pour accéder aux pages protégées`.
2. Modifiez la page User Self Care située dans *`FIM_install_dir`*`/pages/C/usc/password/changepassword_success.html` pour ajouter une balise de redirection meta qui achemine le client vers la page WebSEAL de *réussite de modification de mot de passe*.

Modification d'une fédération User Self Care

Il existe des restreintes quant à la manière de modifier des fédérations User Self Care existantes.

- L'interface de ligne de commande ne prend pas en charge la modification des fédérations User Self Care. Utilisez la console d'administration pour définir la propriété d'exécution STS.showUSCChains sur `true`. Affichez les chaînes d'accréditation User Self Care et modifiez-les, ainsi que les propriétés, selon nécessaire.

  Notez que vous pouvez également configurer User Self Care en répétant les étapes de déploiement initiales. Dans ce cas, vous devez créer et éditer un nouveau fichier de réponse, puis utilisez l'interface de ligne de commande pour déployer la fédération.
- Il est impossible de capturer, au sein d'un fichier de réponse, les paramètres de configuration spécifiques à une chaîne particulière. Par exemple, les modules STS de mappage d'attributs utilisent un fichier de règle de mappage. Différentes chaînes peuvent avoir différentes règles de mappage. Vous ne pouvez pas spécifier les différentes règles de mappage lors de la création d'un fichier de réponse d'une configuration existante.

  Les paramètres pouvant être spécifiques à une chaîne particulière n'ont pas de valeurs définies dans le fichier de réponse. Lorsque différentes chaînes ont différentes règles de mappage, utilisez la console d'administration afin de modifier les modules de chaîne pour utiliser différents fichiers de règles

Annulation de la configuration de User Self Care

Utilisez **wsadmin** pour annuler la configuration de User Self Care.

Pourquoi et quand exécuter cette tâche

Cette tâche supprime les chaînes d'accréditation User Self Care et la fédération User Self Care.

Procédure

1. Démarrez **wsadmin**.
2. Exécutez la commande :

```
$AdminTask manageItfimUserSelfCare {-operation unconfigure
-fimDomainName your_domain_name -federationName uscfed}
```

Chapitre 37. Réglage de User Self Care

Vous pouvez améliorer les performances de User Self Care en ajustant les paramètres pour plusieurs caches distribués.

User Self Care prend en charge trois caches distribués différents :

- Cache de création de compte
- Cache de mot de passe oublié
- Cache d'échec de question secrète

Les caches sont partagés parmi les membres de cluster WebSphere Application Server pour permettre la bonne gestion d'une opération utilisateur. Ce partage est requis au cas où différentes phases de l'opération ont lieu sur différents noeuds.

User Self Care utilise la technologie WebSphere Distributed Object Cache pour implémenter les caches. Voir la documentation WebSphere Application Server pour plus de détails sur cette technologie de mise en cache.

Il existe deux types de paramètres qui affectent chaque cache distribué User Self Care :

Durées de vie d'entrées
Ces paramètres sont définis dans le fichier de réponses. Les entrées de cache sont conservées jusqu'à la fin de la durée de vie ou jusqu'à ce que l'utilisateur termine l'opération demandant l'entrée de cache.Les noms et paramètres de cette configuration spécifique à la mise en cache sont décrits dans les descriptions de réglage de cache individuel plus loin dans ce document.

Tailles de cache
Ces paramètres sont définis dans la console d'administration en accédant à **Ressources > Instances de cache > Instances de cache de l'objet**. Le paramètre de `taille de cache` contrôle le nombre d'entrées concurrentes conservées dans le cache. Les noms et paramètres de cette configuration spécifique à la mise en cache sont décrits dans les descriptions

Vous devez définir la taille des caches de manière appropriée pour que les utilisateurs puissent effectuer des opérations nécessitant un cache distribué dans la période configurée. Si un cache est trop petit, il peut arriver que les utilisateurs ne puissent pas valider leurs comptes ou récupérer leurs mots de passe durant la période spécifiée. Vous pouvez spécifier la période dans la configuration de durée de vie des entrées du cache.

Par exemple, pour donner à vos utilisateurs deux minutes pour finir une validation de récupération de compte, configurez la durée de vie de l'entrée pour le cache de validation de récupération de compte sur deux minutes. Si vous attendez deux utilisateurs par seconde pour effectuer une opération de récupération de compte, définissez le cache de validation de récupération de compte sur une valeur d'au moins 240.

Déterminez la taille appropriée à l'aide des calculs suivants :

```
120 secondes x 2 utilisateurs/seconde = 240
```

La taille par défaut du cache de validation de récupération de compte est de 1000 entrées. Cette valeur par défaut serait appropriée dans le cas l'exemple précédent. D'autres opérations, telles que la création de compte, peuvent nécessiter une augmentation de la taille du cache.

Selon l'utilisation attendue de votre système, vous pouvez augmenter la taille d'un ou plusieurs caches. Cet ajustement peut affecter la configuration matérielle requise. Les entrées de cache utilisent de la mémoire ; elles doivent être répliquées entre les systèmes du cluster.

Il est recommandé de fournir un tampon pour la taille du cache attendue.

Voir les rubriques suivantes :

- «Cache de création de compte»
- «Cache de mot de passe oublié», à la page 475
- «Cache d'échec relatif à la question secrète», à la page 475
- «Remarques concernant le réglage des caches», à la page 475

Cache de création de compte

Ce cache stocke les données des entrées utilisateur pendant la création de compte et le message envoyé après le processus de validation. Dès que l'utilisateur termine la validation, User Self Care récupère les données à partir du cache pour créer un compte dans le registre.

Tableau 127. Paramètres de cache de création de compte

Paramètre	Description
AccountCreateLifetime	Les durées de vie des entrées sont contrôlées par le paramètre `AccountCreateLifetime` décrit à la rubrique : Chapitre 38, «Paramètres de fichier de réponses», à la page 477
itfim-usc_accountcreate	La taille du cache est contrôlée par la taille du cache `itfim-usc_accountcreate`.

Contrairement aux autres opérations, chaque opération de création de compte crée deux entrées de cache. Une entrée est uniquement composée de l'ID utilisateur et d'une clé. La seconde entrée est composée de toutes les données entrées par l'utilisateur dans le formulaire de création de compte.

Vous configurez les durées de vie d'entrée de cache sur 120 secondes. Attendez-vous à une valeur maximale d'utilisateurs s'inscrivant lors d'une nouvelle opération d'application des accès de 10 chacun/seconde. Vous pouvez décider de la taille de cache suivante :

```
10 utilisateurs/seconde x 2 entrées/utilisateur x 120 secondes/entrée =
2400 x 20% tampon ~= 3000.
```

Cache de mot de passe oublié

Ce cache stocke l'ID utilisateur lors de l'opération de validation Mot de passe oublié.

Tableau 128. Paramètres de cache de mot de passe oublié

Paramètre	Description
AccountRecoveryValidationLifetime	Les durées de vie des entrées sont contrôlées par le paramètre `AccountRecoveryValidationLifetime` décrit à la rubrique : Chapitre 38, «Paramètres de fichier de réponses», à la page 477.
itfim-usc_forgottenpassword	La taille du cache est contrôlée par la taille du cache `itfim-usc_forgottenpassword`. Cette entrée est courte, elle est principalement composée de l'ID utilisateur et d'une clé.

Cache d'échec relatif à la question secrète

Ce cache stocke le nombre de tentatives échouées de réponses à la question secrète ayant eu lieu jusque là.

Tableau 129. Paramètres de cache d'échec relatif à la question secrète

Paramètre	Description
AccountRecoveryFailureLifetime	Les durées de vie des entrées sont contrôlées par le paramètre `AccountRecoveryFailureLifetime` décrit à la rubrique : Chapitre 38, «Paramètres de fichier de réponses», à la page 477
itfim-usc_secretquestionfailures	La taille du cache est contrôlée par la taille du cache `itfim-usc_secretquestionfailures`. Cette entrée est composée d'un chiffre et d'une clé.

Remarques concernant le réglage des caches

La configuration des opérations WebSphere Application Server peut améliorer votre réglage des caches.

- Réplication

  WebSphere ne réplique pas automatiquement toutes les données mises en cache entre les noeuds. A la place, il réplique uniquement les clés entre les noeuds et extrait uniquement les données lorsque la requête est effectuée par un noeud particulier. Si une clé est demandée sur un noeud particulier introuvable sur le cache, User Self Care tente une opération de recherche de cache. La tentative fournit du temps à WebSphere Application Server pour terminer toute réplication possible.
- Vidages de cache

  Le redémarrage de WebSphere Application Server efface les caches et les renvoie à un état propre.
- Suppression de caches User Self Care

  Les entrées de cache sont conservées jusqu'à la fin de la durée de vie de l'entrée ou jusqu'à ce que l'utilisateur termine l'opération demandant l'entrée de cache.

Chapitre 38. Paramètres de fichier de réponses

Utilisez les paramètres décrits dans cette section pour configurer les fichiers de réponses pour User Self Care.

AccountCreateLifetime
Indique la durée, en secondes, pendant laquelle Self Care utilisateur reconnaît la demande de création de compte comme étant valide, et conserve la requête dans le cache interne. Si la chaîne d'accréditation Create Account n'effectue pas de création de compte dans la durée spécifiée, la demande est annulée et la création de compte prend fin.

Cette propriété est obligatoire.
Type : entier
Valeur par défaut : 86 400
Maximum :
aucun
Minimum : 0

Un paramètre de '0' désactive les créations de compte car les entrées ne sont pas conservées dans le cache. Des paramètres plus gros peuvent affecter l'exploitation de mémoire et affecter potentiellement les performances dans les environnements répliqués à cause de l'augmentation de données répliquées à l'aide de DynaCache sur les noeuds.

Lors de la définition de cette propriété, considérez également une taille adéquate pour le `cache itfim-usc_accountcreate`. Voir : Chapitre 37, «Réglage de User Self Care», à la page 473.

AccountRecoveryFailureLifetime
Indique pendant combien de temps, en secondes, le programme conserve l'enregistrement d'une tentative de validation de compte ayant échoué. Lorsque la période indiquée est écoulée, l'enregistrement de la tentative ayant échoué est supprimé et le compteur est décrémenté de un.

Type : entier
Valeur par défaut : 86 400
Maximum :
aucun
Minimum : 0. La valeur 0 indique une désactivation du verrouillage.

Lors de la définition de cette propriété, considérez également une taille adéquate pour le `itfim-usc_secretquestionfailures`. Ce paramètre est configuré séparément lors du réglage de User Self Care. Voir : Chapitre 37, «Réglage de User Self Care», à la page 473.

AccountRecoveryFailureLimit
Indique le nombre de fois qu'un utilisateur peut tenter de restaurer en vain l'accès au compte avant que le programme ne verrouille le compte. Si l'utilisateur ne donne pas la bonne réponse à la question secrète, l'accès au compte n'est pas restauré. Si l'utilisateur échoue à restaurer l'accès au compte, la valeur de cette propriété s'incrémente de un. Lorsque la valeur est égale au nombre indiqué, le programme verrouille le compte.

Type : entier
Valeur par défaut : 3
Maximum :
aucun
Minimum : 0.

Un paramètre de 0 ou 1 pour la valeur minimum entraîne le verrouillage du compte dès le premier échec.

AccountRecoveryFailureLockoutTime
Indique pendant combien de temps, en secondes, le programme laisse le compte verrouillé une fois que l'utilisateur a dépassé le nombre maximum de tentatives de validation ayant échoué. Si le programme a verrouillé le compte, cette valeur définit le temps qui doit s'écouler avant que le programme ne déverrouille le compte.

Type : entier
Valeur par défaut : 86 400
Maximum :
aucun
Minimum : 0. La valeur 0 désactive le verrouillage.

AccountRecoveryLookupAttribute
Indique un attribut que Self Care utilisateur utilise comme cible de message au cours de l'opération liée au mot de passe oublié. Par défaut, User Self Care définit paramètre cet attribut sur l'attribut de registre mail. User Self Care envoie un courrier à la valeur détectée pour l'attribut de registre indiqué.

Type : chaîne
Par défaut : `mail`

AccountRecoveryLookupField
Cette zone est dépréciée. Ne pas la modifier.

AccountRecoveryValidationAttributes
Indique un attribut utilisateur utilisé pour la recherche d'ID utilisateur. Cette propriété indique un attribut unique que l'utilisateur saisit dans le formulaire Forgotten user ID (ID utilisateur oublié) pour récupérer son ID utilisateur (identité). Self Care utilisateur se sert de cet attribut de registre comme d'une zone de recherche. Self Care utilisateur recherche une entrée contenant l'attribut fourni par l'utilisateur et retourne l'ID utilisateur correspondant.

Type : chaîne
Par défaut : `mail`

La valeur que vous entrez ici représente le nom réel de l'attribut de registre. Le module de service de jetons sécurisé de mappage d'attribut ne mappe pas ce paramètre lors du mappage de zones d'entrée fournies par l'utilisateur sur les attributs de registre. Le nom d'attribut `mail` représente la zone LDAP standard utilisée pour l'adresse de messagerie électronique.

AccountRecoveryValidationLifetime
Indique la durée (en secondes) pendant laquelle User Self Care considère que la demande de validation de compte est valide.

Au cours de la récupération de mot de passe, les utilisateurs doivent exécuter une étape de validation avant de récupérer leur mot de passe. L'étape de validation consiste à répondre à un courrier électronique User Self Care

indiquant un lien d'accès. Si l'utilisateur ne répond pas dans la temps défini par ce paramètre, le programme invalide le lien du courrier électronique.

Type : entier
Valeur par défaut : 86 400
Maximum :
aucun
Minimum : 0

Un paramètre de 0 pour la valeur minimum désactive la capacité de récupérage d'un compte.

Lors de la définition de cette propriété, considérez également une taille adéquate pour le cache `itfim-usc_forgottenpassword`. Ce paramètre est configuré séparément lors du réglage de User Self Care. Voir : Chapitre 37, «Réglage de User Self Care», à la page 473.

AttributeMappingFilename
Indique le chemin vers l'emplacement d'un fichier contenant les règles de transformation à utiliser avec le module STS de mappage d'attribut. Ce fichier peut être un fichier JavaScript ou XSLT.

User Self Care est livré avec un fichier JavaScript par défaut appelé `usc.js` :
Federated_Identity_Manager_installation_dir`/examples/js_mappings`

Cette propriété est obligatoire.
Type : chaîne
Par défaut : aucun

Exemple :
```
/opt/IBM/FIM/examples/js_mappings/usc.js
```

BaseURL
Indique une URL complète pour la racine de la fédération User Self Care. User Self Care utilise la racine pour créer des éléments HTML dynamiques. La syntaxe est la suivante :
method`//`*POC_server:port*`/`*FIM_junction*`/sps`

Où :

method
Doit être `http:`ou `https:`

POC_server:port
Le nom d'hôte complet, et numéro de port facultatif, du serveur point de contact.

FIM_junction
Le nom de la jonction WebSEAL. Cette valeur est requise uniquement lors de l'utilisation d'un serveur point de contact WebSEAL.

Cette propriété est obligatoire.
Type : chaîne
Par défaut : aucun

Exemple :
```
https://myWebSEALserver.example.com/myTFIMjct/sps
```

Remarque : Si vous utilisez WebSEAL en serveur point de contact, vous n'avez probablement pas encore créé de jonction vers le serveur Tivoli Federated Identity Manager. La plupart du temps, vous créez cette jonction à la fin des étapes de configuration de User Self Care. Toutefois, vous devez déterminer le nom de la jonction maintenant, de sorte à pouvoir définir la valeur BaseURL dans le fichier de réponses. Vous devez mémoriser le nom de jonction, pour une utilisation ultérieure lors de l'exécution de la commande **tfimcfg**.

CaptchaSTSModuleId
Indique le module Captcha de démonstration ou un module de marque de réservation qui ne réalise aucune action. Lorsque cette valeur est spécifiée, User Self Care active le module de démonstration Captcha.

Cette propriété est obligatoire.
Type : chaîne
Par défaut : aucun

Il existe deux valeurs valides pour cette zone :

- `usc-captcha-demo`

  Utilisez cette valeur si vous voulez activer le module de démonstration Captcha. Si vous utilisez ce paramètre, vous devez définir les autres paramètres Captcha dans ce fichier de réponses. Pour utiliser la démonstration Captcha, vous devez également configurer le module. Voir : «Configuration de la démonstration Captcha», à la page 464.

- `default-usc-captcha-noop`

  Utilisez cette valeur si vous voulez utiliser le module de marque de réservation `USCNoOpsSTSModule`. Ce module n'effectue aucune action, mais sert de marque de réservation pour un module de validation fourni par le client qui peut être utilisé, par exemple, pour la validation Captcha. USCNoOpsSTSModule facilite aux clients l'entrée de leur propre module sans redéfinir les chaînes d'accréditation.

DemoCaptchaImageAndKeyList
Cette zone est requise si vous utilisez le module de démonstration Captcha.

Le contenu est fixe et ne peut pas être modifié.

Remarque : Le paramètre `DemoCaptchaImageAndKeyList` a déjà été défini. Le programme ignore ce paramètre si vous n'utilisez pas le module de démonstration Captcha.

DemoCaptchaImageRootURL
Indique l'URL d'un répertoire contenant les images utilisées pour le module de démonstration Captcha fourni avec User Self Care.

Vous devez indiquer une valeur pour cette propriété si vous souhaitez utiliser le module de démonstration Captcha.

Exemple :

```
https://images.example.com/captcha/demo
```

EnrollmentEmailSender
Indique une adresse électronique qualifiée complète pour le compte que Self Care utilisateur utilise pour envoyer un message à l'utilisateur. Le message valide l'inscription de l'utilisateur. La plupart du temps, il s'agit d'une adresse électronique qui ne reçoit pas de réponse.

Cette propriété est obligatoire.
Type : chaîne
Par défaut : aucun

Exemple :

```
no-reply@example.com
```

EntitySuffix
Indique un suffixe dans lequel les utilisateurs créés sont stockés dans le registre. Ce suffixe doit identifier un identifiant de manière unique le registre que User Self Care utilise pour toutes les opérations.

Cette propriété est obligatoire.
Type : chaîne
Valeur par défaut :

```
o=ibm,c=us
```

GroupMembershipGroups
Indique une liste de groupes auxquels ajouter des utilisateurs qui viennent d'être écrits. Indique un ou plusieurs groupes définis dans le registre d'utilisateurs utilisé par la chaîne d'accréditation Create Account. Les noms de groupes sont spécifiques au registre d'utilisateurs.

Type : chaîne
Par défaut : aucun

Exemple :

```
<void method="add">
 <string>Group1</string>
</void>
<void method="add">
 <string>Group2</string>
</void>
```

PasswordRecoveryEmailSender
Indique une adresse électronique qualifiée complète pour le compte Self Care utilisateur qui envoie un message à l'utilisateur. Self Care utilisateur utilise le message pour valider une opération de récupération de mot de passe. La plupart du temps, cette adresse électronique ne reçoit pas de réponse.

Cette propriété est obligatoire.
Type : chaîne
Par défaut : aucun

Exemple :

```
no-reply@example.com
```

ProfileManagementAttributes
Définit l'ensemble d'attributs de registre utilisés pour les informations de profil. Afin de fournir un prototype de travail, la solution User Self Care définit un ensemble d'attributs de registre à utiliser avec la fonction par défaut. User Self Care ne modifie pas le schéma du registre cible. Pour cette raison, le nombre d'attributs de profil est limité ; il utilise des attributs LDAP standard qui sont présents dans la plupart des cas.

Cette propriété est obligatoire. Voici la liste des attributs utilisés :

- businessCategory
- roomNumber
- mobile
- mail

Les attributs sont représentés dans le fichier de configuration comme suit :

```
<object class="java.util.ArrayList">
 <void method="add">
  <string>businessCategory</string>
 </void>
 <void method="add">
  <string>roomNumber</string>
 </void>
 <void method="add">
       <string>mail</string>
     </void>
 <void method="add">
       <string>mobile</string>
     </void>
</object>
```

Figure 54. Attributs de gestion de profil dans le fichier de réponses

SMTPAuthenticatePassword
Mot de passe correspondant au compte indiqué par le paramètre SMTPAuthenticateUsername lors de l'utilisation de l'authentification dans le serveur SMTP. Cette propriété est facultative.

Type : chaîne
Par défaut : aucun

SMTPAuthenticateUsername
Nom d'utilisateur permettant de s'authentifier auprès du serveur SMTP. Cette propriété est facultative.

Type : chaîne
Par défaut : aucun

SMTPServerName
Nom de système hôte qualifié complet du serveur Simple Mail Transport Protocol (SMTP) qui envoie un message électronique pour l'utilisateur. Cette propriété est obligatoire.

Type : chaîne
Par défaut : aucun

Partie 6. Personnalisation

Les rubriques de la section Personnalisation expliquent comment personnaliser les composants et fonctions de Tivoli Federated Identity Manager pour mieux répondre aux besoins de votre environnement.

Chapitre 39. Personnalisation des propriétés de l'environnement d'exécution

Les propriétés personnalisées permettent de personnaliser le service d'exécuton de Tivoli Federated Identity Manager afin de répondre à vos besoins spécifiques.

L'utilisation des propriétés personnalisées fait partie des tâches de niveau avancé. Vous devez sans doute vous familiariser avec des sujets plus étendus concernant l'architecture et les services de Tivoli Federated Identity Manager, afin de comprendre le mode d'utilisation des propriétés personnalisées. Pour plus d'informations sur la définition de ces paramètres, reportez-vous au centre de documentation de Tivoli Federated Identity Manager : http://publib.boulder.ibm.com/infocenter/tiv2help/index.jsp

Création d'une propriété personnalisée

Vous pouvez personnaliser la configuration d'un domaine en définissant une propriété personnalisée.

Pourquoi et quand exécuter cette tâche

La syntaxe des propriétés personnalisées est la suivante :

nom_propriété = valeur_propriété

Procédure

1. Connectez-vous à la console, puis cliquez sur **Tivoli Federated Identity Manager → Gestion des domaines → Gestion des noeuds d'exécution**.
2. Le panneau Gestion des noeuds d'exécution s'affiche. Cliquez sur **Propriétés personnalisées de l'environnement d'exécution**. Le panneau Propriétés personnalisées de l'environnement d'exécution s'affiche.
3. Sélectionnez la portée de la propriété personnalisée (cellule ou noeud) dans la liste **Portée**. La liste de propriétés de la portée sélectionnée s'affiche.
4. uliquez sur **Créer**. Un élément est ajouté à la liste des propriétés, avec le nom **nouvelle clé** et la valeur **nouvelle valeur**.
5. Sélectionnez la propriété de la marque de réservation.
6. Entrez une chaîne dans la zone **Nom**. N'insérez pas d'espace dans cette zone.
7. Entrez une chaîne dans la zone **Valeur**. Les espaces sont autorisés dans cette zone.
8. Cliquez sur **OK** pour appliquer les modifications effectuées et quitter le panneau.

Suppression d'une propriété personnalisée

Procédure

1. Connectez-vous à la console, puis cliquez sur **Tivoli Federated Identity Manager → Gestion des domaines → Gestion des noeuds d'exécution**.
2. Le panneau Gestion des noeuds d'exécution s'affiche. Cliquez sur **Propriétés personnalisées de l'environnement d'exécution**. Le panneau Propriétés personnalisées de l'environnement d'exécution s'affiche.

3. Sélectionnez la portée de la propriété personnalisée (cellule ou noeud) dans la liste **Portée**. La liste de propriétés de la portée sélectionnée s'affiche.
4. Sélectionnez une paire nom-valeur.
5. Cliquez sur **Supprimer**. Le panneau est régénéré et la paire nom-valeur est supprimée de la liste des propriétés personnalisées.
6. Choisissez l'une des actions suivantes :
   - Cliquez sur **Appliquer** pour appliquer les modifications effectuées sans quitter le panneau.
   - Cliquez sur **OK** pour appliquer les modifications effectuées et quitter le panneau.

Liste de référence des propriétés personnalisées

Vous pouvez définir les valeurs de plusieurs propriétés personnalisées. Cette section décrit chacune de ces propriétés.

Pour ajouter des propriétés personnalisées à la configuration de votre domaine, voir «Création d'une propriété personnalisée», à la page 485.

Propriétés générales

DistributedMap.GetRetryLimit
Lorsque cette valeur est définie et supérieure à 0, l'encapsuleur interroge la mappe distribuée autant de fois qu'indiqué dans la configuration avant de renvoyer un message indiquant que les données ne s'y trouvent pas.
- Type de valeur : entier
- Exemple de valeur : 2

DistributedMap.GetRetryDelay
Lorsque le nombre de relances est supérieur à 1, cette valeur définit le temps d'attente entre deux relances (en millisecondes). La valeur par défaut est 2000, soit 2 secondes.
- Type de valeur : entier
- Exemple de valeur : 2000

componentName.**statisticsEnabled**
Lorsque la valeur 'True' est spécifiée, la fonction de suivi statistique d'un composant spécifique est activée et les données collectées peuvent être extraites à l'aide des mécanismes présentés par le composant. Lorsque la valeur 'false'

est définie, le suivi statistique n'a pas lieu. En règle générale, cette propriété est définie sur la valeur 'true' pour les composant nécessitant un comptage numérique ou temporel.

- Type de valeur : booléen
- Exemple de valeur : False

Propriétés personnalisées du service de protocole de connexion unique

requireSoapActionForSoap
Ce paramètre surveille le comportement du service de protocole de connexion unique lorsqu'il reçoit une requête via la méthode POST du navigateur et qu'il doit en déterminer le type (SOAPRequest ou BrowserRequest). Il permet au service de gérer les clients SOAP non conformes qui n'envoient pas l'en-tête SOAPAction nécessaire dans les requêtes.

Valeur par défaut : 'true'

- Type de valeur : booléen
- Exemple de valeur : true

requireContentTypeForSoap
Ce paramètre détermine si une requête SOAP doit contenir ou non un type de contenu `text/xml` ou `application/soap+xml`. Il permet au service de protocole de connexion unique de gérer les clients SOAP non conformes.

Remarque : Lorsque ce paramètre et requestSoapActionForSoap ont tous deux pour valeur 'false', toutes les requêtes reçues sont interprétées comme des requêtes SOAP.

Valeur par défaut : 'true'

- Type de valeur : booléen
- Exemple de valeur : true

POC.allowsCredRefresh
Lorsqu'il a pour valeur 'true', ce paramètre permet d'ignorer LocalLogoutAction au niveau du fournisseur de services lors de la connexion unique et de la fédération. A la place, il régénère les données d'identification. Définissez ce paramètre sur la valeur true pour les plug-ins Web. Sinon, attribuez-lui la valeur false.

Valeur par défaut : 'true'

- Type de valeur : booléen
- Exemple de valeur : true

SPS.PageFactory.HtmlEscapedTokens
Une liste de jetons séparés par des virgules devant utiliser les caractères d'échappement HTML lors de l'affichage sur les pages envoyées au navigateur. En général, cette propriété inclut les macros de la propriété personnalisée d'exécution SPS.PageFactory.Exception2Macro (si elle est utilisée). Cette propriété est une considération de sécurité importante pour empêcher les vulnérabilités de scripts intersites.

- Type de valeur : chaîne
- Exemple de valeur : @TOKEN_A@,@TARGET@

SPS.PageFactory.Exception2Macro
Cette propriété personnalisée d'exécution est une liste séparée par des virgules de paires classname:macro. Le nom de classe représente le nom complet d'une

classe d'exception. La macro est la macro de remplacement avec laquelle la classe est mappée. La macro doit commencer et finir par “@”, comme indiqué dans les exemples de valeurs.

- Type de valeur : chaîne
- Valeurs d'exemples : com.demo.MyException: @MYEXCEPTION@, com.tivoli.am.fim.trustserver.sts.STSException: @STSEXCEPTION@

SPS.POC.Default.Header.Names.Enabled
cette propriété, lorsqu'elle est spécifiée, permet d'utiliser des noms d'en-tête par défaut comme valeurs d'en-tête du point de contact. Si ce paramètre est défini sur FALSE, les seuls en-têtes qui seront lus ou écrits devront faire partie du fichier de configuration sps.xml.

- Type de valeur : booléen
- Exemple de valeur : false

POC.WebSeal.SignOutInfoDelegate.UserSessionIdHeaderName
Cette valeur se substitue à la valeur par défaut tagvalue_user_session_id.

- Type de valeur : chaîne
- Exemple de valeur : tagvalue_user_session_id

SPS.WebSealPoc.ContextPoolSize
Indique le nombre d'objets PDContext disponibles dans le pool. Cette valeur correspond au nombre de clients à autoriser lors de l'utilisation de la connexion unique. Il peut s'avérer nécessaire d'augmenter cette valeur en fonction de la charge représentée par les déconnexions. En cas de déconnexions simultanées massives, l'environnement d'exécution Tivoli Federated Identity Manager risque de contenir un nombre d'objets PDContext insuffisant, ce qui peut entraîner l'échec des déconnexions. Etant donné que chaque objet PDContext utilise des ressources système, telles que la mémoire et des descripteurs de fichier, cette valeur doit être sélectionnée avec soin. Elle doit être supérieure à 0.

Valeur par défaut : 5

- Type de valeur : entier
- Exemple de valeur : 5

SPS.WebSealPoc.DisablePDSignout
Lorsqu'il a pour valeur 'true', ce paramètre désactive la fonctionnalité de déconnexion du client point de contact WebSEAL du service de protocole de connexion unique. En cas d'appel de l'opération de déconnexion, il consigne l'absence de déconnexion et renvoie une réponse positive. Lorsque ce paramètre est activé, la configuration de Tivoli Access Manager Java Runtime (PDJRTE) n'est pas nécessaire pour le service de protocole de connexion unique.

Valeur par défaut : 'false'.

- Type de valeur : booléen
- Exemple de valeur : true

SPS.WebSealPoc.Force.PdAdmin.Task
Lorsqu'il a pour valeur 'true', ce paramètre impose, lors du rappel du point de contact WebSeal, l'utilisation systématique des tâches **pdadmin server** pour déconnecter l'utilisateur.

- Type de valeur : booléen
- Exemple de valeur : false

SPS.WebSealPoc.ContextPoolInitAttempts
Cette valeur représente le nombre de tentatives d'initialisation des objets PDContext. La valeur par défaut est 1 et cette valeur doit être supérieure à 0.

- Type de valeur : entier
- Exemple de valeur : 1

SPS.WebSealPoc.ContextPoolInitTimeout
cette valeur représente le nombre maximal d'initialisations des objets PDContext. Une fois le délai expiré, l'initialisation prend fin. La valeur par défaut est 10000 et cette valeur (exprimée en millisecondes) doit être supérieure à 0.

- Type de valeur : entier
- Exemple de valeur : 10000

Propriétés personnalisées du service d'accréditation

username.disable.password.validation
Lorsqu'il a pour valeur 'true', ce paramètre permet à UsernameTokenSTSModule d'ignorer la validation du mot de passe.

La valeur par défaut est 'false'.

- Type de valeur : booléen
- Exemple de valeur : true

username.jaas.provider.hostname
Ce paramètre permet de définir un autre nom pour le système hôte local, au cas où le nom d'hôte indiqué dans la configuration WebSphere ne soit pas localhost.

La valeur par défaut est localhost.

- Type de valeur : chaîne
- Exemple de valeur : localhost

username.jaas.provider.port
Ce paramètre permet de spécifier le port configuré pour le service WebSphere NameServer local.

La valeur par défaut est 2809.

- Type de valeur : entier
- Exemple de valeur : 2809

pdjrte.context.min.pool.size
Indique la taille minimale du pool de contextes d'autorisation. Ce paramètre est utilisé par UsernameTokenSTSModule. Il ne doit être défini que s'il est recommandé à la suite d'une évaluation de performances.

- Type de valeur : entier
- Exemple de valeur : 5

pdjrte.context.max.pool.size
Indique la taille maximale du pool de contextes d'autorisation. Ce paramètre est utilisé par UsernameTokenSTSModule. Il ne doit être défini que s'il est recommandé à la suite d'une évaluation de performances.

- Type de valeur : entier
- Exemple de valeur : 50

ivcred.allow.groupUpdate
Lorsqu'il a pour valeur 'true', ce paramètre tente de modifier les données d'identification en ajoutant des groupes.

Remarque : Ne jamais utiliser ce paramètre.

- Type de valeur : booléen
- Exemple de valeur : false

saml.use.rst.lifetime
Indique aux modules SAML d'utiliser la durée de vie de l'élément RequestSecurityToken pour déduire celle de la vérification SAML émise. Lorsqu'il a pour valeur 'false', il n'utilise pas la durée de vie de RequestSecurityToken.

Valeur par défaut : false.

- Type de valeur : booléen
- Exemple de valeur : false

passticket.disable.uppercase.principal
Ordonne au module PassTicket de ne pas convertir le nom de principal en majuscules sans tenter au préalable de générer un Passticket à l'aide d'un gestionnaire RACF natif. Lorsqu'il a pour valeur FALSE, il convertit toujours le nom de principal en majuscules pour le gestionnaire RACF natif.

Valeur par défaut : false.

- Type de valeur : booléen
- Exemple de valeur : false

sts.use.issuer.saml20.sso
La valeur par défaut "false" ordonne au module SAML 2.0 d'utiliser la valeur "Issuer" au lieu de la valeur "NameID NameQualifier" pour rechercher un alias lors d'une opération de connexion unique.

Valeur par défaut : 'false'.

- Type de valeur : booléen
- Exemple de valeur : false

username.wss.namespace.override
Lorsque cette propriété n'est pas précisée, la valeur par défaut est l'espace de nom du profil de jeton WSS 1.1. La clé de cette propriété peut être utilisée comme préfixe pour définir la portée de la propriété sur une chaîne STS spécifique (exemple : username.wss.namespace.override.uuid1234)

- Type de valeur : chaîne
- Exemple de valeur : *<a_URI_namespace>*

Propriétés personnalisées du service de clés

kessjksservice.include.keyinfo.x509.certificate.data
Inclut un certificat codé en Base64 dans l'élément KeyInfo de la signature. Lorsque ce paramètre a pour valeur 'true', implicitement ou par l'utilisation explicite de cette propriété, les autres propriétés d'exécution KESS sont ignorées. Lorsque cette propriété n'est pas précisée, la valeur par défaut est 'true'.

- Type de valeur : booléen
- Exemple de valeur : true

kessjksservice.include.keyinfo.x509.subject.key.identifier
Inclut l'identificateur de clé du sujet dans l'élément KeyInfo de la signature lorsque le certificat délivré le prend en charge. Utilisable en supplément de issuer.details et subject.name. Lorsque cette propriété n'est pas précisée, la valeur par défaut est 'false'.

- Type de valeur : booléen
- Exemple de valeur : true

kessjksservice.include.keyinfo.x509.issuer.details
Ajoute des informations sur l'émetteur X509 dans l'élément KeyInfo de la signature. Utilisable en supplément de subject.key.identifier et subject.name. Lorsque cette propriété n'est pas précisée, la valeur par défaut est 'false'.

- Type de valeur : booléen
- Exemple de valeur : true

kessjksservice.include.keyinfo.x509.subject.name
Ajoute le nom distinctif du sujet X509 dans l'élément KeyInfo de la signature. Utilisable en supplément de subject.key.identifier et issuer.details. Lorsque cette propriété n'est pas précisée, la valeur par défaut est 'false'.

- Type de valeur : booléen
- Exemple de valeur : true

kessjksservice.exclude.inclusive.namespace.prefixes
Liste de noms de préfixe séparés par des virgules. Lorsque cette propriété est définie, les préfixes de la liste ne sont pas ajoutés à la liste InclusiveNamespaces de l'élément Signature.

- Type de valeur : chaîne
- Exemple de valeur : ds

Propriétés personnalisées d'un client SOAP

com.tivoli.am.fim.soap.client.jsse.provider
Nom de fournisseur Java Secure Socket Extension (JSSE) devant être utilisé à la place d'IBMJSSE pour les connexions socket client SOAP.

- Type de valeur : chaîne
- Exemple de valeur : IBMJSSE

com.tivoli.am.fim.soap.client.jce.provider
Nom de fournisseur Java Cryptography Extension (JCE) Cryptography Socket Extension (JCE) devant être utilisé à la place d'IBMJCE pour les fichiers de clés certifiées de client SOAP.

- Type de valeur : chaîne
- Exemple de valeur : IBMJCE

com.tivoli.am.fim.soap.client.trust.provider
Nom d'algorithme du fournisseur Java Trust Manager qu'il convient d'utiliser à la place d'IbmX509 pour les gestionnaires d'accréditation SOAP client.

- Type de valeur : chaîne
- Exemple de valeur : IbmX509

Propriétés personnalisées de SAML 2.0

SAML20.LogoutRequest.NotOnOrAfter.Enabled
Lorsque l'attribut NotOnOrAfterAttribute est défini sur TRUE, il est inclus dans les messages LogoutRequest envoyés par le fournisseur d'identité au fournisseur de services.

Valeur par défaut : True

- Type de valeur : booléen
- Exemple de valeur : true

SAML20.LogoutRequest.NotOnOrAfter.Lifetime
Indique le délai à utiliser pour définir l'attribut NotOnOrAfter lors de la demande de déconnexion.

Valeur par défaut : 120

- Type de valeur : entier
- Exemple de valeur : 300

Propriétés personnalisées de la console

STS.showSSOChains
Ce paramètre permet de vérifier si la console autorise un administrateur à gérer ou à modifier des chaînes générées automatiquement pour les transactions de connexion unique. Si vous définissez cette valeur sur `false`, la propriété personnalisée n'est pas désactivée. Vous devez supprimer la paire valeur et clé de la table de propriétés personnalisées.

- Type de valeur : booléen
- Exemple de valeur : true

STS.showUSCChains
Ce paramètre permet de vérifier si la console autorise un administrateur à gérer ou à modifier des chaînes générées automatiquement pour les fédérations User Self Care. Si vous définissez cette valeur sur `false`, la propriété personnalisée n'est pas désactivée. Vous devez supprimer la paire valeur et clé de la table de propriétés personnalisées.

- Type de valeur : booléen
- Exemple de valeur : true

STS.showAQChains
Ce paramètre permet de vérifier si la console autorise un administrateur à gérer ou à modifier des chaînes générées automatiquement pour les fédérations SAML 2 activant le service de requête d'attribut. Si vous définissez cette valeur sur `false`, la propriété personnalisée n'est pas désactivée. Vous devez supprimer la paire valeur et clé de la table de propriétés personnalisées.

- Type de valeur : booléen
- Exemple de valeur : true

Propriété personnalisée pour OpenID

OpenID.TrustedSitesManagerModuleID
Ceci est un identificateur de module d'extension qui implémente le point d'extension com.tivoli.am.fim.protocols.openid_trusted_sites_manager. Il existe deux exemples d'implémentaton de cette extension :

- TrustedSitesManagerCookieImpl
- TrustedSitesManagerMemoryImpl

Lorsque ce paramètre n'est pas spécifié, la valeur par défaut est TrustedSitesManagerCookieImpl.

- Type : chaîne
- Exemple de valeur : TrustedSitesManagerCookieImpl

Propriété personnalisée pour le protocole de sécurité de transport

Définition du protocole de sécurité de transport pour les connexions HTTPS

Le protocole sécurisé par défaut pour les connexions HTTPS créées par IBM Tivoli Federated Identity Manager est `SSL_TLS`. Pour modifier (substituer) le protocole par défaut, indiquez la propriété personnalisée d'exécution suivante dans le fichier `fim.appservers.properties` :

```
com.tivoli.am.fim.soap.client.ssl.protocol= PROTOCOL
```

où la valeur de *PROTOCOL* peut être l'une des suivantes : `SSL_TLS`, `SSL`, `SSLv2`, `SSLv3`, `TLS` ou `TLSv1`.

Propriétés personnalisées pour les jetons LTPA

Spécification des propriétés d'exécution de Tivoli Federated Identity Manager personnalisées qui forcent la génération QName compatible

Les versions 6.0.2 et 6.1 de WebSphere Application Server ne font pas la distinction entre les jetons LTPA v1 et LTPA v2 dans le services Web. Seules les valeurs BinarySecurityToken ValueType sont prises en charge pour les jetons LTPA, et le QName du type de valeur est :

```
http://www.ibm.com/websphere/appserver/tokentype/5.0.2#LTPA
```

Lorsque le module STS de Tivoli Federated Identity Manager émet un jeton LTPA v2, le jeton est créé avec le QName suivant. Ce QName est correct, mais il n'est pas pris en charge par WebSphere Application Server versions 6.0.2 et 6.1 :

```
http://www.ibm.com/websphere/appserver/tokentype#LTPAv2
```

Cet APAR fournit des propriétés d'exécution Tivoli Federated Identity Manager personnalisées qui forcent la génération QName compatible si nécessaire. Pour activer le mode de compatibilité, définissez une ou deux des propriétés d'exécution personnalisées suivantes :

```
ltpa.enable.compat.mode.[chainid_uuid]=true ltpa.enable.compat.mode=true
```

où *chainid_uuid* représente la valeur de l'UUID de la chaîne. Par exemple :

ltpa.enable.compat.mode.[uuideb42e428-011b-1ebc-a0cb-9e6c4b35c1c7]=true

Pour déterminer la valeur de l'UUID de la chaîne, sélectionnez **Chaînes du service d'accréditation**-> **Sélectionner Action**, dans la console d'administration, puis sélectionnez l'option d'**affichage d'ID de chaîne dans la colonne de la table**. Cette sélection d'action entraîne l'affichage d'une nouvelle colonne dans la table qui présente l'ID de chaîne unique.

Chapitre 40. Personnalisation d'un formulaire de connexion d'authentification pour une connexion unique

Personnalisez un formulaire de connexion d'authentification en ajoutant des paramètres à un profil de serveur point de contact WebSphere ou WebSEAL.

Lorsque des requêtes utilisateur accèdent à une fédération de connexion unique, le fournisseur d'identité lance une connexion unique en authentifiant l'utilisateur. Pour authentifier l'utilisateur, le fournisseur d'identité utilise un serveur point de contact afin d'afficher une page de connexion basée sur des formulaires.

Lorsqu'un fournisseur d'identité participe à plusieurs fédérations ou héberge plusieurs partenaires dans une fédération, l'administrateur peut personnaliser le formulaire de connexion par défaut.

En tant qu'administrateur, vous pouvez personnaliser

- La page de connexion selon le contenu des requêtes envoyées par les fournisseurs de service.
- L'apparence du formulaire de connexion.
- Le type d'authentification requis.
- Les pages de connexion pour les serveurs point de contact WebSEAL et WebSphere.

Pour personnaliser la page de connexion, utilisez la console d'administration Tivoli Federated Identity Manager pour configurer un nouveau profil de serveur point de contact. Dans le nouveau profil, ajoutez un paramètre à l'appel d'authentification, et indiquez une ou plusieurs valeurs pour le paramètre.

Tivoli Federated Identity Manager fournit des paramètres qui sont toujours disponibles et cohérents sur tous les types de fédération et d'autres qui sont spécifiques au type de fédération.

Les protocoles qui prennent en charge les paramètres spécifiques au protocole sont les suivants :

- SAML 1.x
- SAML 2
- OpenID

L'ensemble de valeurs définies sont décrites dans la rubrique «Macros prises en charge pour la personnalisation d'un formulaire de connexion d'authentification», à la page 496

Présentation des tâches :

1. Consultez les valeurs prises en charge pour votre type de protocole et identifiez celles que vous souhaitez utiliser. Voir «Macros prises en charge pour la personnalisation d'un formulaire de connexion d'authentification», à la page 496.
2. Créez un nouveau profil de serveur point de contact. Voir «Configuration d'un serveur point de contact pour prendre en charge la personnalisation des pages de connexion», à la page 499.

Macros prises en charge pour la personnalisation d'un formulaire de connexion d'authentification

Cette rubrique décrit l'ensemble de macros permettant de personnaliser un formulaire de connexion d'authentification.

Tivoli Federated Identity Manager fournit des paramètres d'authentification contextuels dans la personnalisation des formulaires de connexion. Lors de la configuration de WebSEAL en serveur point de contact, ce sont les paramètres chaîne-requête de la page de connexion. Pour WebSphere, ils sont situés dans le cookie WASReqURL lorsque la page de connexion est chargée. Les paramètres sont des macros dans la configuration de l'appel d'authentification pour le profil de serveur point de contact.

Remarque : Lorsque vous utilisez le point de contact WebSphere, l'URL de la valeur du paramètre de chaîne requête doit être décodée deux fois.

Les macros prises en charge sont les suivantes :

- Macros indépendantes du protocole
- Macros du protocole SAML
- Macros du protocole OpenID

Remarque : Si la valeur de `authentication.macros` est plis longue que la longueur autorisée du paramètre de chaîne-requête, le cookie WASReqURL ne sera pas présent dans le fournisseur d'identité.

Macros indépendantes du protocole pour la personnalisation d'un formulaire de connexion d'authentification

Les macros suivantes sont indépendantes du protocole et elles peuvent être utilisées quel que soit le type de fédération utilisé.

Tableau 130. Macros indépendantes du protocole prises en charge

Macro	Nom du paramètre de chaîne de requête	Description
%FEDID%	FedId	Spécifie une identificateur unique (UUID) utilisé en interne par Tivoli Federated Identity Manager pour identifier la fédération.
%FEDNAME%	FedName	Spécifie le nom affecté par l'utilisateur de la fédération.

Macros prises en charge par le protocole SAML pour la personnalisation d'un formulaire de connexion d'authentification

Les macros suivantes sont prises en charge pour le protocole SAML. Les macros sont prises en charge pour SAML 1.x et SAML 2.0, sauf mention contraire.

Tableau 131. Macros de protocole SAML prises en charge

Macro	Nom du paramètre de chaîne de requête	Description
%PARTNERID%	PartnerId	Représente le partenaire SSO auquel l'utilisateur tente de se connecter. Valeur SAML : la valeur est l'ID fournisseur du partenaire.
%TARGET%	Target	Représente l'URL cible au niveau du partenaire, si elle est connue. Valeur SAML : la valeur est la valeur du paramètre cible.
%ACSURL%	AssertionConsumerURL	Représente l'URL de service d'assertion client du partenaire, si applicable. Valeur SAML : la valeur est l'URL ACS partenaire.
%AUTHNCONTEXT%	AuthnContext	**Prise en charge pour SAML 2.0 uniquement** Représente la valeur AuthnContext dans la demande (si applicable). Valeur SAML : la valeur est une chaîne encodée de base 64 représentant le fichier XML de RequestedAuthnContext dans SAML AuthnRequest (si présent).
%SSOREQUEST%	SSORequest	**Prise en charge pour SAML 2.0 uniquement** Représente la valeur entière SSO (si applicable). Valeur SAML : la valeur est une chaîne encodée de base 64 représentant le fichier XML de toute la valeur SAML AuthnRequest.

Tableau 131. Macros de protocole SAML prises en charge (suite)

Macro	Nom du paramètre de chaîne de requête	Description
%FORCEAUTHN%	ForceAuthn	**Prise en charge pour SAML 2.0 uniquement** La valeur `true` ou `false`. Valeur SAML : si l'indicateur ForceAuthn est défini dans la requête SAML 2 SSO impliquant la ré-authentification de l'utilisateur, la valeur est `true`. Sinon, la valeur est `false`.

Macros prises en charge par OpenID pour la personnalisation d'un formulaire de connexion d'authentification

Les macros suivantes sont prises en charge pour le protocole OpenID.

Tableau 132. Macros prises en charge par le protocole OpenID

Macro	Nom du paramètre de chaîne de requête	En-tête
%PARTNERID%	PartnerId	Représente le partenaire SSO auquel l'utilisateur tente de se connecter. Valeur OpenID : la valeur du paramètre openid.trustroot.
%TARGET%	Target	Représente l'URL cible au niveau du partenaire, si elle est connue. Valeur OpenID : la valeur du paramètre openid.return_to.
%SSOREQUEST%	SSORequest	Représente la valeur entière SSO (si applicable). Valeur OpenID : la requête checkid_setup en version encodée basée 64 de la requête SSO codée dans l'URL.
%UNSATISFIEDPAPEPOLICIES%	UnsatisfiedPapePolicies	Représente une liste de chaînes représentant les règles PAPE. Ces chaînes sont renvoyées comme "pas encore satisfaites" par la règle de mappage du fournisseur d'identité dans une fédération de fournisseur d'identité OpenID. Valeur OpenID : règles renvoyées dans l'attribut ContextAttributes openid.pape.to_be_satisfied_auth_policies

Tableau 132. Macros prises en charge par le protocole OpenID (suite)

Macro	Nom du paramètre de chaîne de requête	En-tête
%FORCEAUTHN%	ForceAuthn	Spécifie si l'authentification est appliquée au niveau du fournisseur d'identité. Les valeurs sont `true` ou `false`. Valeur OpenID : la valeur est `true` si l'un des critères suivants est satisfait : • la valeur PAPE max_auth_age est zéro (ce qui signifie que l'authentification est réappliquée) • la règle de mappage IDP du fournisseur d'identité OpenID applique l'authentification à cause de règles PAPE non satisfaites • l'heure d'authentification renvoyée par la règle de mappage IDP ne satisfait pas la valeur max_auth_age demandée par le RP (hors zéro) Sinon, la valeur est `false`.

Configuration d'un serveur point de contact pour prendre en charge la personnalisation des pages de connexion

Cette rubrique décrit comment configurer un serveur point de contact pour prendre en charge la personnalisation d'une page de connexion.

Avant de commencer

Vérifiez que vous :

- Comprenez la manière dont les pages de connexion personnalisées sont prises en charge. Voir Chapitre 40, «Personnalisation d'un formulaire de connexion d'authentification pour une connexion unique», à la page 495.
- Connaissez les macros à spécifier pour le paramètre d'appel d'authentification. Voir «Macros prises en charge pour la personnalisation d'un formulaire de connexion d'authentification», à la page 496.

Remarque : Vous n'avez pas besoin de créer ni de publier un plug-in d'appel point de contact personnalisé avant de spécifier les macros d'authentification. La prise en charge des macros d'authentification est fournie par défaut. Lorsque vous exécutez l'assistant de configuration, vous pouvez ignorer le message indiquant que vous devez publier un plug-in avant d'utiliser l'assistant.

Pourquoi et quand exécuter cette tâche

La procédure suivante explique comment ajouter un serveur point de contact personnalisé tel que les serveurs point de contact déjà définis dans votre environnement afin de modifier les informations affichées dans une page de connexion.

Procédure

1. Connectez-vous à la console d'administration.
2. Cliquez sur **Tivoli Federated Identity Manager → Gestion des domaines → Point de contact**
3. Sélectionnez le serveur point de contact existant que vous souhaitez utiliser comme base pour votre nouveau serveur point de contact.Vous devez sélectionner un profil pour WebSEAL ou **WebSphere**.
4. Cliquez sur **Créer comme** pour afficher le panneau de bienvenue de l'assistant de profil point de contact.
5. Cliquez sur **Suivant** pour afficher le panneau de noms de profils. Il affiche les informations issues du profil sur lequel vous basez votre nouveau serveur point de contact.
6. Tapez un nom pour le profil, et éventuellement une description.
7. Cliquez sur **Suivant** pour afficher le panneau de connexion.
8. Acceptez les entrées par défaut pour les appels de connexion, les paramètres pour chaque appel, ainsi que l'ordre dans lequel ils sont utilisés, puis cliquez sur **Suivant**.
9. Acceptez les entrées par défaut pour le panneau Connexion et cliquez sur **Suivant**.
10. Acceptez les entrées par défaut pour le panneau ID local et cliquez sur **Suivant**.
11. Cliquez sur **Ajouter des paramètres** dans la section Paramètres d'appel du panneau Authentification.
12. Entrez `authentication.macros` dans Nom.
13. Entrez les macros que vous souhaitez utiliser dans Valeurs. Pour spécifier plusieurs valeurs et séparer les macros, placez une barre oblique inversée (\) et une virgule entre les valeurs. Par exemple : %FEDID%\,%FEDNAME%\, %PARTNERID%
14. Cliquez sur **Suivant** pour afficher le panneau Récapitulatif. Ce panneau affiche la liste de tous les rappels et des paramètres que vous avez spécifiez au cours des étapes précédentes.
15. Cliquez sur **Terminer** pour achever la configuration ou cliquez sur **Précédent** pour revenir aux panneaux précédents et modifier vos sélections.
16. Cliquez sur le **portlet Domaine en cours**.
17. Cliquez sur **Charger les modifications de configuration dans l'environnement d'exécution de Tivoli Federated Identity Manager**.

Que faire ensuite

«Activation d'un serveur point de contact», à la page 526

Chapitre 41. Personnalisation des pages d'événement de connexion unique

Tivoli Federated Identity Manager génèrent des fichiers qui s'affichent à la suite d'événements survenus lors des demandes de connexion unique. Il se peut que la réponse affichée corresponde à un formulaire (par exemple, lorsque des informations de connexion sont requises) ou à une instruction d'erreur ou d'information concernant une condition qui s'est produite lors du traitement de la requête.

Vous avez la possibilité de personnaliser les pages d'événement en procédant comme suit :

- Modification de leur aspect ou de leur contenu.
- Spécification de l'environnement local ou linguistique utilisé lors de l'affichage des pages.

Avant de poursuivre la personnalisation, il convient que vous ayez une connaissance approfondie de la manière dont les pages d'événement sont générées et affichées. Voir «Génération des pages d'événement».

Génération des pages d'événement

Les pages d'événement sont affichées à la suite d'événements survenus lors des demandes de connexion unique. Elles contiennent généralement un formulaire (tel qu'une invite d'informations relatives au nom d'utilisateur et au mot de passe) ou du texte (tel qu'un message d'information ou d'erreur).

Les pages d'événement sont des pages dynamiques générées par Tivoli Federated Identity Manager à partir des informations suivantes :

Fichiers modèles
Il s'agit de fichiers XML ou HTML fournis avec Tivoli Federated Identity Manager et contenant des éléments tels que des zones, du texte ou des graphiques, et parfois de macros remplacées par des informations propres à la requête afin de répondre à cette dernière.

Identificateurs de page
Informations d'événement correspondant à un ou plusieurs fichiers modèles. Chaque identificateur de page correspond à une condition d'événement spécifique, telle qu'une erreur spécifique ou une condition dans laquelle un message ou un formulaire doit être affiché. Pour créer une page d'événement, les identificateurs de page sont mappés vers un ou plusieurs fichiers modèles. La fonction de mappage permet à plusieurs identificateurs de page de désigner le même fichier modèle.

Catalogue de messages
Texte utilise pour remplacer les macros dans les fichiers modèles.

Lorsqu'une requête est reçue, la page de réponse appropriée est générée comme suit :

1. La requête est traitée et une réponse à un événement est requise.
2. Les fichiers modèles et les identificateurs de page sont lus à partir du système de fichiers.

3. Les macros des fichiers modèles sont remplacées par des valeurs appropriées pour la réponse demandée.
4. Aucune page d'événement n'est générée.
5. La page d'événement générée s'affiche.

Pour plus d'informations sur les relations entre les identificateurs de page et les fichiers modèles, reportez-vous à la rubrique «Identificateurs de page et fichiers modèle».

Identificateurs de page et fichiers modèle

Un identificateur de page spécifie un événement et chaque événement correspond à un ou plusieurs *fichiers modèle*. Certains identificateurs de page sont propres à la spécification (par exemple, SAML 1.x), tandis que d'autres sont généraux. Pour modifier les éléments (texte, graphiques, etc.) de la page affichée pour un événement, vous devez modifier le fichier modèle ou copier un fichier modèle, utiliser la copie en tant que base d'un nouveau fichier, puis mapper l'événement vers ce nouveau fichier.

Identificateurs de page généraux et fichiers modèles correspondants

Tableau 133. Identificateurs de page généraux et fichiers modèles correspondants

Identificateur de page (événement)	Description	Fichier modèle
/proper/errors/noprotdet	Affiché lorsque le protocole est inconnu	/proper/errors/noprotdet.html
/proper/errors/missing_component	Affiché lorsque le protocole est inconnu	/proper/errors/ missingcomponent.html
/proper/errors/protocol_error	Affiché lorsqu'un module de protocole émet une exception	/proper/errors/protocol_error.html
/proper/errors/need_authentication	S'affiche lorsque les informations initiales d'URL sont introuvables dans la session utilisateur.	/proper/errors/ need_authentication.html
/proper/errors/access_denied	S'affiche lors d'un refus d'accès.	/proper/errors/access_denied.html
/proper/errors/missing-initial-url.html	S'affiche lorsque les informations initiales d'URL sont introuvables dans la session utilisateur.	/proper/errors/allerror.html
/proper/errors/unauth-access-to-waspoc-delegate.html	S'affiche lorsqu'un accès au protocole de délégation du point de contact WebSphere a eu lieu sans authentification appropriée.	/proper/errors/allerror.html
/proper/login/formlogin.html	Affiché lors de l'utilisation de l'authentification par formulaires. **Avertissement :** Ne modifiez pas la valeur d'action et les noms de paramètre de la page POST. Ils doivent rester inchangés pour que la page fonctionne correctement.	/proper/login/formlogin.html

Tableau 133. Identificateurs de page généraux et fichiers modèles correspondants (suite)

Identificateur de page (événement)	Description	Fichier modèle
/proper/login/formloginerror.html	Affiché quand une erreur se produit lors de l'utilisation du fichier formlogin.html. Pour plus d'informations, voir «Personnalisation du formulaire de connexion», à la page 80.	/proper/login/formloginerror.html
/proper/genericpoc/ login_success.html	S'affiche lorsque l'implémentation du point de contact générique effectue une connexion avec succès sans adresse URL cible.	/proper/login/login_success.html
/proper/waspoc/login_success.html	S'affiche lorsque l'implémentation du point de contact WebSphere effectue une connexion avec succès sans adresse URL cible.	/proper/login/login_success.html
/proper/waspoc/login_failure.html	S'affiche lorsqu'une erreur se produit lors d'une connexion via l'implémentation de point de contact WebSphere.	/proper/login/login_failure.html

Identificateurs de page SAML 1.x et fichiers modèles correspondants

Tableau 134. Identificateurs de page SAML 1.x et fichiers modèles correspondants

Identificateur de page (événement)	Description	Fichier modèle
/saml/invalid_request.html	Indique qu'une requête n'est pas valide.	/saml/allerror.html
/saml/unknown_sp.html	Indique qu'un fournisseur de services inconnu a été détecté.	/saml/allerror.html
/saml/unknown_ip.html	Indique qu'un fournisseur d'identité inconnu a été détecté.	/saml/allerror.html
/saml/invalid_ip_request.html	Indique qu'un fournisseur d'identité est à l'origine d'une requête non valide.	/saml/allerror.html
/saml/unauth_user.html	Indique que l'utilisateur en question ne s'est pas authentifié.	/saml/allerror.html
/saml/cannot_exchange_for_sp.html	Indique la présence d'une erreur lors de l'échange de jeton.	/saml/allerror.html
/saml/no_ip_post_page.html	Indique que le fournisseur d'identité n'a pas de page POST.	/saml/allerror.html
/saml/no_return_token.html	Indique qu'aucun jeton de retour n'est présent.	/saml/allerror.html
/saml/ip_post_to_sp.html	Affiche la page HTML POST lorsque le fournisseur d'identité envoie la réponse SAML au fournisseur de services.	/saml/allerror.html
/saml/invalid_response.html	Indique qu'un message de réponse non valide a été détecté.	/saml/allerror.html
/saml/ip_response_invalid.html	Indique que la réponse du fournisseur d'identité n'est pas valide.	/saml/allerror.html

Tableau 134. Identificateurs de page SAML 1.x et fichiers modèles correspondants (suite)

Identificateur de page (événement)	Description	Fichier modèle
/saml/ cannot_exchange_for_resource.html	Indique la présence d'une erreur lors de l'échange de jeton.	/saml/allerror.html
/saml/missing_context_attribute.html	Indique que l'attribut de contexte requis est absent.	/saml/allerror.html
/saml/ missing_config_parameter.html	Indique qu'un élément de configuration SPS requis est absent.	/saml/allerror.html
/saml/ could_not_retrieve_assertion.html	Indique que le fournisseur de services n'a pas pu extraire l'assertion de la réponse ou du canal de retour SOAP.	/saml/allerror.html
/saml/ could_not_perform_local_auth.html	Indique la présence d'une erreur lors du renvoi de l'en-tête EAI.	/saml/allerror.html
/saml/ could_not_create_signed_request.html	S'affiche lorsque la génération d'une requête d'assertion SAML est impossible.	/saml/allerror.html
/saml/sp_missing_target.html	S'affiche au niveau du fournisseur de services si la requête initiale adressée au noeud final WAYF ne contient pas de paramètre TARGET.	/saml/allerror.html
/saml/ error_parsing_soap_response.html	Indique la présence d'une erreur lorsque le fournisseur de services essaie d'extraire l'assertion du noeud final SOAP du fournisseur d'identité.	/liberty/ error_parsing_soap_response.html
/saml/unknown_ip_wayf.html	S'affiche lorsque le cookie WAYF contient un ID de fournisseur d'identité qui n'est pas configuré sur la fédération.	/saml/allerror.html

Identificateurs de page SAML 2.0 et fichiers modèles correspondants

Tableau 135. Identificateurs de page SAML 2.0 et fichiers modèles correspondants

Identificateur de page	Description	Fichiers modèles
/saml20/error_building_msg.html	Utilisé en cas d'erreur de génération des messages SAML 2.	/saml20/error_building_msg.html
/saml20/ error_missing_config_param.html	S'affiche lorsqu'un paramètre de configuration invalide est détecté pendant l'exécution.	/saml20/ error_missing_config_param.html
/saml20/error_sending_msg.html	S'affiche en cas d'erreur d'envoi des messages SAML 2.	/saml20/error_sending_msg.html
/saml20/error_validating_msg.html	S'affiche en cas d'erreur de validation de messages SAML 2.	/saml20/error_validating_msg.html
/saml20/error_validating_art.html	S'affiche en cas d'erreur de validation des artefacts SAML 2.	/saml20/error_validating_art.html
/saml20/invalid_msg.html	S'affiche en cas d'erreur de validation de messages SAML 2.	/saml20/invalid_msg.html
/saml20/invalid_art.html	S'affiche en cas d'erreur de validation des artefacts SAML 2.	/saml20/invalid_art.html

Tableau 135. Identificateurs de page SAML 2.0 et fichiers modèles correspondants (suite)

Identificateur de page	Description	Fichiers modèles
/saml20/authn_failed.html	S'affiche en cas d'échec de l'authentification SAML 2.	/saml20/authn_failed.html
/saml20/logout_failed.html	S'affiche en cas d'échec de la déconnexion.	/saml20/logout_failed.html
/saml20/art_exchange_failed.html	S'affiche en cas d'échec de l'échange d'un artefact SAML contre une réponse.	/saml20/art_exchange_failed.html
/saml20/nimgmt_update_failed.html	S'affiche en cas d'échec de la mise à jour de la gestion des identificateurs de nom.	/saml20/nimgmt_update_failed.html
/saml20/ nimgmt_terminate_failed.html	S'affiche en cas d'échec de l'arrêt de la gestion des identificateurs de nom.	/saml20/ nimgmt_terminate_failed.html
/saml20/ error_validating_msg_signature.html	S'affiche en cas d'erreur de validation de signatures de messages SAML 2.	/saml20/ error_validating_msg_signature.html
/saml20/error_decrypting_msg.html	S'affiche en cas d'erreur de déchiffrement de messages SAML 2.	/saml20/error_decrypting_msg.html
/saml20/error_parsing_msg.html	S'affiche en cas d'erreur d'analyse syntaxique des messages SAML 2.	/saml20/error_parsing_msg.html
/saml20/error_parsing_art.html	S'affiche en cas d'erreur d'analyse d'artefacts SAML 2.	/saml20/error_parsing_art.html
/saml20/invalid_init_msg.html	S'affiche en cas d'erreur de validation de messages SAML 2.	/saml20/invalid_init_msg.html
/saml20/ error_validating_init_msg.html	S'affiche en cas d'erreur de validation de messages SAML 2.	/saml20/ error_validating_init_msg.html
/saml20/logout_success.html	S'affiche en cas de succès de la déconnexion.	/saml20/logout_success.html
/saml20/logout_partial_success.html	S'affiche en cas de succès de la déconnexion partielle.	/saml20/logout_partial_success.html
/saml20/ nimgmt_terminate_success.html	S'affiche en cas de succès de l'arrêt de la gestion des identificateurs de nom.	/saml20/ nimgmt_terminate_success.html
/saml20/ nimgmt_update_success.html	S'affiche en cas de succès de la mise à jour de la gestion des identificateurs de nom.	/saml20/ nimgmt_update_success.html
/saml20/consent_to_federate.html	S'affiche pour demander l'accord de l'utilisateur pour une fédération.	/saml20/consent_to_federate.html
/saml20/saml_post_artifact.html	S'affiche pour l'envoi d'artefacts SAML 2.0 pour les profils POST.	/saml20/saml_post_artifact.html
/saml20/saml_post_request.html	S'affiche pour l'envoi de requêtes SAML 2.0 pour les profils POST.	/saml20/saml_post_request.html
/saml20/saml_post_response.html	S'affiche pour l'envoi de réponses SAML 2.0 pour les profils POST.	/saml20/saml_post_response.html
/saml/ could_not_create_signed_request.html	S'affiche lorsque la génération d'une requête d'assertion SAML est impossible.	/saml/allerror.html
/saml/sp_missing_target.html	Utilisé au niveau du fournisseur de services si la requête initiale adressée au noeud final WAYF ne contient pas de paramètre TARGET.	/saml/allerror.html

Identificateurs de page Liberty

Tableau 136. Identificateurs de page Liberty

Identificateur de page	Description
/liberty/error_parsing_soap_response.html	Indique que la réponse SOAP n'a pas pu être analysée
/liberty/fed-terminate-success.html	Indique que la résiliation a abouti
/liberty/lib-cant-modify-alias.html	Indique que la modification d'alias a échoué
/liberty/lib-fed-consent.html	Envoyé pour demander l'accord de l'utilisateur pour une fédération
/liberty/lib-fed-post-request.html	Formulaire utilisé pour envoyer une requête d'authentification
/liberty/lib-fed-post.html	Formulaire utilisé pour envoyer une réponse
/liberty/lib-internal-error-page.html	Envoyé en cas d'erreur si aucune autre message ne peut être envoyé
/liberty/lib-ipi-consent.html	Permet de demander l'accord de l'utilisateur pour une présentation du fournisseur d'identité aux fournisseurs de services
/liberty/lib-ipi-post.html	Signale la réussite de la présentation de fournisseur d'identité
/liberty/lib-login-failed-page.html	Inutilisé actuellement.
/liberty/lib-logout-failed-page.html	Envoyé à l'utilisateur par le fournisseur d'identité en cas d'échec de la déconnexion pour une raison ou pour une autre
/liberty/lib-logout-page.html	Indique à l'utilisateur destinataire toutes les résiliations de session après déconnexion
/liberty/lib-logout-success-page.html	Envoyé à l'utilisateur par le fournisseur d'identité pour signaler que la déconnexion a abouti
/liberty/logoutFailure.gif	Image indiquant l'échec de la déconnexion si la technique de déconnexion unique HTTP GET est utilisée
/liberty/logoutSuccess.gif	Image indiquant la réussite de la déconnexion si la technique de déconnexion unique HTTP GET est utilisée
/liberty/lib-message-timestamp-failure.html	Envoyé si le temps d'émission dépasse la plage autorisée
/liberty/lib-no-fed-exists.html	Envoyé lorsqu'aucune fédération n'existe
/liberty/lib-no-liberty-assertion.html	Indique que la réponse ne comporte aucune assertion
/liberty/lib-no-local-login.html	Indique l'échec de la connexion locale
/liberty/lib-no-service-available.html	Indique l'absence de service d'alias ou d'assertion
/liberty/lib-register-name-identifier-success.html	Indique que l'enregistrement d'un identificateur de nom a abouti
/liberty/lib-request-id-not-matching-resp.html	Indique qu'une réponse ne correspond à aucune requête connue
/liberty/lib-sig-validation-failure.html	Inutilisé actuellement.
/liberty/lib-version-mismatch.html	Inutilisé actuellement.

Tableau 136. Identificateurs de page Liberty (suite)

Identificateur de page	Description
/pages/itfim/wayf/wayf-html.html	Réponse WAYF HTML

Identificateurs de page WS-Federation

Tableau 137. Identificateurs de page WS-Federation

Identificateur de page	Description
/wsfederation/ cannot_exchange_for_resource.html	Indique que la requête WS-Trust du fournisseur d'identité a échoué sur le fournisseur de services.
/wsfederation/cannot_exchange_for_sp.html	Indique que le fournisseur d'identité n'a pas pu échanger de jeton pour le fournisseur de services.
/wsfederation/cannot_local_auth.html	Indique que le fournisseur de services ne peut pas valider de jeton.
/wsfederation/invalid_ip_response.html	Indique que le fournisseur de services n'a pas compris une réponse du fournisseur d'identité.
/wsfederation/invalid_request.html	Il ne s'agit pas d'une requête WS-Federation.
/wsfederation/invalid_sp_request.html	Indique qu'une requête n'est pas valide.
/wsfederation/ip_post_to_sp.html	WS-Federation l'utilise pour l'envoi d'informations du fournisseur d'identité au fournisseur de services.
/wsfederation/no_ip_post_page.html	Indique que le fournisseur d'identité n'a pas de page d'affichage.
/wsfederation/no_return_token.html	Indique que le fournisseur d'identité n'a pas pu trouver de jeton à renvoyer au fournisseur de services.
/wsfederation/signout_cleanup_failed.html	Inutilisé actuellement.
/wsfederation/ signout_cleanup_failed_no_auth.html	Utilisé lorsque la déconnexion WS-Federation a échoué parce qu'un utilisateur n'a pas été authentifié.
/wsfederation/signout_cleanup_to_sp.html	Le processus de déconnexion unique de WS-Federation l'utilise pour déclencher des déconnexions uniques sur les fournisseurs de services.
/wsfederation/signout_successful.html	Utilisé lorsque la déconnexion unique WS-Federation a abouti.
/wsfederation/sp_ip_returned_fault.html	Indique que le fournisseur d'identité a renvoyé une erreur au fournisseur de services.
/wsfederation/unauth_user.html	Indique que l'utilisateur n'a pas été authentifié sur ce fournisseur d'identité.
/wsfederation/unknown_ip_wayf.html	Indique que le fournisseur de services n'a pas pu déterminer le fournisseur d'identité.
/wsfederation/unknown_sp.html	Indique que le fournisseur de services est inconnu de ce fournisseur d'identité.

Identificateurs de page indépendants de bas niveau

Tableau 138. Identificateurs de page indépendants

Identificateur de page	Description
/proper/errors/cannot_process	Utilisé pour les erreurs internes non spécifiées
/proper/errors/missing_component	Affiché lorsque le protocole est inconnu
/proper/errors/noprotdet	Affiché lorsque le protocole est inconnu
/proper/errors/not_started	Utilisé lorsque le service SPS n'est pas en cours d'exécution, ce qui indique généralement une erreur de configuration quelconque
/proper/errors/protocol_error	Affiché lorsqu'un module de protocole émet une exception
/pages/itfim/wayf/error-no-ips.html	Signale qu'aucun fournisseur d'identité n'est présent et qu'aucun traitement WAYF ne peut donc être effectué
/pages/itfim/wayf/error-missing-template.html	Utilisé lorsque le programme ne trouve aucun modèle de page WAYF
/pages/itfim/wayf/error-invalid-template.html	Utilisé lorsque le modèle de page WAYF n'est pas valide
/pages/itfim/wayf/wayf-html.html	Affiché lorsqu'une fédération a plusieurs fournisseurs d'identité et que le paramètre de chaîne de requête ITFIM_WAYF_IDP ou le cookie WAYF n'est pas présent.

Emplacement des fichiers modèle

Par défaut, les fichiers modèles sont stockés dans le répertoire suivant :

AIX

`/usr/IBM/FIM/pages/`*`environnement_local`*`/`

HP-UX, Linux ou Solaris

`/opt/IBM/FIM/pages/`*`environnement_local`*`/`

Windows

`C:\Program Files\IBM\FIM\pages\`*`environnement_local`*`\`

Le sous-répertoire de l'environnement local est spécifique à chaque région géographique ou environnement linguistique des fichiers modèle. Le répertoire de l'environnement local par défaut est intitulé `C` et tous les fichiers sont en anglais. Si un module de langue a été installé, des environnements locaux supplémentaires sont disponibles.

Les fichiers modèles sont publiés depuis leurs sous-répertoires par défaut vers les répertoires de WebSphere Application Server. Voir «Publication des mises à jour», à la page 515.

Avertissement : Si vous avez besoin de modifier les fichiers modèle, effectuez la modification sur le serveur Tivoli Federated Identity Manager. *Ne modifiez pas* les fichiers dans les répertoires de WebSphere Application Server.

Contenu des fichiers modèle

Les fichiers modèles HTML peuvent contenir des macros qui sont remplacées par des informations spécifiques au contexte qui sont extraites lorsque la page de réponse est générée et renvoyée. Si votre fichier modèle contient, par exemple, la macro `@EXCEPTION_MSG@`, un message d'exception est inclus dans la page de réponse.

La présence d'une macro dans un fichier modèle ne garantit pas l'affectation d'une valeur réelle à la macro lors de la génération de la page de réponse. Une valeur doit être définie pour la macro lors de l'élaboration de la page, afin que la macro puisse renvoyer une valeur.

Lors de la personnalisation d'un fichier modèle HTML, utilisez uniquement les macros définies dans le fichier modèle. Si vous ajoutez de nouvelles macros dans le fichier modèle, les valeurs des macros ajoutées ne sont pas renvoyées lors de la génération de la page de réponse définitive.

Les macros utilisent le format suivant :

```
@MACRO@
```

Où *MACRO* représente le nom de la macro, par exemple, `@EXCEPTION_MSG@`

Les macros suivantes sont utilisées dans les fichiers modèle.

Tableau 139. Macros utilisées dans les fichiers modèles

Macro de substitution	Description abrégée
@ACTION@	L'action correspond à l'adresse URL vers laquelle le formulaire contenant la réponse POST sera envoyé. Utilisée dans un réponse POST HTML envoyée par un fournisseur d'identité à un navigateur pour une demande de service de protocole de connexion unique.
@CAUSE@	Informations relatives à la cause de l'erreur.
@DETAIL@	Informations supplémentaires relatives à une erreur ou une exception qui s'est produite dans le cadre du traitement d'une requête. Dans la mesure où du texte supplémentaire n'est pas toujours disponible, même si la macro @DETAIL@ est utilisée dans un fichier modèle HTML, il n'y a aucune garantie que les macros fournissent du texte supplémentaire concernant l'exception.
@EXCEPTION_MSG@	Message de texte décrivant une exception qui s'est produite lors du traitement d'une requête.
@EXCEPTION_STACK@	Pile complète d'une exception qui s'est produite lors du traitement d'une requête.
@FEDERATION_DISPLAY@	Nom de la fédération actuelle, c'est-à-dire celle qui est en cours d'utilisation.
@FEDERATION_ID@	Identificateur unique de la fédération actuelle.
@PARTNER_ID@	Protocole de connexion unique de fédération d'un partenaire de la fédération.
@REQ_ADDR@	Adresse IP (Internet Protocol) du noeud final qui a demandé une action de fédération.

Tableau 139. Macros utilisées dans les fichiers modèles (suite)

Macro de substitution	Description abrégée
@RESPONSE@	Utilisée dans une réponse POST HTML d'un fournisseur d'identité, remplacée par la réponse SAML.
@SAMLSTATUS@	Collection des valeurs d'état SAML reçues au cours du traitement d'une action de connexion unique.
@SOAP_ENDPOINT@	Adresse URL du noeud final SOAP servant à extraire l'assertion au moyen d'un artefact SAML.
@TARGET@	Permet de fournir la cible de fournisseur de services dans un réponse POST HTML envoyée par un fournisseur d'identité à un navigateur pour une demande de service de protocole de connexion unique.
@TIMESTAMP@	Valeur de l'heure en cours.
@TOKEN:form_action@	Adresse URL vers laquelle le formulaire contenant le message POST est envoyé lors d'une liaison POST.
@TOKEN:IPDisplayName@	Nom unique du fournisseur d'identité.
@TOKEN:IPProviderID@	Identificateur unique du fournisseur d'identité.
@TOKEN:PartnerID@	Identificateur unique du partenaire.
@TOKEN:RelayState@	Valeur RelayState du protocole SAML.
@TOKEN:SamlMessage@	Message SAML codé en base 64 et envoyé dans un formulaire.
@TOKEN:SPDisplayName@	Nom unique du fournisseur de services.
@TOKEN:SPProviderID@	Identificateur unique du fournisseur de services.
@TOKEN:UserName@	Nom de l'utilisateur authentifié qui a soumis l'action de connexion unique.
@WAYF_FEDERATION_DISPLAY_NAME@	Nom affiché de la fédération en cours, comme présenté dans la console. Utilisée dans une page présentant une demande d'authentification WAYF (Where Are You From : D'où venez-vous) et demandant à un utilisateur de choisir un fournisseur d'identité.
@WAYF_FEDERATION_ID@	Identificateur de la fédération en cours dans le fichier de configuration. Utilisée dans une page présentant une demande d'authentification WAYF et demandant à un utilisateur de choisir un fournisseur d'identité.
@WAYF_FORM@	Informations d'identification relatives au formulaire WAYF HTML qui est présenté à un utilisateur pour acquérir des informations de fournisseur d'identité dans une action SPS, où le fournisseur d'identité du demandeur n'a pas encore été déterminé (il ne figure pas encore dans le cookie présenté).
@WAYF_FORM_ACTION@	Noeud final du service de protocole de connexion unique ; il doit s'agir de l'adresse initialement demandée (URL). Utilisée dans une page présentant une demande d'authentification WAYF et demandant à un utilisateur de choisir un fournisseur d'identité.
@WAYF_FORM_METHOD@	Méthode HTTP utilisée dans une demande qui a donné lieu à un formulaire WAYF sur une page qui invite l'utilisateur à entrer les informations relatives au fournisseur d'identité. La méthode peut être GET, POST ou HEAD.

Tableau 139. Macros utilisées dans les fichiers modèles (suite)

Macro de substitution	Description abrégée
@WAYF_FORM_PARAM_ID@	Identificateur du paramètre de formulaire pour le fournisseur d'identité en cours ; il s'agit généralement du nom de cookie configuré. Utilisée dans une page présentant une demande d'authentification WAYF et demandant à un utilisateur de choisir un fournisseur d'identité.
@WAYF_HIDDEN_NAME@	Nom d'un des paramètres initiaux d'une demande qui donne lieu à un formulaire WAYF ; cette macro est utilisée dans une page qui invite l'utilisateur à entrer les informations relatives au fournisseur d'identité.
@WAYF_HIDDEN_VALUE@	Valeur d'un des paramètres initiaux d'une demande qui donne lieu à un formulaire WAYF ; cette macro est utilisée dans une page qui invite l'utilisateur à entrer les informations relatives au fournisseur d'identité.
@WAYF_IP_DISPLAY_NAME@	Nom affiché configuré du fournisseur d'identité en cours dans une page présentant une demande d'authentification WAYF.
@WAYF_IP_ID@	ID configuration du fournisseur d'identité en cours dans une page présentant une demande d'authentification WAYF.

Modèle de page pour la page WAYF

La page WAYF (Where Are You From) est utilisée au niveau du fournisseur de service. Elle permet aux utilisateurs de sélectionner leur fournisseur d'identité si plusieurs d'entre eux sont configurés dans la fédération.

Lorsqu'un utilisateur arrive au niveau d'un fournisseur de service, un identificateur WAYF peut être envoyé via un cookie ou un paramètre de chaîne de requête avec la demande. L'ID d'entité du fournisseur d'identité est stocké en tant que valeur du cookie ou du paramètre de chaîne de requête. Si le cookie d'identificateur WAYF ou le paramètre de chaîne de requête n'est pas présent, la page WAYF s'affiche.

Voici un exemple d'URL incluant le paramètre de chaîne de requête pour WAYF :

```
https://sp.host.com/FIM/sps/samlfed/saml20/
logininitial?RequestBinding=HTTPRedirect&ResponseBinding
=HTTPPost&ITFIM_WAYF_IDP=https://idp.host.com/FIM/sps/samlfed/saml20
```

Cet exemple est destiné à une URL de connexion unique SAML 2.0. Le nom du paramètre de chaîne de requête est `ITFIM_WAYF_IDP`. La valeur de l'ID de fournisseur d'identité est `https://idp.host.com/FIM/sps/samlfed/saml20`.

La page WAYF demande à l'utilisateur d'indiquer sa provenance. Si l'utilisateur n'est plus connecté au fournisseur d'identité, il est invité à se connecter. Selon les attributs analysés, le fournisseur de service peut accorder ou refuser l'accès au service.

Les pages de modèle sont stockées par défaut dans le répertoire suivant :

<FIM_Install_Dir>`/pages/`*<locale>*`/pages/itfim/wayf`

Voir «Identificateurs de page indépendants de bas niveau», à la page 508 pour plus d'informations sur les modèles de pages WAYF.

Les administrateurs peuvent utiliser cette page sans modifications, mais peuvent dans certains cas souhaiter modifier le style du code HTML pour répondre aux exigences spécifiques de leur environnement de déploiement.

Ce fichier modèle prend en charge plusieurs macros de remplacement :

@WAYF_FORM_ACTION@
Cette macro est remplacée par le noeud final de la requête originale. Cette macro n'appartient pas à la section répétable.

@WAYF_FORM_METHOD@
Cette macro est remplacée par la méthode HTTP de la requête originale. Cette macro n'appartient pas à la section répétable.

@WAYF_FORM_PARAM_ID@
Cette macro est remplacée par l'ID utilisé par l'action pour le fournisseur d'identité. Cette macro est répétée une fois pour chaque fournisseur d'identité.

@WAYF_IP_ID@
Cette macro est remplacée par l'ID unique du fournisseur d'identité. Cette macro est répétée une fois pour chaque fournisseur d'identité.

@WAYF_IP_DISPLAY_NAME@
Cette macro est remplacée par le nom d'affichage configuré du fournisseur d'identité. Cette macro est répétée une fois pour chaque fournisseur d'identité.

@WAYF_HIDDEN_NAME@
Cette macro est remplacée par le nom du paramètre masqué. Cette macro est répétée une fois pour chaque paramètre de requête original, puis elle est masquée.

@WAYF_HIDDEN_VALUE@
Cette macro est remplacée par la valeur du paramètre masqué. Cette macro est répétée une fois pour chaque paramètre de requête original, puis elle est masquée.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">

<!--
Le modèle html wayf présente les choix sous forme de boutons radio.
-->
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
        <title>Where are you from</title>
    </head>
    <body style="background-color:#ffffff">
        <div>
            <!--
            Insert the federation ids here just so we can show some tokens
            [RPT federations]
                @WAYF_FEDERATION_ID@
                @WAYF_FEDERATION_DISPLAY_NAME@
            [ERPT federations]
            -->
            <form id="wayfForm" name="wayfForm"
                    action="@WAYF_FORM_ACTION@" method="@WAYF_FORM_METHOD@">
                <div>
                    <table>

                    [RPT ips]
                        <tr>
                            <td>
                                <input type="radio" id="@WAYF_FORM_PARAM_ID@"
                                    name="@WAYF_FORM_PARAM_ID@"
                                    value="@WAYF_IP_ID@"/>@WAYF_IP_DISPLAY_NAME@
                            </td>
                        </tr>
                    [ERPT ips]

                    </table>
                    <!-- the hidden inputs must be present -->

                    [RPT hidden]
                    <input type="hidden" name="@WAYF_HIDDEN_NAME@"
                        id="@WAYF_HIDDEN_NAME@"
                        value="@WAYF_HIDDEN_VALUE@"/ >
                    [ERPT hidden]

                </div>
                <input type="submit" name="submit" value="Submit" />
            </form>
        </div>
    </body>
</html>
```

Figure 55. Modèle de page wayf-html.html

Modification ou création des fichiers modèles

Pour personnaliser la présentation des pages d'événement, vous pouvez modifier les fichiers modèles ou en créer de nouveaux.

Avant de commencer

Avant de poursuivre cette procédure, assurez-vous de maîtriser le mode de génération des pages d'événement. Voir «Génération des pages d'événement», à la page 501.

Pourquoi et quand exécuter cette tâche

Avertissement : Modifiez les fichiers modèles dans le répertoire du serveur Tivoli Federated Identity Manager (selon la description ci-dessous). Une fois toutes les modifications terminées, publiez-les dans le répertoire de référentiel de configuration WebSphere Application Server. *N'éditez pas* ces fichiers dans le référentiel de configuration.

Pour modifier ou créer des fichiers modèles, procédez comme suit :

Procédure

1. Sélectionnez les pages d'événement que vous souhaitez modifier. Reportez-vous à la liste des événements et aux fichiers modèles correspondants dans la rubrique «Identificateurs de page et fichiers modèle», à la page 502.
2. Arrêtez le poste WebSphere Application Server sur lequel le composant d'exécution est installé. Exécutez la commande stopServer. Pour plus d'informations, consultez le centre de documentation de WebSphere.
3. Recherchez le fichier modèle qui correspond à la page d'événement que vous souhaitez modifier, ou effectuez une copie d'un fichier modèle existant et utilisez-la pour générer un nouveau fichier. Les fichiers modèles sont situés dans un sous-répertoire de l'environnement local spécifique au lieu géographique ou à la langue, sous le répertoire du fichier. Le sous-répertoire de l'environnement local par défaut est intitulé `C` et tous les fichiers sont en anglais. Si un module de langue a été installé, des environnements locaux supplémentaires sont disponibles. Vous pouvez également créer vos propres paramètres nationaux, comme décrit à la rubrique «Création d'un environnement local de page», à la page 515. Le répertoire par défaut contenant les fichiers modèles est le suivant :

   AIX
   `/usr/IBM/FIM/pages/`*`locale`*`/`

   HP-UX, Linux ou Solaris
   `/opt/IBM/FIM/pages/`*`environnement_local`*`/`

   Windows
   `C:\Program Files\IBM\FIM\pages\`*`locale`*`\`
4. Utilisez un éditeur de texte pour modifier ou créer des fichiers.
5. Sauvegardez les fichiers à l'emplacement approprié, c'est-à-dire par exemple dans le même répertoire que celui dans lequel vous les avez copiés ou édités.

Que faire ensuite

Une fois que vous avez terminé cette étape, poursuivez la publication des fichiers dans le référentiel de configuration, selon la procédure décrite dans la section «Publication des mises à jour», à la page 515.

Publication des mises à jour

Une fois l'ensemble des mises à jour et ajouts effectués dans les fichiers modèles, vous devez publier les fichiers dans le référentiel de configuration, afin de permettre leur affichage.

Pourquoi et quand exécuter cette tâche

Pour publier des mises à jour de pages d'événements, procédez comme suit :

Procédure

1. Connectez-vous à la console de gestion.
2. Dans la console, cliquez sur **Tivoli Federated Identity Manager → Gestion des domaines → Pages d'événements**.
3. Localisez les événements que vous souhaitez mapper avec les pages nouvelles ou actualisées.
4. Dans la page **Page HTML affichée** de chaque événement que vous modifiez, indiquez le chemin d'accès et le nom de fichier que vous souhaitez utiliser pour cet événement.
5. Cliquez sur **Valider**. Un message d'avertissement s'affiche pour vous indiquer que vous devez publier les fichiers mis à jour dans le référentiel de configuration.
6. Cliquez sur **Publier les pages** afin de publier immédiatement les modifications. Sinon, cliquez sur **Fermer** et, lorsque vous serez prêt à publier le moment venu, cliquez sur **Gestion de domaines → Gestion des noeuds d'exécution** et, dans le panneau Gestion des noeuds d'exécution, cliquez sur le bouton **Publier les pages**.

Création d'un environnement local de page

Les fichiers modèles utilisés pour générer des pages d'événement sont situés dans un sous-répertoire de l'environnement local spécifique au lieu géographique ou à la langue, sous le répertoire du fichier. Le sous-répertoire de l'environnement local par défaut est intitulé `C` et tous les fichiers sont en anglais. Des paramètres nationaux, ainsi que les langues correspondantes, sont également disponibles. En outre, vous pouvez créer votre propre environnement local.

Avant de commencer

Avant de poursuivre cette procédure, assurez-vous de maîtriser le mode de génération des pages d'événement. Voir «Génération des pages d'événement», à la page 501.

Pourquoi et quand exécuter cette tâche

Pour créer votre propre environnement local, procédez comme suit :

Procédure

1. Connectez-vous à la console de gestion.
2. Dans la console, cliquez sur **Tivoli Federated Identity Manager → Gestion des domaines → Pages d'événements**. Le panneau Pages d'événement s'affiche.
3. Cliquez sur l'onglet **Environnement local de page** pour ouvrir le panneau correspondant.

4. Cliquez sur **Créer**. Un élément de liste représentant une marque de réservation est ajouté à la liste des environnements locaux de page, caractérisé par le nom **locale** et le répertoire principal **page_root**.
5. Entrez une abréviation d'environnement local pour remplacer la valeur **locale**.
6. Entrez le nom de répertoire de l'environnement local à la place de la valeur **page_root**.
7. Cliquez sur **Appliquer** ou sur **OK**. Un message d'avertissement s'affiche pour vous indiquer que vous devez publier les fichiers mis à jour dans le référentiel de configuration.
8. Cliquez sur **Publier** afin de publier immédiatement les modifications. Sinon, cliquez sur **Fermer** et, lorsque vous serez prêt à publier le moment venu, cliquez sur **Gestion de domaines → Gestion des noeuds d'exécution** et, dans le panneau Gestion des noeuds d'exécution, cliquez sur le bouton **Publier les pages**.

Suppression d'un environnement local sur une page

Vous pouvez supprimer n'importe quel environnement local de page autre que l'environnement C par défaut installé en même temps que Tivoli Federated Identity Manager.

Pourquoi et quand exécuter cette tâche

La suppression d'un environnement local de page empêche l'affichage des pages dans cet environnement.

Procédure

1. Connectez-vous à la console de gestion.
2. Dans la console, cliquez sur **Tivoli Federated Identity Manager → Gestion des domaines → Pages d'événements**. La page d'événements s'affiche.
3. Cliquez sur l'onglet **Environnement local de page** (Page Locale) pour ouvrir le panneau correspondant.
4. Dans la zone **Sélectionner**, choisissez le bouton jouxtant l'environnement local de page à supprimer. Pour obtenir une description des environnements locaux, reportez-vous à l'aide en ligne.
5. Cliquez sur **Supprimer**, puis sur **Appliquer** pour valider vos modifications et rester dans le portlet Environnement local de page, ou cliquez sur **OK** pour valider les modifications et quitter le portlet.

Personnalisation des modèles de page physique à usages multiples

Dans certains cas, vous serez amené à personnaliser des modèles de page physique désignés par plusieurs identificateurs de page.

Pourquoi et quand exécuter cette tâche

Certains modèles de page physique sont désignés par plusieurs identificateurs de page dans le fichier `sps.xml`.

Par exemple : `<sps:PageIdentifierMapping name="/liberty/error_parsing_soap_response.html" location="/liberty/error_parsing_soap_response.html" />` et `<sps:PageIdentifierMapping name="/saml/error_parsing_soap_response.html" location="/liberty/error_parsing_soap_response.html" />`

Si les réponses SAML et Liberty doivent être différentes, vous devez modifier les pages comme suit :

Procédure

1. Pour chaque environnement local affecté, copiez la page Liberty dans le répertoire SAML.
2. Modifiez les deux pages selon vos besoins.
3. Modifiez la seconde expression PageIdentifierMapping comme suit :
   ```
   <sps:PageIdentifierMapping name="/saml/error_parsing_soap_response.html"
   location="/saml/error_parsing_soap_response.html"/>
   ```
4. Propagez ces modifications (voir «Publication des mises à jour», à la page 515).

Personnalisation de l'accord pour fédérer la page pour SAML 2.0

Une *page Accord de fédération* est un formulaire HTML qui invite l'utilisateur à donner son accord pour rejoindre une fédération. Vous pouvez personnaliser la *page Accord de fédération* pour indiquer les informations demandées à un utilisateur.

Avant de commencer

Déterminez les valeurs que vous souhaitez utiliser pour la page d'accord de fédération. Voir A propos de cette tâche pour une liste de valeurs.

Pourquoi et quand exécuter cette tâche

Lorsqu'un utilisateur accède à une fédération, il donne son accord pour la rejoindre. Le formulaire HTML `consent_to_federate.html` invite à donner cet accord. Vous pouvez personnaliser ce que le formulaire demande en ajoutant des valeurs d'accord. Ces valeurs indiquent la manière dont un utilisateur accepte de rejoindre une fédération et si les fournisseurs de service sont informés de cet accord. Les fournisseurs d'identité reçoivent les valeurs d'accord dans la réponse SAML 2.0.

Les valeurs suivantes déterminent la manière dont un utilisateur rejoint une fédération :

1 Un utilisateur accepte de rejoindre une fédération sans informer le fournisseur de service.

0 Un utilisateur refuse de rejoindre une fédération

Une valeur URI
Un URI peut indiquer si l'utilisateur accepte de rejoindre une fédération et si vous souhaitez informer le fournisseur de service de l'accord. La table suivante répertorie et décrit les valeurs d'URI prises en charge.

Tableau 140. Valeurs d'accord prises en charge pour la réponse SAML 2.0

Valeur d'accord	URI	Description
Non spécifié	`urn:oasis:names:tc: SAML:2.0:consent: unspecified`	L'accord de l'utilisateur n'est pas spécifié.
Obtenu	`urn:oasis:names:tc: SAML:2.0:consent: obtained`	Indique que l'accord de l'utilisateur est acquis par l'émetteur du message.
Précédent	`urn:oasis:names:tc: SAML:2.0:consent: prior`	Indique que l'accord de l'utilisateur est acquis par l'émetteur du message avant l'action qui a initié le message.

Tableau 140. Valeurs d'accord prises en charge pour la réponse SAML 2.0 (suite)

Valeur d'accord	URI	Description
Implicite	`urn:oasis:names:tc: SAML:2.0:consent: current-implicit`	Indique que l'accord de l'utilisateur est acquis de manière implicite par l'émetteur du message au lancement de ce dernier.
Explicite	`urn:oasis:names:tc: SAML:2.0:consent: current-explicit`	Indique que l'accord de l'utilisateur est acquis de manière explicite par l'émetteur du message lors de l'instance à laquelle le message a été envoyé.
Non disponible	`urn:oasis:names:tc: SAML:2.0:consent: unavailable`	Indique que l'émetteur du message n'a pas pu obtenir l'accord de l'utilisateur.
Inapplicable	`urn:oasis:names:tc: SAML:2.0:consent: inapplicable`	Indique que l'émetteur du message n'a pas besoin d'obtenir ou rapporter l'accord de l'utilisateur.

Suivez les étapes suivantes pour personnaliser l'accord de fédération :

Important : Modifiez les fichiers modèles sur le serveur Tivoli Federated Identity Manager. Une fois que toutes les modifications sont terminées, vous pouvez les publier dans le répertoire de référentiel de configuration WebSphere® Application Server. **N'éditez pas** ces fichiers dans le référentiel de configuration.

Procédure

1. Utilisez la commande `stopServer` pour arrêter WebSphere Application Server où Tivoli Federated Identity Manager est installé. Pour plus d'informations, voir le centre de documentation de WebSphere.
2. Utilisez un éditeur de texte pour accéder à `consent_to_federate.html`.

   Les fichiers modèles sont situés dans un sous-répertoire de l'environnement local spécifique au lieu géographique ou à la langue. Tous les fichiers sont en anglais. Si vous avez installé un module de langue, des environnements locaux supplémentaires sont disponibles. Le répertoire par défaut dépend du système d'exploitation.

   AIX® `/usr/IBM/FIM/pages/locale/saml20/`

   HP-UX, Linux® ou Solaris
   `/opt/IBM/FIM/pages/locale/saml20/`

   Windows®
   `C:\Program Files\IBM\FIM\pages\locale\saml20\`
3. Ajoutez les valeurs d'accord appropriées pour votre fédération. Voir A propos de cette tâche pour une liste complète des valeurs.
4. Sauvegardez les fichiers à l'emplacement approprié. Il peut s'agir du répertoire dans lequel vous les avez modifiés.
5. Redémarrez WebSphere Application Server.

Exemple

L'exemple suivant présente une URI ajoutée avec une valeur d'accord `Obtenu`:

```
<input type="radio" checked name="Consent"
value="urn:urn:oasis:names:tc:SAML:2.0:consent:obtained"/>
Consent Obtained.br/>
```

Dans cet exemple, l'accord de l'utilisateur est acquis par l'émetteur du message.

Que faire ensuite

Publiez les fichiers dans le référentiel de configuration. Voir «Publication des mises à jour», à la page 515.

Chapitre 42. Développement d'un serveur point de contact personnalisé

Le serveur point de contact de votre environnement Tivoli Federated Identity Manager représente la première entité qui traite une requête visant à accéder à une ressource. Vous pouvez choisir l'une des options fournies pour un serveur point de contact, ou créer un serveur point de contact personnalisé.

Pourquoi et quand exécuter cette tâche

Un serveur point de contact personnalisé est constitué de plusieurs modules de rappel personnalisés d'ouverture qui définissent les paramètres d'ouverture de session, de fermeture de session, d'ID local et d'authentification. Un serveur point de contact personnalisé peut constituer le choix approprié pour votre environnement si vous souhaitez intégrer une application d'authentification ou de gestion d'accès Web existante à Tivoli Federated Identity Manager. Un serveur point de contact personnalisé peut s'avérer utile dans les situations suivantes :

- Si vous disposez d'un cookie de connexion unique existant, qui est utilisé sur l'ensemble de l'entreprise, vous pouvez mettre en oeuvre un serveur point de contact personnalisé utilisant un rappel SignIn qui définit le cookie du domaine de connexion unique conformément à votre stratégie de connexion unique.
- Si vous disposez d'un logiciel de gestion d'accès Web qui expose une interface API personnalisée en vue de certifier l'identité d'un utilisateur dans l'environnement, ou d'extraire l'utilisateur actuel pour les besoins de la requête. Vous pouvez mettre en oeuvre un serveur point de contact qui exécute un un rappel d'identité local (afin d'extraire l'utilisateur lié à la transaction), ou mettre en oeuvre un serveur point de contact personnalisé utilisant un rappel SignIn pour certifier l'identité d'un utilisateur dans l'environnement, ou bien mettre en oeuvre un serveur point de contact qui exploite ces deux types de rappel.

La mise au point d'un serveur point de contact personnalisé nécessite une certaine expérience dans la programmation de modules de rappel, ainsi qu'une bonne connaissance des concepts de programmation de Tivoli Federated Identity Manager. Consultez les liens des documents developerWorks dans le centre de documentation à l'adresse http://publib.boulder.ibm.com/infocenter/tiv2help/index.jsp.

Une fois le travail de développement terminé, vous devez effectuer l'intégration de la solution à votre environnement Tivoli Federated Identity Manager en procédant comme suit :

Procédure

1. Publiez les plug-ins de rappel dans le module d'exécution Tivoli Federated Identity Manager. Voir «Publication des plug-ins de rappel», à la page 522.
2. Rassemblez les paramètres nécessaires pour la configuration de chacun des modules de rappel.
3. Créez un nouveau profil de serveur point de contact. Vous avez la possibilité de créer un profil nouveau, ou de réutiliser un profil existant comme base de votre nouveau profil de serveur point de contact. Voir, au choix :
   - «Création d'un nouveau serveur point de contact», à la page 522

- «Création d'un serveur point de contact comme un serveur existant», à la page 525

4. Activez le serveur point de contact. Voir «Activation d'un serveur point de contact», à la page 526.

Publication des plug-ins de rappel

Si vous avez développé les modules pour un serveur point de contact personnalisé, vous devez publier leurs plug-ins pour pouvoir les utiliser dans votre environnement Tivoli Federated Identity Manager.

Avant de commencer

Avant de poursuivre cette tâche, vérifiez que vous avez développé les modules de rappel appropriés pour votre serveur point de contact. Pour plus d'informations, voir Chapitre 42, «Développement d'un serveur point de contact personnalisé», à la page 521.

Procédure

1. Copiez les plug-ins de rappel dans le répertoire /plugins dans lequel vous avez installé Tivoli Federated Identity Manager. Par exemple, sous Windows, il s'agit du répertoire `/opt/IBM/FIM/plugins`.
2. Connectez-vous à la console, puis cliquez sur **Tivoli Federated Identity Manager → Gestion de la configuration → Gestion des noeuds d'exécution**.
3. Le panneau Gestion des noeuds d'exécution s'affiche. Cliquez sur **Publier les plug-ins**.

Que faire ensuite

Après avoir publié les plug-ins, vous pouvez poursuivre avec la création du profil de point de contact.

Création d'un nouveau serveur point de contact

Tivoli Federated Identity Manager fournit plusieurs options pour chaque serveur point de contact, suivant le rôle que vous tenez dans la fédération. De plus, vous avez la possibilité de développer votre propre serveur point de contact. Si vous avez développé votre propre serveur, vous devez l'ajouter à votre environnement via la console.

Avant de commencer

Avant d'ajouter le serveur point de contact personnalisé à votre environnement, vous devez :

- Publier chaque point personnalisé des plug-ins de rappel de contact sur le noeud d'exécution. Voir «Publication des plug-ins de rappel».
- Connaître le type de paramètres à utiliser, le cas échéant, et les valeurs correspondantes qui doivent être transmises à ces rappels.

Pourquoi et quand exécuter cette tâche

La procédure qui suit explique comment ajouter un serveur point de contact personnalisé autre que les serveurs point de contact déjà définis dans votre environnement. Si vous ajoutez un serveur point de contact personnalisé similaire

à un autre serveur, appliquez la procédure de la rubrique «Création d'un serveur point de contact comme un serveur existant», à la page 525.

Procédure

1. Connectez-vous à la console. Cliquez sur **Tivoli Federated Identity Manager** → **Gestion de la configuration** → **Point de contact**.
2. uliquez sur **Créer**. Le panneau Bienvenue de l'assistant Serveur point de contact s'affiche.
3. Vérifiez que vous avez exécuté les étapes prérequises. Cliquez ensuite sur **Suivant**. Le panneau Nom de profil s'affiche.
4. Indiquez le nom de profil de votre serveur point de contact personnalisé et, le cas échéant, une description. Cliquez sur **Suivant**. Le panneau Ouverture de session s'affiche.
5. Dans le panneau Ouverture de session, vous devez spécifier les rappels d'ouverture de connexion à utiliser, l'ordre dans lequel ces rappels doivent être lancés, ainsi que les paramètres appliqués à chaque rappel.
   a. Sélectionnez une entrée dans la liste **Rappels disponibles**. Cliquez sur **Ajouter** pour incorporer l'entrée à la liste **Rappels utilisés**. Répétez cette étape afin d'ajouter tous les rappels dont vous avez besoin pour le serveur point de contact.
   b. Cliquez sur le bouton **Ajouter des paramètres**. Une section relative aux paramètres de rappel s'affiche pour chaque rappel figurant dans la liste Rappels utilisés. Des zones de paramètres comportant les valeurs par défaut `new key` et `new value` s'affichent.
   c. Ajoutez les paramètres de chaque rappel en remplaçant le nom et la valeur par défaut par les paramètres que vous souhaitez ajouter. Pour ajouter d'autres paramètres, cliquez sur **Créer**. Lorsque vous cliquez sur **Créer**, une nouvelle zone de paramètre contenant les valeurs par défaut est ajoutée à la liste des paramètres.
   d. Répétez les étapes précédentes jusqu'à ce que tous les paramètres aient été ajoutés à tous les rappels.
6. Cliquez sur **Suivant**. Le panneau Fermeture de session s'affiche.
7. Dans le panneau Fermeture de session, vous devez spécifier les rappels de fermeture de connexion à utiliser, l'ordre dans lequel ces rappels doivent être lancés, ainsi que les paramètres appliqués à chaque rappel.
   a. Sélectionnez une entrée dans la liste **Rappels disponibles**. Cliquez sur **Ajouter** pour incorporer l'entrée à la liste **Rappels utilisés**. Répétez cette étape afin d'ajouter tous les rappels dont vous avez besoin pour le serveur point de contact.
   b. Cliquez sur le bouton **Ajouter des paramètres**. Une section relative aux paramètres de rappel s'affiche pour chaque rappel figurant dans la liste Rappels utilisés. Des zones de paramètres comportant les valeurs par défaut `new key` et `new value` s'affichent.
   c. Ajoutez les paramètres de chaque rappel en remplaçant le nom et la valeur par défaut par les paramètres que vous souhaitez ajouter. Pour ajouter d'autres paramètres, cliquez sur **Créer**. Lorsque vous cliquez sur **Créer**, une nouvelle zone de paramètre contenant les valeurs par défaut est ajoutée à la liste des paramètres.
   d. Répétez les étapes précédentes jusqu'à ce que tous les paramètres aient été ajoutés à tous les rappels.
8. Cliquez sur **Suivant**. Le panneau ID local s'affiche.

9. Dans le panneau ID local, vous devez spécifier les rappels d'ID locaux à utiliser, l'ordre dans lequel ces rappels doivent être lancés, ainsi que les paramètres appliqués à chaque rappel.
   a. Sélectionnez une entrée dans la liste **Rappels disponibles**. Cliquez sur **Ajouter** pour incorporer l'entrée à la liste **Rappels utilisés**. Répétez cette étape afin d'ajouter tous les rappels dont vous avez besoin pour le serveur point de contact.
   b. Cliquez sur le bouton **Ajouter des paramètres**. Une section relative aux paramètres de rappel s'affiche pour chaque rappel figurant dans la liste Rappels utilisés. Des zones de paramètres comportant les valeurs par défaut `new key` et `new value` s'affichent.
   c. Ajoutez les paramètres de chaque rappel en remplaçant le nom et la valeur par défaut par les paramètres que vous souhaitez ajouter. Pour ajouter d'autres paramètres, cliquez sur **Créer**. Lorsque vous cliquez sur **Créer**, une nouvelle zone de paramètre contenant les valeurs par défaut est ajoutée à la liste des paramètres.
   d. Répétez les étapes précédentes jusqu'à ce que tous les paramètres aient été ajoutés à tous les rappels.
10. Cliquez sur **Suivant**. Le panneau Authentification s'affiche.
11. Dans le panneau Authentification, vous devez spécifier les rappels de fermeture de session, l'ordre dans lequel ces rappels doivent être lancés, ainsi que les paramètres appliqués à chaque rappel.
   a. Sélectionnez une entrée dans la liste **Rappels disponibles**. Cliquez sur **Ajouter** pour incorporer l'entrée à la liste **Rappels utilisés**. Répétez cette étape afin d'ajouter tous les rappels dont vous avez besoin pour le serveur point de contact.
   b. Cliquez sur le bouton **Ajouter des paramètres**. Une section relative aux paramètres de rappel s'affiche pour chaque rappel figurant dans la liste Rappels utilisés. Des zones de paramètres comportant les valeurs par défaut `new key` et `new value` s'affichent.
   c. Ajoutez les paramètres de chaque rappel en remplaçant le nom et la valeur par défaut par les paramètres que vous souhaitez ajouter. Pour ajouter d'autres paramètres, cliquez sur **Créer**. Lorsque vous cliquez sur **Créer**, une nouvelle zone de paramètre contenant les valeurs par défaut est ajoutée à la liste des paramètres.
   d. Répétez les étapes précédentes jusqu'à ce que tous les paramètres aient été ajoutés à tous les rappels.
12. Cliquez sur **Suivant**. Le panneau Récapitulatif s'affiche. Ce panneau affiche la liste de tous les rappels et des paramètres que vous avez spécifiez au cours des étapes précédentes.
13. Cliquez sur **Terminer** pour achever la configuration, ou sur **Précédent** pour revenir aux panneaux précédents et passer en revue vos sélections.

Que faire ensuite

Pour rendre ce serveur point de contact actif, poursuivez avec les instructions de la rubrique «Activation d'un serveur point de contact», à la page 526.

Création d'un serveur point de contact comme un serveur existant

Tivoli Federated Identity Manager fournit plusieurs options pour chaque serveur point de contact, suivant le rôle que vous tenez dans la fédération. De plus, vous avez la possibilité de développer votre propre serveur point de contact et de le baser sur un serveur existant. Si vous avez développé votre propre serveur, vous devez l'ajouter à votre environnement via la console.

Avant de commencer

Avant d'ajouter le serveur point de contact personnalisé à votre environnement, vous devez :

- Publier chaque point personnalisé des plug-ins de rappel de contact sur le noeud d'exécution. Voir «Publication des plug-ins de rappel», à la page 522.
- Connaître le type de paramètres à utiliser, le cas échéant, et les valeurs correspondantes qui doivent être transmises à ces rappels.

Pourquoi et quand exécuter cette tâche

La procédure qui suit explique comment ajouter un serveur point de contact personnalisé tel que les serveurs point de contact déjà définis dans votre environnement. Si vous ajoutez un serveur point de contact personnalisé différent d'un autre serveur, appliquez la procédure de la rubrique «Création d'un nouveau serveur point de contact», à la page 522.

Procédure

1. Connectez-vous à la console. Cliquez sur **Tivoli Federated Identity Manager** → **Gestion de la configuration** → **Point de contact**.
2. Sélectionnez le serveur point de contact existant à utiliser comme base pour votre nouveau serveur point de contact.
3. Cliquez sur **Création à l'identique**. Le panneau Bienvenue de l'assistant Serveur point de contact s'affiche.
4. Vérifiez que vous avez exécuté les étapes prérequises. Cliquez ensuite sur **Suivant**. Le panneau Nom de profil s'affiche et les informations issues du profil sur lequel vous basez votre nouveau serveur point de contact s'affichent.
5. Indiquez le nom de profil de votre serveur point de contact personnalisé et, le cas échéant, une description. Cliquez sur **Suivant**. Le panneau Ouverture de session s'affiche.
6. Dans le panneau Ouverture de session, vous devez spécifier les rappels d'ouverture de connexion à utiliser, l'ordre dans lequel ces rappels doivent être lancés, ainsi que les paramètres appliqués à chaque rappel. Etant que vous avez sélectionné un profil pour servir de base à ce serveur point de contact, les rappels et paramètres affichés pour ce profil seront identiques à ceux en cours d'utilisation. Si vous devez ajouter ou supprimer des rappels, utilisez les boutons **Ajouter** et **Supprimer**. Les rappels indiqués dans la liste Rappels utilisés sont ceux qui seront repris par votre nouveau serveur point de contact.
7. Cliquez sur **Suivant**. Le panneau Fermeture de session s'affiche.
8. Dans le panneau Fermeture de session, vous devez spécifier les rappels d'ouverture de connexion à utiliser, l'ordre dans lequel ces rappels doivent être lancés, ainsi que les paramètres appliqués à chaque rappel. Etant que vous avez sélectionné un profil pour servir de base à ce serveur point de

contact, les rappels et paramètres affichés pour ce profil seront identiques à ceux en cours d'utilisation. Si vous devez ajouter ou supprimer des rappels, utilisez les boutons **Ajouter** et **Supprimer**. Les rappels indiqués dans la liste Rappels utilisés sont ceux qui seront repris par votre nouveau serveur point de contact.

9. Cliquez sur **Suivant**. Le panneau ID local s'affiche.
10. Dans le panneau ID local, vous devez spécifier les rappels d'ouverture de session à utiliser, l'ordre dans lequel ces rappels doivent être lancés, ainsi que les paramètres appliqués à chaque rappel. Etant que vous avez sélectionné un profil pour servir de base à ce serveur point de contact, les rappels et paramètres affichés pour ce profil seront identiques à ceux en cours d'utilisation. Si vous devez ajouter ou supprimer des rappels, utilisez les boutons **Ajouter** et **Supprimer**. Les rappels indiqués dans la liste Rappels utilisés sont ceux qui seront repris par votre nouveau serveur point de contact.
11. Cliquez sur **Suivant**. Le panneau Authentification s'affiche.
12. Dans le panneau Authentification, vous devez spécifier les rappels d'ouverture de session, l'ordre dans lequel ces rappels doivent être lancés, ainsi que les paramètres appliqués à chaque rappel. Etant que vous avez sélectionné un profil pour servir de base à ce serveur point de contact, les rappels et paramètres affichés pour ce profil seront identiques à ceux en cours d'utilisation. Si vous devez ajouter ou supprimer des rappels, utilisez les boutons **Ajouter** et **Supprimer**. Les rappels indiqués dans la liste Rappels utilisés sont ceux qui seront repris par votre nouveau serveur point de contact.
13. Cliquez sur **Suivant**. Le panneau Récapitulatif s'affiche. Ce panneau affiche la liste de tous les rappels et des paramètres que vous avez spécifiez au cours des étapes précédentes.
14. Cliquez sur **Terminer** pour achever la configuration, ou sur **Précédent** pour revenir aux panneaux précédents et passer en revue vos sélections.

Que faire ensuite

Pour rendre ce serveur point de contact actif, poursuivez avec les instructions de la rubrique «Activation d'un serveur point de contact».

Activation d'un serveur point de contact

Pour faire d'un serveur point de contact le serveur actif de votre environnement, vous devez l'activer.

Procédure

1. Connectez-vous à la console. Cliquez sur **Tivoli Federated Identity Manager** → **Gestion de la configuration** → **Point de contact**.
2. Sélectionnez le serveur point de contact à activer.
3. Cliquez sur **Activer**. L'élément sélectionné est activé et devient le serveur point de contact de votre environnement.

Chapitre 43. Personnalisation des paramètres des certificats de signature X.509

Lors de la signature de messages ou d'assertions, le certificat X.509 (clé publique) est inclus dans votre signature sous forme de certificat X.509 codé en base 64. Toutefois, vous avez la possibilité de définir s'il convient d'exclure ces données et/ou d'inclure des données complémentaires à vos signatures.

Avant de commencer

Avant d'appliquer cette procédure, vous devez avoir procédé à la configuration de votre fédération. En outre, si vous êtes un fournisseur d'identité dans une fédération SAML 1.x, la configuration de vos paramètres de signature d'assertions a lieu au moment où vous ajoutez vos fournisseurs de services partenaires. Pour modifier les paramètres de votre signature d'assertion, il vous faut avoir déjà configuré un fournisseur de services partenaire.

Pourquoi et quand exécuter cette tâche

Pour modifier vos paramètres de signature, procédez comme suit :

Procédure

1. Connectez-vous à la console et cliquez sur **Tivoli Federated Identity Manager** → **Configurer la configuration unique fédérée** → **Fédérations**. A l'inverse, si vous êtes un fournisseur d'identité, pour modifier vos paramètres de signature d'assertions SAML 1.x, cliquez sur **Tivoli Federated Identity Manager** → **Configurer la connexion unique fédérée** → **Partenaires**
2. Le panneau Fédérations affiche une liste de fédérations configurées. Sélectionnez une fédération. Le panneau Partenaires affiche une liste de partenaires configurés.
3. Cliquez sur **Propriétés**.
4. Sélectionnez les propriétés à modifier. Les propriétés sont décrites dans l'aide en ligne.
5. Une fois les propriétés modifiées, cliquez sur **OK** pour fermer le panneau Propriétés.

Chapitre 44. Exécution de WebSphere Application Server avec Java 2

Si vous exécutez la sécurité Java 2 sur l'instance de WebSphere Application Server sur laquelle l'identité de Tivoli Federated Identity Tivoli Federated Identity Manager est installée, vous devez modifier le fichier java.policy en vue d'autoriser l'accès aux répertoires de Tivoli Federated Identity situés dans le sous répertoire temporaire de votre profil WebSphere.

Pourquoi et quand exécuter cette tâche

Pour modifier le fichier java.policy:

Procédure

1. Localisez le fichier java.policy et ouvrez-le dans un éditeur de texte. Les emplacements par défaut du fichier sont les suivants :

   Sous AIX :
   /usr/IBM/WebSphere/AppServer/java/jre/lib/security/java.policy

   Sous HP-UX, Linux ou Solaris :
   /opt/IBM/WebSphere/AppServer/java/jre/lib/security/java.policy

   Sous Windows :
   C:\Program Files\IBM\WebSphere\AppServer

2. Ajoutez les lignes suivantes au fichier java.policy :

   ```
   grant codeBase "file:${server.root}/temp/nom_noeud/nom_serveur/
     ITFIMManagementService/-" {permission java.security.AllPermission;
   };
   grant codeBase "file:${server.root}/temp/nom_noeud/nom_serveur/
     ITFIMRuntime/-" {permission java.security.AllPermission;
   };
   ```

   nom_noeud désigne le nom du noeud, tel que IBM-FCFB36CC28ENode05

   nom_serveur désigne le nom du serveur, tel que server1

3. Sauvegardez et fermez le fichier java.policy.
4. Redémarrez WebSphere Application Server.

Partie 7. Annexes

Annexe A. Référence de tfimcfg

La commande tfimcfg peut être utilisée pour configurer les paramètres LDAP de l'installation d'Integrated Solutions Console ainsi que pour configurer WebSEAL comme serveur point de contact.

Syntaxe de tfimcfg

```
TFIM Autoconfiguration Tool version 6.1.0 [060316a]

Syntaxe : java -jar tfimcfg.jar [-action <mode>] [options]
L'outil tfimcfg présente plusieurs modes d'opération.  Chaque mode
utilise des options de ligne de commande différentes.

Configuration et suppression de la configuration de serveurs WebSEAL :
   -action tamconfig : configure un serveur WebSEAL.  Il s'agit du mode
                       par défaut.
   Options :
      -cfgfile <fichier>: fichier de configuration WebSEAL.
         Cette option est obligatoire.
      -rspfile <fichier>: fichier de réponses pour une configuration non interactive.
         Par défaut : configuration interactive

   -action tamunconfig : suppression de la configuration d'un serveur WebSEAL.
   Options :
      -cfgfile <fichier>: fichier de configuration WebSEAL.
         Cette option est obligatoire.
      -rspfile <fichier> : fichier de réponses pour la suppression non interactive
                           d'une configuration.
         Par défaut : configuration interactive

Configuration et suppression de la configuration de serveurs LDAP :
   -action ldapconfig : configure un serveur LDAP.
      -rspfile <fichier> : fichier de réponses destiné à contrôler la configuration.
   Le fichier de réponses doit être basé sur le fichier exemple
   ldapconfig.properties.  Cette option est obligatoire.

   -action ldapunconfig : supprime la configuration d'un serveur LDAP.
      -rspfile <fichier> : fichier de réponses destiné à contrôler la configuration.
Le fichier de réponses doit être basé sur le fichier exemple
ldapconfig.properties.  Cette option est obligatoire.
```

Lorsque l'outil tfimcfg est exécuté pour configurer un serveur LDAP, il crée également plusieurs comptes utilisateur. Les comptes utilisateur sont nécessaires à l'application de démonstration de connexion unique.

Lorsque vous exécutez l'outil **tfimcfg** pour configurer les comptes LDAP pour l'utilisateur de la console d'administration, vous appelez cet outil via les paramètres suivants :

```
-action ldapconfig
```

Cette action crée les comptes utilisateur de démonstration.

Restrictions de tfimcfg sous Sun Java 1.4.2.4

Certaines versions de Sun Java sont incompatibles avec tfimcfg.

L'incompatibilité provoque l'erreur suivante :

```
HPDAZ0602E Corrupted file: Insufficient information to contact Policy Server
```

L'incident se produit parce que l'interpréteur JRE de Sun ne peut pas lire les fichiers de clés générés par la commande PDJrteCfg de Tivoli Access Manager. Lorsque cette erreur se produit, utilisez une machine virtuelle Java IBM ou appliquez le dernier module de correction JRE de Sun. Si l'incident persiste après l'application du module de correction de Sun, utilisez une machine virtuelle Java IBM pour la configuration.

Référence des propriétés LDAP tfimcfg

L'utilitaire tfimcfg consulte un fichier de propriétés pour obtenir les valeurs applicables lors de la configuration d'un registre d'utilisateurs LDAP. Le fichier de propriétés contient des valeurs que vous pouvez modifier.

ldap.hostname
Nom d'hôte du serveur LDAP. Valeur par défaut : `localhost`

ldap.port
Numéro du port LDAP. Valeur par défaut : `389`

La valeur par défaut est pour la communication non SSL. Lorsque le serveur LDAP est configuré pour communiquer via SSL, le port par défaut est 636.

ldap.suffix.add
Valeur booléenne qui définit si tfimcfg ajoute des suffixes au serveur LDAP, le cas échéant. Prend uniquement en charge IBM Tivoli Directory Server versions 6.1, 6.0 et 5.2.

Valeur par défaut :

```
ldap.suffix.add=true
```

ldap.suffix.user.configuration
ldap.organization.configuration
Valeurs booléennes qui définissent si tfimcfg crée des conteneurs LDAP pour stocker les utilisateurs et groupes Tivoli Federated Identity Manager. Les utilisateurs et groupes Tivoli Federated Identity Manager sont les suivants :

- Utilisateurs et groupes du serveur Tivoli Federated Identity Manager
- Utilisateurs et groupes d'IVT (Installation Verification Tool) Tivoli Federated Identity Manager

Si vous n'avez pas besoin de ces utilisateurs et groupes ou si vous avez déjà des conteneurs LDAP que vous utiliserez pour ces utilisateurs et groupes, entrez `false` pour ces valeurs.

Lorsque ldap.organization.configuration a la valeur true, tfimcfg crée les objets LDAP `dc=exemple,dc=com`.

Valeur par défaut :

```
ldap.suffix.user.configuration=true
ldap.organization.configuration=true
```

ldap.suffix.alias.configuration
Valeur booléenne qui définit si tfimcfg crée un suffixe LDAP pour stocker les alias de connexion unique. L'alias par défaut est `cn=itfim`.

```
ldap.suffix.alias.configuration=true
```

ldap.suffix.tam.configuration
Valeur booléenne qui définit si tfimcfg crée le suffixe `secAuthority=Default` pour Tivoli Access Manager.

- Si Tivoli Access Manager est déjà configuré, entrez `false` pour cette valeur.

- Si Tivoli Access Manager n'utilise pas ce serveur LDAP, entrez `false` pour cette valeur.

```
ldap.suffix.tam.configuration=true
```

Remarque : Si le suffixe secAuthority=Default existe déjà, le programme tfimcfg ignore la valeur de la propriété ldap.suffix.tam.configuration.

ldap.fim.configuration
Valeur booléenne qui définit si tfimcfg configure LDAP pour le service d'alias Tivoli Federated Identity Manager.

Valeur par défaut : `true`.

ldap.ivt.sp.configuration
Valeur booléenne qui définit si tfimcfg crée des utilisateurs et des groupes pour le fournisseur de services dans l'application IVT (Installation Verification Tool).

Valeur par défaut : `true`.

ldap.ivt.ip.configuration
Valeur booléenne qui définit si tfimcfg crée des utilisateurs et des groupes pour le fournisseur d'identité dans l'application IVT (Installation Verification Tool).

Valeur par défaut : `true`.

ldap.modify.acls
Valeur booléenne qui définit si tfimcfg connecte les listes de contrôle d'accès appropriées au serveur LDAP. Ces listes octroient l'accès en écriture et en lecture aux administrateurs Tivoli Federated Identity Manager créés par tfimcfg.

L'outil tfimcfg connecte des listes de contrôle d'accès pour les serveurs IBM LDAP et Sun ONE. Pour les autres serveurs LDAP, vous devez connecter ces listes manuellement.

Lorsque ce paramètre est défini sur `false`, vous devez connecter les listes de contrôle d'accès manuellement.

Valeur par défaut : `true`.

ldap.admin.dn
Nom distinctif utilisé par l'administrateur de LDAP pour exécuter les demandes de liaison.

Valeur par défaut : `cn=root`

ldap.admin.password
Mot de passe de l'administrateur LDAP.

Valeur par défaut : `passw0rd`

ldap.security.enabled
Valeur booléenne qui définit si la communication avec le serveur LDAP doit utiliser SSL.

Valeur par défaut : `false`.

ldap.security.trusted.jks.filename
Nom du fichier de clés Java contenant le signataire du certificat SSL présenté par LDAP lors des communications sécurisées.

ldap.suffix.user.dn
ldap.suffix.user.name
ldap.suffix.user.attributes

ldap.suffix.user.objectclasses
Si vous voulez que tfimcfg.jar crée des conteneurs LDAP pour vos utilisateurs, vous pouvez définir ces valeurs pour commander les noms distinctifs utilisés.

Valeurs par défaut :

```
ldap.suffix.user.dn=dc=com
ldap.suffix.user.name=com
ldap.suffix.user.attributes=dc
ldap.suffix.user.objectclasses=domain
```

ldap.suffix.alias.dn
Nom distinctif à utiliser pour stocker les alias de connexion unique. La valeur de cette propriété doit commencer par `cn=`. Modifiez cette valeur lorsque vous ne voulez pas utiliser le nom distinctif par défaut.

Valeur par défaut :

```
ldap.suffix.alias.dn=cn=itfim
```

ldap.organization.dn
ldap.organization.name
ldap.organization.attributes
ldap.organization.objectclasses
Si vous voulez que tfimcfg.jar crée des conteneurs LDAP pour vos groupes, vous pouvez définir ces valeurs pour commander les noms distinctifs utilisés.

Valeurs par défaut :

```
ldap.organization.dn=dc=exemple,dc=com
ldap.organization.name=exemple
ldap.organization.attributes=dc
ldap.organization.objectclasses=domain
```

ldap.user.container.dn
ldap.group.container.dn

Noms distinctifs à utiliser pour les conteneurs des utilisateurs et des groupes.

Valeurs par défaut :

```
ldap.user.container.dn=cn=users,dc=exemple,dc=com
ldap.group.container.dn=cn=groups,dc=exemple,dc=com
```

ldap.fim.server.bind.dn
ldap.fim.server.bind.shortname
ldap.fim.server.bind.password

Nom distinctif, nom abrégé et mot de passe que l'application serveur Tivoli Federated Identity Manager utilise pour se connecter au serveur LDAP.

Valeur par défaut :

```
ldap.fim.server.bind.dn=uid=fimserver,cn=users,dc=exemple,dc=com
ldap.fim.server.bind.shortname=fimserver
ldap.fim.server.bind.password=passw0rd
```

ldap.fim.admin.group.dn
ldap.fim.admin.group.shortname

Nom distinctif et nom abrégé du groupe d'administration Integrated Solutions Console.

Valeur par défaut :

```
ldap.fim.admin.group.dn=cn=fimadmins,cn=groups,dc=exemple,dc=com
ldap.fim.admin.group.shortname=fimadmins
```

ldap.user.objectclasses
ldap.group.objectclasses

ldap.user.shortname.attributes

Valeurs des conteneurs LDAP pour les attributs user.objectclasses, group.objectclasses et user.shortname.

Valeur par défaut :

```
ldap.user.objectclasses=person,organizationalPerson,inetOrgPerson
ldap.group.objectclasses=groupOfUniqueNames
ldap.user.shortname.attributes=cn,sn,uid
```

Fichier ldapconfig.properties par défaut

Le fichier ldapconfig.properties est fourni avec le composant d'exécution et de gestion de services. Des valeurs par défaut existent pour de nombreuses propriétés.

```
ldap.hostname=localhost
ldap.port=389

# If true, new suffixes will be added to the LDAP server as needed.
# Only supported for IDS 5.2 and 6.0
ldap.suffix.add=true

# If true, data for the LDAP user suffix (dc=com, by default) will be
# created.
ldap.suffix.user.configuration=true

# If true, data for the SSO alias suffix (cn=itfim, by default) will be
# created.
ldap.suffix.alias.configuration=true

# If true, create the secAuthority=Default suffix for TAM
ldap.suffix.tam.configuration=true
ldap.fim.configuration=true
ldap.ivt.sp.configuration=true
ldap.ivt.ip.configuration=true
ldap.organization.configuration=true
ldap.modify.acls=true

ldap.admin.dn=cn=root
ldap.admin.password=passw0rd

ldap.security.enabled=false
ldap.security.trusted.jks.filename=

ldap.suffix.user.dn=dc=com
ldap.suffix.user.name=com
ldap.suffix.user.attributes=dc
ldap.suffix.user.objectclasses=domain

# DN to use for storing SSO aliases.  This must begin with cn=
ldap.suffix.alias.dn=cn=itfim

ldap.organization.dn=dc=exemple,dc=com
ldap.organization.name=exemple
ldap.organization.attributes=dc
ldap.organization.objectclasses=domain

ldap.user.container.dn=cn=users,dc=exemple,dc=com
ldap.group.container.dn=cn=groups,dc=exemple,dc=com

ldap.fim.server.bind.dn=uid=fimserver,cn=users,dc=exemple,dc=com
ldap.fim.server.bind.shortname=fimserver
ldap.fim.server.bind.password=passw0rd

ldap.fim.admin.group.dn=cn=fimadmins,cn=groups,dc=exemple,dc=com
ldap.fim.admin.group.shortname=fimadmins

ldap.user.objectclasses=person,organizationalPerson,inetOrgPerson
ldap.group.objectclasses=groupOfUniqueNames
ldap.user.shortname.attributes=cn,sn,uid
```

Figure 56. Valeurs par défaut pour le fichier ldapconfig.properties

Exemple de sortie de la configuration LDAP via tfimcfg

L'illustration suivante montre un exemple de sortie obtenu lors de l'exécution de tfimcfg.

La commande d'exécution de tfimcfg permettant de configurer les entrées LDAP pour le service d'alias et l'application de démonstration est la suivante :

```
java -jar tfimcfg.jar -action ldapconfig -rspfile
   /tmp/ldapconfig.properties
```

Voici un exemple de sortie obtenu lors de l'exécution de la commande sur un fournisseur d'identité. L'exemple utilise un fichier ldapconfig.properties contenant les valeurs par défaut.

```
Configuration du serveur LDAP.
Fournisseur du serveur LDAP : International Business Machines (IBM),
   version 6.0.
Ajout du suffixe LDAP secAuthority=Default.
Rechargement de la configuration IBM Directory Server.
Ajout du suffixe LDAP dc=com.
Rechargement de la configuration IBM Directory Server.
Création de l'objet LDAP dc=com.
Ajout du suffixe LDAP cn=itfim-cmd.
Rechargement de la configuration IBM Directory Server.
Création de l'objet LDAP cn=itfim-cmd.
Création de l'objet LDAP dc=example,dc=com.
Création de l'objet LDAP cn=users,dc=example,dc=com.
Création de l'objet LDAP cn=groups,dc=example,dc=com.
Création de l'objet LDAP uid=fimserver,cn=users,dc=example,dc=com.
Création de l'objet LDAP cn=fimadmins,cn=groups,dc=example,dc=com.
Ajout de l'utilisateur uid=fimserver,cn=users,dc=example,dc=com to group
   cn=fimadmins,cn=groups,dc=example,dc=com.
Création de l'objet LDAP o=identityprovider,dc=com.
Création de l'objet LDAP cn=MEemployee,o=identityprovider,dc=com.
Création de l'objet LDAP cn=MEmanager,o=identityprovider,dc=com.
Création de l'objet LDAP cn=MEexecutive,o=identityprovider,dc=com.
Création de l'objet LDAP cn=elain,o=identityprovider,dc=com.
Création de l'objet LDAP cn=mary,o=identityprovider,dc=com.
Création de l'objet LDAP cn=chris,o=identityprovider,dc=com.
Mise à jour des listes de contrôle d'accès IBM LDAP pour le suffixe CN=ITFIM-CMD.
Mise à jour des listes de contrôle d'accès IBM LDAP pour le suffixe
   SECAUTHORITY=DEFAULT.
Mise à jour des listes de contrôle d'accès IBM LDAP pour le suffixe DC=COM.
Mise à jour de la configuration du serveur LDAP terminée.
```

Figure 57. Exemple de sortie de tfimcfg.jar

Modification de la classe d'objets pour les utilisateurs créés via l'utilitaire tfimcfg

L'utilitaire **tfimcfg**, lorsqu'il est appelé via l'argument **-action ldapConfig**, crée un ensemble d'utilisateurs de démonstration dans LDAP. Les classes d'objet de ces utilisateurs *demo* sont toutefois incompatibles avec les paramètres de recherche par défaut de WebSphere portant sur les entrées d'utilisateur dans IBM Tivoli Directory Server. Les règles de mappage de démonstration supposent que ces utilisateurs de démonstration sont disponibles dans LDAP.

L'utilitaire **tfimcfg** crée des entrées d'utilisateur dans LDAP avec ces classes d'objets : `person,organizationalPerson,inetOrgPerson`. Toutefois, les paramètres de recherche WebSphere pour IBM Tivoli Directory Server exigent que ces entrées d'utilisateur contiennent la classe d'objets `ePerson`. En raison de cette absence de concordance entre les classes d'objets, WebSphere ne peut pas localiser ces utilisateurs de démonstration dans le registre d'utilisateurs.

Une solution palliative à ce problème consiste à modifier les classes d'objets des utilisateurs créés via l'utilitaire tfimcfg.

Pour ajouter cette classe d'objets à la liste, procédez comme suit :

1. Dans un éditeur, ouvrez le fichier ldapconfig.properties :
   ```
   /opt/IBM/FIM/tools/tamcfg/ldapconfig.properties
   ```
2. Recherchez la ligne suivante :
   ```
   ldap.user.objectclasses=person,organizationalPerson,
     inetOrgPerson
   ```
3. Modifiez la ligne comme suit :
   ```
   ldap.user.objectclasses=person,ePerson,organizationalPerson,
     inetOrgPerson
   ```
4. Invoke tfimcfg -action ldapConfig.

Pour afficher un exemple du résultat de cette modification, exécutez la commande suivante :

```
# idsldapsearch -D cn=root -w passw0rd -b dc=com uid=mary
cn=mary,o=identityprovider,dc=com
displayName=Mary Manor
mail=mmanor@identityprovider.example.com
uid=Mary
userPassword=abcd1234
objectclass=top
objectclass=person
objectclass=ePerson
objectclass=organizationalPerson
objectclass=inetOrgPerson
employeenumber=987-65-4321
sn=Manor
cn=Mary
```

Annexe B. Adresses URL pour l'initialisation d'actions de connexion unique

Les spécifications SAML ne contiennent pas ou peu d'informations sur les noeuds finals ou les méthodes que l'utilisateur final doit employer pour initier des actions de connexion unique. Toutefois, dans un environnement Tivoli Federated Identity Manager, des adresses URL sont définies afin de permettre à l'utilisateur final d'initier des actions de connexion unique.

La référence est utile pour les architectes ou développeurs d'applications qui implémentent les composants d'interaction utilisateur de leur fédération.

Remarque : Ces adresses URL ne sont pas employées pour les communications inter-partenaires. Pour plus d'informations, voir Chapitre 14, «Noeuds finals SAML et adresses URL», à la page 157.

Adresse URL initiale SAML 1.x

L'adresse URL du service de transfert inter-sites constitue le point de départ du processus de requête de connexion unique dans une fédération SAML 1.x. L'URL d'émission d'une requête de connexion unique se caractérise par la syntaxe suivante :

Syntaxe

```
https://nomhôte_fournisseur_identité:numéro_port/sps/
  nom_fédération/samlxx/login?TARGET=
  id_fournisseur_services/emplacement_application_cible
  [chaînes de requête optionnelles]
```

Eléments

https *ou* **http**
: Schéma d'URI. `https` pour les ressources qui sont protégées par SSL (Secure Socket Layer). `http` pour les ressources qui ne sont pas protégées par SSL.

nomhôte_fournisseur_identité
: Nom d'hôte du serveur point de contact du fournisseur d'identité.

numéro_port
: Numéro de port du noeud final de service de transfert inter-sites. Le valeur par défaut est 9443.

sps
: Désignation de l'instance Tivoli Federated Identity Manager Server. Cet élément ne peut pas être modifié.

nom_fédération
: Nom affecté à la fédération lorsque vous la créez.

saml*xx*
: Désignation du protocole SAML que vous choisissez d'utiliser dans votre fédération. Les valeurs peuvent correspondre à une des suivantes :
  - saml (pour SAML 1.0)
  - saml11 (pour SAML 1.1)

login Cet élément indique le type de noeud final qui utilise le port. **login** est utilisé pour le service de transfert inter-sites.

Vous devez également spécifier la chaîne de requête **TARGET** et avez la possibilité de préciser l'une ou l'autre des chaînes de requête facultatives (**SP_PROVIDER**) et (**PROTOCOL**), ou les deux, comme suit :

TARGET
Adresse URL de l'application cible à laquelle un utilisateur peut accéder via une connexion unique.

SP_PROVIDER_ID
La valeur de cette chaîne de requête indique l'ID du fournisseur de services correspondant à la cible de la demande de connexion unique. Cette chaîne de requête est facultative, mais recommandée. L'utilisation de cette chaîne de requête évite toute ambiguïté quant au fournisseur de services qui est la cible de la demande de connexion unique. Sans cette chaîne de requête, le fournisseur de services est déterminé via le mappage de l'*URI://nomhôte[:port]* de l'URL dans la chaîne de requête TARGET vers l'*URI://nomhôte[:port]* de l'ID du fournisseur de services partenaire qui est configuré pour la fédération. Ce paramètre est utilisé pour les requêtes initiées par le fournisseur d'identité.

PROTOCOL
La valeur de ce paramètre indique le type de profil de connexion unique (Artefact du navigateur ou POST du navigateur) qui doit être utilisé pour la demande de connexion unique. La syntaxe de l'extension est `PROTOCOL=[BA|POST]`, où BA correspond à 'Browser Artifact' et POST à 'Browser POST'. La chaîne de requête remplace la configuration locale du fournisseur d'identité. L'utilisation de l'extension est facultative. En l'absence d'extension, le choix du profil est déterminé par les paramètres du fichier de configuration. Pour permettre le recours à cette extension, vous devez activer le paramètre d'extension IBM PROTOCOL pendant la procédure de configuration de la création d'une fédération SAML 1.x sur un fournisseur d'identité.

Ces chaînes de requête peuvent être utilisées individuellement ou en association. Par exemple, l'URL servant à déclencher la connexion unique lorsque le paramètre SP_PROVIDER_ID est utilisé alors que l'extension PROTOCOL ne l'est pas, comporte la syntaxe suivante :

```
https://URL_service_transfert_inter-sites?SP_PROVIDER_ID=
  ID_fournisseur_services&TARGET=URL_application_cible
```

Avec le paramètre SP_PROVIDER_ID et l'extension PROTOCOL, l'URL comporte la syntaxe suivante :

```
https://URL_service_transfert_inter-sites?SP_PROVIDER_ID=
  ID_fournisseur_services&TARGET=URL_application_cible
  &PROTOCOL=[BA|POST]
```

Exemples

URL de connexion unique, sans les paramètres facultatifs :
L'exemple suivant présente l'URL de connexion unique d'un fournisseur d'identité utilisant une fédération nommée `ipfed`, le protocole SAML 1.1, un fournisseur de services dont l'ID est `https://sp.example.com:9443`, ainsi qu'une application appelée `snoop` :

```
https://idp.example.com:9443/sps/ipfed/saml11/login?TARGET=
  https://sp.example.com:9443/snoop/
```

URL de connexion unique, lorsque le paramètre SP_PROVIDER_ID et l'extension PROTOCOL *sont* utilisés :

L'exemple ci-dessous présente une URL qui sert à déclencher la connexion unique lorsque l'extension IBM PROTOCOL *est* utilisée. Dans cet exemple, même si le fournisseur d'identité est configuré pour utiliser un profil POST pour le fournisseur de services nommé sp, l'utilisation suivante de l'extension PROTOCOL force le fournisseur d'identité à utiliser le profil Artefact du navigateur :

```
https://idp.example.com:9443/sps/ipfed/saml11/login?SP_PROVIDER_ID=
  https://sp.example.com:9443/sps/spfed/saml11&TARGET=
  https://sp.example.com:9443/
  snoop&PROTOCOL=BA
```

URL de connexion unique, lorsque le paramètre SP_PROVIDER_ID est utilisé alors que l'extension PROTOCOL ne l'est *PAS* :

L'exemple suivant présente une URL qui sert à déclencher la connexion unique lorsque le paramètre SP_PROVIDER_ID est utilisé alors que l'extension IBM PROTOCOL ne l'est *PAS* :

```
https://idp.example.com:9443/sps/ipfed/saml11/login?SP_PROVIDER_ID=
  https://sp.example.com:9443/sps/spfed/saml11&TARGET=
  https://sp.example.com:9443/snoop
```

Adresses URL initiales de profil SAML 2.0

La spécification SAML 2.0 définit les noeuds finals utilisés par les communications entre partenaires, mais pas la manière dont les utilisateurs finals peuvent initier une connexion unique via ces noeuds.

Dans un environnement Tivoli Federated Identity Manager, des URL spécifiquement formatées, incorporant l'action de connexion unique à entreprendre, la liaison à utiliser pour l'action, ainsi que l'emplacement de l'action, peuvent être utilisées pour les actions de connexion unique lancées par les utilisateurs. Ces adresses sont appelées *URL initiales de profil*.

Les architectes et développeurs d'applications qui conçoivent et mettent en oeuvre l'interaction des utilisateurs avec le processus de connexion unique, doivent pouvoir cerner le concept des URL initiales de profil afin de les incorporer dans leurs applications Web.

Les sections suivantes décrivent le format des URL initiales de profil SAML 2.0 qui sont prises en charge dans un environnement Tivoli Federated Identity Manager.

Adresse URL initiale du service d'assertion client (fournisseur de services)

Dans une fédération SAML 2.0, les URL du service d'assertion client peuvent être initiées au niveau du site du fournisseur d'identité, ou celui du fournisseur de services. La présente rubrique décrit la syntaxe d'initiation de la connexion unique au niveau du fournisseur de services.

Syntaxe d'initialisation de connexion unique sur le fournisseur de services

```
https://nom_hôte_fournisseur:numéro_port/sps/
nom_fédération/saml20/logininitial?RequestBinding=RequestBindingType&
ResponseBinding=ResponseBindingType&
NameIdFormat=NameIDFormatType&
```

```
IsPassive=[true|false]&
ForceAuthn=[true|false]&
AllowCreate=[true|false]&
AuthnContextClassRef = ClassReference&
AuthnContextDeclRef = DeclarationReference&
AuthnContextComparison = [exact| minimum | maximum |better]&
Target=target_application_location
```

Eléments

https *ou* **http**
Schéma d'URI. `https` pour les ressources qui sont protégées par SSL (Secure Socket Layer). `http` pour les ressources qui ne sont pas protégées par SSL.

nom_hôte_fournisseur
Le nom d'hôte du serveur point de contact du fournisseur.

numéro_port
Numéro de port du noeud final de service de transfert inter-sites. Le valeur par défaut est 9443.

sps Désignation de l'instance Tivoli Federated Identity Manager Server. Cet élément ne peut pas être modifié.

nom_fédération
Nom affecté à la fédération lorsque vous la créez.

saml20
Désignation de la fédération SAML 2.0.

logininitial
Cet élément indique le type de noeud final qui utilise le port. Le paramètre **logininital** initialise le service de connexion unique.

Les chaînes de requête suivantes doivent également être utilisées dans l'adresse URL :

RequestBinding
Liaison utiliser pour envoyer la requête. Les valeurs admises pour l'initialisation de connexion unique sur le fournisseur de services sont les suivantes :

- HTTPPost
- HTTPArtifact
- HTTPRedirect

ResponseBinding
Liaison utilisée par l'émetteur de la réponse renvoyée. Les valeurs admises pour l'initialisation de connexion unique sur le fournisseur de services sont les suivantes :

- HTTPPost
- HTTPArtifact

Target Adresse URL de l'application à laquelle un utilisateur peut accéder via une connexion unique.

NameIdFormat
Format utilisé pour les identificateurs de nom. Les valeurs admises sont :

- Transient (anonyme)
- Persistent
- Encrypted (pour les identificateurs de noms chiffrés)

- E-mail

Le paramètre 'Persistent' est défini par défaut. Si l'attribut 'NameIdFormat' n'est pas inclus, un ID de nom persistant est spécifié.

AllowCreate
Indique si une nouvelle liaison de compte persistante est appliquée à la requête. La valeur par défaut est `true`. **Remarque :** Pour permettre l'utilisation de ce paramètre, la propriété **NameIdFormat** doit être définie sur 'Persistent'.

ForceAuthn
Indique si le fournisseur d'identité authentifie l'utilisateur ou non. Une valeur de `true` signifie que l'utilisateur doit être authentifié. La valeur par défaut est `false`.

Remarque :

- Selon la configuration de fédération, le paramètre le plus restrictif est implémenté. Par exemple, si vous définissez la configuration de fédération pour forcer un utilisateur à l'authentification, la définition de l'élément ForceAuthn sur `false` n'est pas implémentée.
- Si vous comptez utiliser la gestion de cookie WebSEAL avec SAML 2.0 ForceAuthn, assurez-vous que la liste des cookies gérés n'inclut pas le cookie de session WebSphere. Voir «Configuration de WebSEAL pour gérer les cookies», à la page 430.

IsPassive
Indique si le fournisseur d'identité doit prendre le contrôle de l'agent utilisateur si la valeur est définie sur `true`. Le fournisseur d'identité n'est pas autorisé à demander à l'utilisateur ses données d'identification de connexion.

La valeur par défaut est `false`.

Remarque : Selon la configuration de fédération, le paramètre le plus restrictif est implémenté. Par exemple, si vous définissez la configuration de fédération pour autoriser le fournisseur d'identité à prendre le contrôle de l'agent utilisateur, la définition de l'élément IsPassive `false` n'est pas implémentée.

AuthnContextClassRef
Indique une ou plusieurs valeurs de chaînes qui identifient les références URI de classe de contexte d'authentification.

Remarque : Utilisez `AuthnContextClassRef` ou `AuthnContextDeclRef`. Si les deux valeurs sont fournies, c'est la valeur `AuthnContextClassRef` qui est utilisée.

AuthnContextDeclRef
Indique une ou plusieurs valeurs de chaînes qui identifient les références URI de déclaration de contexte d'authentification.

Remarque : Utilisez `AuthnContextClassRef` ou `AuthnContextDeclRef`. Si les deux valeurs sont fournies, c'est la valeur `AuthnContextClassRef` qui est utilisée.

AuthnContextComparison

Indique le type de comparaison utilisé pour déterminer les déclarations ou classes de contexte demandées. Le type de comparaison doit être l'un des suivants :

- exact
- minimum
- maximum
- better

La valeur par défaut est exact.

Exemple

Adresse URL de connexion unique initialisée au niveau du fournisseur de services :

L'exemple suivant illustre l'adresse URL de connexion unique initialisée au niveau d'un fournisseur de service. Le nom de la fédération est `spfed`, utilisant le protocole SAML 2.0, HTTPPost en liaison de requête et de liaison de réponse, et une application cible à l'adresse https://sp.example.com:9443/banking:

```
https://sp.example.com:9443/sps/
spfed/saml20/logininitial?
RequestBinding=HTTPPost&
ResponseBinding=HTTPPost&
NameIdFormat=persistent&
IsPassive=true&
ForceAuthn=true&
AllowCreate=true&
RequestedAuthnContext Comparison=minimum&
AuthnContextClassRef=classref1&
Target=https://sp.example.com:9443/banking
```

Adresse URL initiale du service de connexion unique (fournisseur d'identité)

Dans une fédération SAML 2.0, les URL du service de connexion unique peuvent être initiées au niveau du site du fournisseur d'identité, ou celui du fournisseur de services. La présente rubrique décrit la syntaxe d'initiation du service au niveau du fournisseur d'identité.

Syntaxe d'initialisation de connexion unique sur le fournisseur d'identité

```
https://nom_hôte_fournisseur:numéro_port/sps/
  nom_fédération/saml20/logininitial?RequestBinding=RequestBindingType&
  &PartnerId=ID_fournisseur_partenaire_cible
  &NameIdFormat=NameIDFormatType&AllowCreate=[true|false]
```

Eléments

https *ou* **http**

Schéma d'URI. `https` pour les ressources qui sont protégées par SSL (Secure Socket Layer). `http` pour les ressources qui ne sont pas protégées par SSL.

nom_hôte_fournisseur

Nom d'hôte du serveur point de contact du fournisseur.

numéro_port
Numéro de port du noeud final de service de transfert inter-sites. Le valeur par défaut est 9443.

sps Désignation de l'instance Tivoli Federated Identity Manager Server. Cet élément ne peut pas être modifié.

nom_fédération
Nom affecté à la fédération lorsque vous la créez.

saml20
Désignation de la fédération SAML 2.0.

logininitial
Cet élément indique le type de noeud final qui utilise le port. Le paramètre **logininital** initialise le service de connexion unique.

L'URL doit contenir les chaînes de requête suivantes :

RequestBinding
Liaison utilisée pour envoyer la réponse au fournisseur de services. Les valeurs admises pour l'initialisation de connexion unique sur le fournisseur d'identité sont les suivantes :

- HTTPPost
- HTTPArtifact

PartnerId
ID de fournisseur du partenaire cible.

NameIdFormat
Format utilisé pour les identificateurs de nom. Les valeurs admises sont :

- Transient (anonyme)
- Persistent
- Encrypted (pour les identificateurs de noms chiffrés)
- Email

Le paramètre 'Persistent' est défini par défaut. Si l'attribut 'NameIdFormat' n'est pas inclus, un ID de nom persistant est spécifié.

AllowCreate
Indique si une nouvelle liaison de compte persistante doit être appliquée à la requête. False est la valeur par défaut. **Remarque :** Pour permettre l'utilisation de ce paramètre, la propriété **NameIdFormat** doit être définie sur 'Persistent'.

Exemple

Adresse URL de connexion unique initialisée au niveau du fournisseur d'identité :
L'exemple suivant présente l'URL de connexion unique d'un fournisseur d'identité utilisant une fédération nommée `ipfed`, le protocole SAML 2.0, HTTPPOST en tant que liaison de requête et l'ID de partenaire https://sp.example:9443/sps/saml20ip2/saml20. Si aucune valeur n'est spécifiée pour 'NameIdFormat', l'ID de nom persistant utilisé est le suivant :

```
https://idp.example.com:9443/sps/ipfed/saml20/logininitial?
  RequestBinding=HTTPPost&
  PartnerId=https://sp.example:9443/sps/saml20ip2/saml20
```

URL initiale du service SLO

Dans une fédération SAML 2.0, l'adresse URL du service SLO est utilisée par un partenaire afin de contacter le profil Single Logout. L'URL d'initialisation du service comporte la syntaxe suivante :

Syntaxe

```
https://nom_hôte_fournisseur:numéro_port/sps/
  nom_fédération/saml20/sloinitial
..?RequestBinding=RequestBindingType
```

Eléments

https *ou* **http**
Schéma d'URI. `https` pour les ressources qui sont protégées par SSL (Secure Socket Layer). `http` pour les ressources qui ne sont pas protégées par SSL.

nom_hôte_fournisseur
Nom d'hôte du serveur point de contact du fournisseur de services ou d'identité.

numéro_port
Numéro de port du noeud final de service de résolution des artefacts. La valeur par défaut est 9444.

sps Désignation du serveur Tivoli Federated Identity Manager. Cet élément ne peut pas être modifié.

nom_fédération
Nom affecté à la fédération lorsque vous la créez.

saml20
Désignation de SAML 2.0 dans votre fédération.

sloinitial
Cet élément indique le type de noeud final qui utilise le port. Le paramètre **sloinitial** initialise le service de déconnexion unique.

Les requêtes suivantes doivent également être incluses :

RequestBinding
Liaison utiliser pour envoyer la requête. Les valeurs admises sont les suivantes :

- HTTPPost
- HTTPRedirect
- HTTPArtifact
- HTTPSOAP

Exemples

Adresse URL de déconnexion unique initialisée au niveau du fournisseur de services :
L'exemple suivant illustre l'adresse URL de déconnexion unique initialisée au niveau d'un fournisseur de services au sein d'une fédération nommée `spfed`, qui utilise le protocole SAML 2.0 et le type de liaison de requête HTTPRedirect Artifact :

```
https://sp.example.com:9443/sps/spfed/saml20/sloinitial?
  RequestBinding=HTTPRedirect
```

Adresse URL de déconnexion unique initialisée au niveau du fournisseur d'identité :

L'exemple suivant illustre l'adresse URL de déconnexion unique initialisée au niveau d'un fournisseur d'identité au sein d'une fédération nommée `ipfed`, qui utilise le protocole SAML 2.0 et le type de liaison de requête HTTPArtifact :

```
https://idp.example.com:9444/sps/ipfed/saml20/sloinitial?
  RequestBinding=HTTPArtifact
```

URL initiale du service de gestion des identificateurs de nom

Dans une fédération SAML 2.0, l'adresse URL du service de gestion des identificateurs de noms est utilisée par un partenaire afin de contacter le service Name Identifier Management. L'URL d'initialisation du service comporte la syntaxe suivante :

Syntaxe

```
https://nom_hôte_fournisseur:numéro_port/sps/
  nom_fédération/mnidsinitial?RequestBinding=RequestBindingType
  &PartnerId=ID_fournisseur_partenaire_cible&NameIdTerminate=[True|False]
```

Eléments

https *ou* **http**

Schéma d'URI. `https` pour les ressources qui sont protégées par SSL (Secure Socket Layer). `http` pour les ressources qui ne sont pas protégées par SSL.

nom_hôte_fournisseur

Nom d'hôte du serveur point de contact du fournisseur de services ou d'identité.

numéro_port

Numéro de port du noeud final de service de résolution des artefacts. La valeur par défaut est 9444.

sps Désignation du serveur Tivoli Federated Identity Manager. Cet élément ne peut pas être modifié.

nom_fédération

Nom affecté à la fédération lorsque vous la créez.

saml20

Désignation de SAML 2.0 dans la fédération.

mnidsinitial

Cet élément indique le type de noeud final qui utilise le port. La propriété **mnidsinitial** est utilisée pour initialiser l'identificateur de noms.

Les chaînes de requête suivantes doivent également être incluses :

RequestBinding

Liaison utiliser pour envoyer la requête au partenaire. Les valeurs admises pour l'initialisation de connexion unique sur le fournisseur d'identité sont les suivantes :

- HTTPPost
- HTTPArtifact
- HTTPRedirect
- HTTPSOAP

PartnerId
ID de fournisseur du partenaire cible.

NameIdTerminate
Valeur qui indique si le flux de gestion des identificateurs de nom doit arrêter l'activité de mappage. Les valeurs admises sont :

True Arrête la liaison des comptes.

False Indique que le flux d'identificateurs de noms doit mettre à jour les identificateurs de noms (alias). La valeur 'False' est définie par défaut si aucune valeur explicite n'est spécifiée.

Exemples

Identificateur de nom initialisé au niveau du fournisseur d'identité :
L'exemple suivant illustre l'adresse URL de l'identificateur de noms initialisée au niveau d'un fournisseur d'identité au sein d'une fédération nommée `ipfed`, qui utilise le protocole SAML 2.0 et le type de liaison de requête HTTP SOAP :

```
https://idp.example.com:9444/sps/ipfed/saml20/mnidsinitial?
  RequestBinding=HTTPSOAP&PartnerId=https://saml20sp:444/sps/
  saml20/saml20&NameIdTerminate=true
```

Identificateur de nom initialisé au niveau du fournisseur de services :
L'exemple suivant illustre l'adresse URL de l'identificateur de noms initialisée au niveau d'un fournisseur de services au sein d'une fédération nommée `spfed`, qui utilise le protocole SAML 2.0 et le type de liaison de requête HTTP Artifact :

```
https://sp.example.com:9444/sps/spfed/saml20/mnidsinitial?
  RequestBinding=HTTPArtifact&PartnerId=https://saml20ip/FIM/sps/
  saml20/saml20&NameIdTerminate=true
```

Annexe C. Désactivation de la consignation en vue d'améliorer les performances

Lors de l'utilisation de Tivoli Federated Identity Manager avec Tivoli Access Manager, vous pouvez améliorer les performances obtenues sur un fournisseur de services en désactivation la fonction de consignation du serveur de règles Tivoli Access Manager.

Pour réduire la sollicitation de l'unité centrale (CPU), procédez comme suit :

1. Sauvegardez le répertoire de Policy Director. Par exemple, sous Linux ou UNIX :

   ```
   /opt/IBM/WebSphere/AppServer/java/jre/PolicyDirector
   ```

2. Ouvrez le fichier suivant dans un éditeur de texte:

   ```
   /opt/IBM/WebSphere/AppServer/java/jre/PolicyDirector/PDJLog.properties
   ```

3. Désactivez la consignation des messages en configurant le paramètre suivant sur la valeur 'false' :

   ```
   baseGroup.PDJMessageLogger.isLogging=false
   ```

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, un programme ou un service IBM n'implique pas que seul ce produit, programme ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Toutefois, il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM est susceptible de posséder des brevets ou des applications brevetées en attente qui couvrent le sujet décrit dans ce 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.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Pour les demandes de licence concernant les informations à deux octets (DBCS), contactez le Département des propriétés intellectuelles IBM de votre pays ou envoyez vos demandes, par courrier, à :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd
3-3-12, Roppongi, Minato-ku, Tokyo 106-8711 Japan

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun autre pays dans lequel il serait contraire aux lois locales : LE PRESENT DOCUMENT EST LIVRE «EN L'ETAT». IBM DECLINE TOUTE RESPONSABILITE, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS ET DE FACON NON LIMITATIVE, TOUTE GARANTIE IMPLICITE DE NON-CONTREFACON OU 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. Il est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Europe Middle-East Africa
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ces informations et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA IBM, 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.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp., enregistrées dans un grand nombre de juridictions partout dans le monde. Les autres noms de produits et services peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à http://www.ibm.com/legal/copytrade.shtml

Adobe, Acrobat, PostScript® ainsi que toutes les marques incluant Adobe sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

Intel®, le logo Intel, Intel Inside®, le logo Intel Inside, Intel® Centrino®, le logo Intel Centrino, Celeron®, Intel® Xeon®, Intel SpeedStep®, Itanium® et Pentium® sont des marques d'Intel Corporation ou de ses filiales aux Etats-Unis et dans certains autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT® et le logo Windows sont des marques de Microsoft Corporation aux Etats unis et/ou dans d'autres pays.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Le logo Java ainsi que toutes les marques incluant Java sont des marques de Sun Microsystems, Inc. aux Etats-Unis et/ou dans certains autres pays'.

Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.

Glossaire

artefact
Dans le contexte du protocole SAML, un objet de données structurées qui désigne un message de protocole SAML.

artefact du navigateur
Un profil (qui est en fait un ensemble de règles) basé sur la norme SAML et qui indique qu'un artefact est échangé pour établir et utiliser une session digne de confiance standard entre deux partenaires au sein d'une fédération. Par opposition au *POST du navigateur*.

assertion
Dans le contexte du protocole SAML, des données qui contiennent des informations d'authentification et/ou d'attribut dans un message.

canal de retour SOAP
Communications qui ont lieu directement entre deux noeuds finaux SOAP.

connexion unique
Processus d'authentification par lequel l'utilisateur peut accéder à plusieurs systèmes ou applications en entrant un ID utilisateur et un mot de passe uniques.

domain
Déploiement du composant d'exécution Tivoli Federated Identity Manager sur WebSphere Application Server.

fédération
Une relation dans laquelle les entités, telles que des entreprises distinctes, se mettent d'accord pour utiliser les mêmes normes techniques (comme SAML ou Liberty), ce qui permet à chaque partenaire dans la relation d'accéder aux ressources et aux données de l'autre partenaire. Voir aussi fournisseur d'identité et fournisseur de services.

fournisseur de services
Partenaire au sein d'une fédération qui fournit des services aux utilisateurs.

fournisseur d'identité
Partenaire au sein d'une fédération qui a la responsabilité d'authentifier l'identité d'un utilisateur.

gestion de la sécurité des services Web
Composant de Tivoli Federated Identity Manager utilisé pour établir et gérer les relations avec les fédérations pour les applications de service Web exécutées sur WebSphere Application Server et utilisant les jetons WS-Security.

jeton Message ou suite de bits spécifique qui indique la permission ou le contrôle temporaire relativement à l'envoi d'informations sur un réseau. Dans le contexte du protocole SAML, jeton est utilisé dans le même sens que le mot *assertion*.

liaison
Dans le contexte du protocole SAML, la méthode de communication utilisée pour transporter les messages.

mappage d'identité
Processus de modification d'une identité qui est valide dans un contexte d'entrée en une identité qui l'est dans un contexte de sortie.

métadonnées
Données décrivant une information spécifique, comme les paramètres d'une configuration par exemple.

noeud final
Le destinataire final d'une opération.

POST du navigateur
Un profil (qui est en fait un ensemble de règles) basé sur la norme SAML et qui indique qu'un formulaire à envoi automatique doit être utilisé pour établir et utiliser une session digne de confiance standard entre deux partenaires au sein d'une fédération. Par opposition à l'*artefact du navigateur*.

profil Dans le contexte de la spécification SAML, une combinaison de protocoles, d'assertions et de liaisons qui sont utilisés ensemble pour créer une fédération et activer la connexion unique fédérée.

protocol
Dans le contexte de la spécification SAML, un type de message de demande et de message de réponse utilisé pour

obtenir des données d'identification et pour gérer des identités.

SAML Voir *security assertion markup language*.

security assertion markup language
Ensemble de spécifications écrites par le consortium OASIS dans le but de décrire le traitement sécurisé des messages de demande et de réponse basés sur XML et qui contiennent des informations d'autorisation et d'authentification.

serveur point de contact
Dans le contexte d'une fédération, le serveur de proxy ou d'application qui correspond à la première entité traitant une demande d'accès à une ressource.

service consommateur d'assertion
Dans le contexte du protocole SAML, le noeud final d'une fédération qui reçoit des assertions ou des artefacts dans le cadre d'une requête ou d'une réponse à connexion unique.

service d'accréditation
Composant de Tivoli Federated Identity Manager qui gère les jetons de sécurité qui sont échangés entre les domaines de sécurité. Le service d'accréditation est également appelé *Service de jeton de sécurité*.

service d'alias
Composant de Tivoli Federated Identity Manager qui gère les alias ou les identificateurs de nom qui sont transférés entre différents domaines sécurisés.

service de résolution d'artefact
Dans le contexte du protocole SAML, le noeud final d'une fédération où les artefacts sont remplacés par des assertions.

service de transfert intersite
Dans le contexte du protocole SAML, le noeud final d'une fédération auquel une requête à connexion unique est envoyée.

service Web
Application modulaire autonome et auto-descriptive qui peut être publiée, découverte et appelée sur un réseau à l'aide de protocoles réseau standard. De manière générale, les données sont balisées au format XML, le protocole SOAP sert à transférer les données, le langage WSDL est utilisé pour décrire les services disponibles, alors que le système UDDI permet de lister les services disponibles.

Simple and Protected GSS API Negotiation Mechanism (SPNEGO)
Mécanisme d'authentification qui fournit une fonctionnalité de connexion unique dans les environnements Microsoft Windows.

SOAP Protocole XML simple conçu pour l'échange d'informations dans un environnement décentralisé et distribué. Ce protocole permet d'envoyer des demandes et de recevoir des informations ou d'appeler des services sur Internet.

SPNEGO
Simple and Protected GSS API Negotiation Mechanism

Index

D

E

F

G

H

I

J

L

M

N

P

R

S

T

U

V

W

X

GC11-6781-00