CA Identity Manager™

Configuration Guide (Manuel de configuration)

12.6.4

Support technique

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse http://www.ca.com/worldwide.

Produits CA Technologies référencés

Ce document contient des références aux produits CA suivants :

- CA Identity Manager
- CA Siteminder®
- Annuaire de listes CA
- CA User Activity Reporting
- CA Identity Governance

Table des matières

Chapitre 4: Gestion des bases de données relationnelles 103

Chapitre 5: Annuaires CA Identity Manager 157

Chapitre 1: Introduction aux environnements CA Identity Manager

Ce chapitre traite des sujets suivants :

Composants d'environnement CA Identity Manager

Un *environnement* CA Identity Manager est une vue d'un espace de noms de gestion qui permet aux administrateurs CA Identity Manager de gérer des objets, tels que des utilisateurs, des groupes et des organisations. Un ensemble de rôles et de tâches associés est affecté à ces objets. L'environnement CA Identity Manager contrôle la gestion et la présentation graphique d'un annuaire.

Un référentiel d'utilisateurs unique peut associer plusieurs environnements (page 15) CA Identity Manager pour définir différentes vues de l'annuaire. Toutefois, un environnement CA Identity Manager est associé à un seul référentiel d'utilisateurs.

Les environnements CA Identity Manager contiennent les éléments suivants :

Annuaire

Décrit un référentiel d'utilisateurs dans CA Identity Manager. L'élément annuaire inclut :

- Un pointeur vers un référentiel d'utilisateurs, qui stocke les objets gérés, tels que des utilisateurs, des groupes et des organisations
- Des métadonnées qui décrivent la méthode de stockage des objets gérés dans l'annuaire et leur représentation dans CA Identity Manager

Annuaire de provisionnement (facultatif)

Stocke des données pertinentes pour le serveur de provisionnement pour gérer des comptes supplémentaires sur des terminaux gérés. Vous pouvez associer un seul annuaire de provisionnement à un environnement.

Remarque : Pour plus d'informations sur le serveur de provisionnement ou l'annuaire de provisionnement, consultez le *Manuel d'installation*.

Console d'utilisateur

Permet aux administrateurs CA Identity Manager d'effectuer des tâches dans un environnement CA Identity Manager.

Définitions de tâches et de rôles

Définit les droits d'utilisateur dans les applications CA Identity Manager et d'autres applications. Initialement, ces définitions de tâches et de rôles sont disponibles dans l'environnement CA Identity Manager dans lequel vous pouvez les affecter à des utilisateurs.

Vous pouvez personnaliser les rôles et les tâches par défaut à l'aide de la console d'utilisateur.

Auto-administration

Permet aux utilisateurs de créer et de gérer leurs propres comptes pour accéder à des ressources, telles qu'un site Web client. L'auto-administration permet également aux utilisateurs de demander un mot de passe temporaire en cas d'oubli de leur mot de passe actuel.

Définitions de flux de travaux

CA Identity Manager inclut des définitions de flux de travaux par défaut qui automatisent l'approbation et la notification des tâches de gestion des utilisateurs, telles que la création de profils d'utilisateur ou l'affectation d'utilisateurs à des rôles ou des groupes. Vous pouvez modifier les processus de flux de travaux par défaut dans CA Identity Manager pour prendre en charge les conditions relatives à chaque entreprise.

Skins (Apparences)

Déterminez l'apparence de l'interface utilisateur CA Identity Manager.

Custom features (Fonctionnalités personnalisées)

Vous pouvez modifier CA Identity Manager pour répondre aux besoins de votre entreprise à l'aide des API CA Identity Manager. Reportez-vous au *Manuel de programmation Java*.

Chaque environnement CA Identity Manager requiert un ou plusieurs responsables du système pour personnaliser les tâches et rôles initiaux à l'aide de la console d'utilisateur. Lorsqu'un responsable du système crée les tâches et rôles initiaux, il peut accorder des droits d'administration à des utilisateurs dans cet environnement. Ces utilisateurs deviennent des administrateurs qui gèrent des utilisateurs, des groupes et des organisations. Consultez le *Manuel d'administration*.

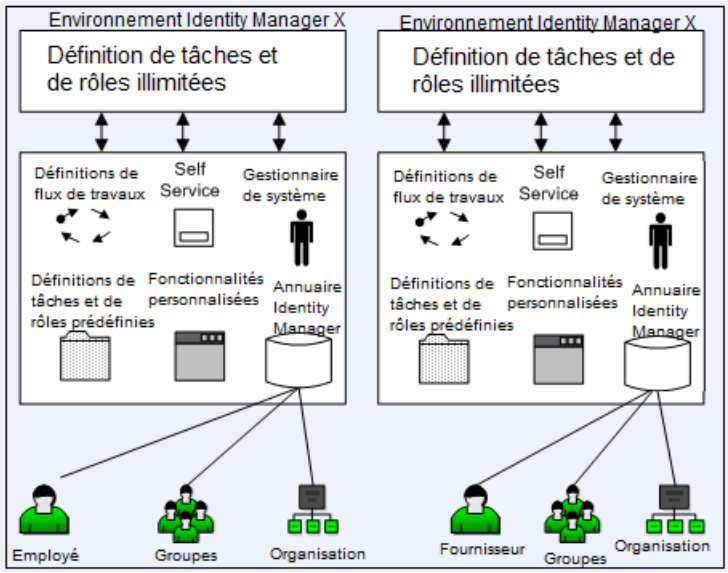
Multiple CA Identity Manager Environments (Plusieurs environnements CA Identity Manager)

Créez plusieurs environnements CA Identity Manager lorsque vous voulez :

Gérer des référentiel d'utilisateurs supplémentaires : vous pouvez gérer des utilisateurs dans différents types de référentiels d'utilisateurs. Par exemple, votre société stocke tous les profils de ses utilisateurs dans un annuaire LDAP Sun Java System. Vous créez une entreprise commune avec un partenaire qui utilise une base de données Oracle pour stocker les informations d'utilisateur et vous souhaitez utiliser un environnement CA Identity Manager différent pour chaque ensemble d'utilisateurs.

- Gérer des objets avec différentes classes d'objet LDAP : prévoyez la gestion par CA Identity Manager d'un annuaire LDAP. Dans ce même annuaire, vous pouvez gérer des objets de même type avec différentes classes d'objets et différents attributs. Par exemple, le graphique suivant illustre un annuaire qui contient deux types d'utilisateurs :
  - Des employés, qui ont un numéro d'ID d'employé
  - Des fournisseurs, identifiés par un numéro de fournisseur

Equation 1: Diagramme illustrant deux environnements Identity Manager avec des annuaires incluant des employés et des fournisseurs



Console de gestion CA Identity Manager

En tant qu'administrateur système CA Identity Manager, vos responsabilités incluent les suivantes :

- Création d'un annuaire CA Identity Manager
- Configuration d'un annuaire de provisionnement
- Configuration d'un environnement CA Identity Manager
- Affectation d'un responsable du système
- Activation des fonctionnalités personnalisées pour l'utilisation initiale

Pour configurer un environnement CA Identity Manager, utilisez la console de gestion, qui est une application Web.

La console de gestion est divisée en deux sections :

- Annuaires : utilisez cette section pour créer et gérer des annuaires CA Identity Manager et un annuaire de provisionnement, qui décrivent les référentiels d'utilisateurs dans CA Identity Manager.
- Environnements : utilisez cette section pour créer et gérer des environnements CA Identity Manager, qui contrôlent la gestion et la présentation graphique d'un annuaire.

Accès à la console de gestion CA Identity Manager

Pour accéder à la console de gestion, saisissez l'URL suivante dans un navigateur :

http://*nom_hôte:port*/iam/immanage

hostname

Définit le nom de domaine complet ou l'adresse IP du serveur sur lequel CA Identity Manager est installé.

Remarque : Si vous accédez à la console de gestion à l'aide d'Internet Explorer 7 et que le nom d'hôte inclut une adresse IPv6, la console de gestion sera incorrectement affichée. Pour éviter ce problème, utilisez le nom d'hôte complet ou une adresse IPv4.

port

Définit le port du serveur d'applications.

Remarque : Si vous utilisez un agent Web pour fournir une authentification avancée à CA Identity Manager, ne spécifiez pas de numéro de port.

Remarque : Pour accéder à la console de gestion, activez JavaScript dans le navigateur que vous utilisez.

Exemples de chemins d'accès à la console de gestion :

- Pour Geologic Weblogs :

  http://myserver.mycompany.org:7001/iam/immanage

- Pour JBoss :

  http://myserver.mycompany.org:8080/iam/immanage

- Pour WebSphere :

  http://myserver.mycompany.org:9080/iam/immanage

Création d'un environnement CA Identity Manager

Pour créer un environnement CA Identity Manager, suivez la procédure suivante dans la console de gestion :

1. Utilisez l'assistant de configuration d'annuaire (page 158) pour créer un annuaire CA Identity Manager.
2. Si votre environnement inclut le provisionnement, utilisez l'assistant de configuration d'annuaire pour créer un annuaire de provisionnement (page 173).
3. Créez un environnement CA Identity Manager.
4. Accédez à l'environnement (page 196) pour vérifier son exécution correcte.

Chapitre 2: Exemple d'environnement CA Identity Manager

Ce chapitre traite des sujets suivants :

Présentation de l'exemple d'environnement CA Identity Manager

CA Identity Manager inclut un exemple d'environnement que vous pouvez utiliser pour comprendre et tester CA Identity Manager.

L'exemple d'environnement est basé sur une société automobile appelée NeteAuto. Les administrateurs de NeteAuto utilisent CA Identity Manager pour gérer des employés, des fournisseurs et des concessions régionales.

Les configurations de référentiels d'utilisateurs pour utiliser l'exemple d'environnement NeteAuto sont les suivantes :

- Référentiels d'utilisateurs LDAP prenant en charge des organisations
- Référentiels d'utilisateurs LDAP ne prenant pas en charge les organisations
- Référentiels d'utilisateurs de base de données relationnelles prenant en charge des organisations
- Référentiels d'utilisateurs de base de données relationnelles ne prenant pas en charge les organisations

Remarque : Les fonctionnalités de provisionnement sont indisponibles, car cet environnement ne contient aucun annuaire de provisionnement.

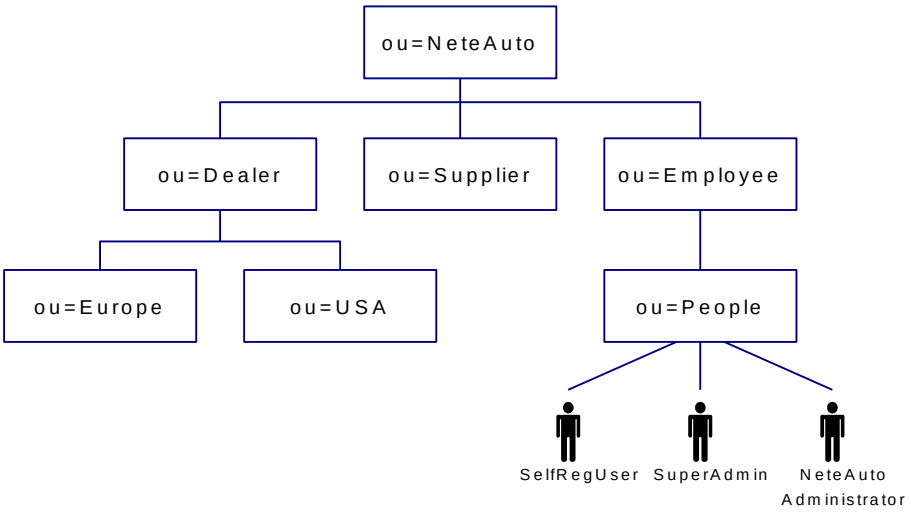
Configuration de l'exemple NeteAuto avec la prise en charge d'organisations

La configuration de l'exemple NeteAuto avec la prise en charge d'organisations implique la procédure suivante :

- Installation du logiciel requis
- Installation de l'exemple d'environnement CA Identity Manager
- Configuration d'un annuaire d'utilisateurs LDAP
- Configuration d'une base de données relationnelles
- Création d'un annuaire CA Identity Manager
- Création de l'environnement CA Identity Manager pour NeteAuto

Structure de l'annuaire LDAP pour NeteAuto

Le schéma suivant illustre les exemples d'annuaires LDAP pour NeteAuto :



L'exemple d'environnement CA Identity Manager inclut les utilisateurs suivants :

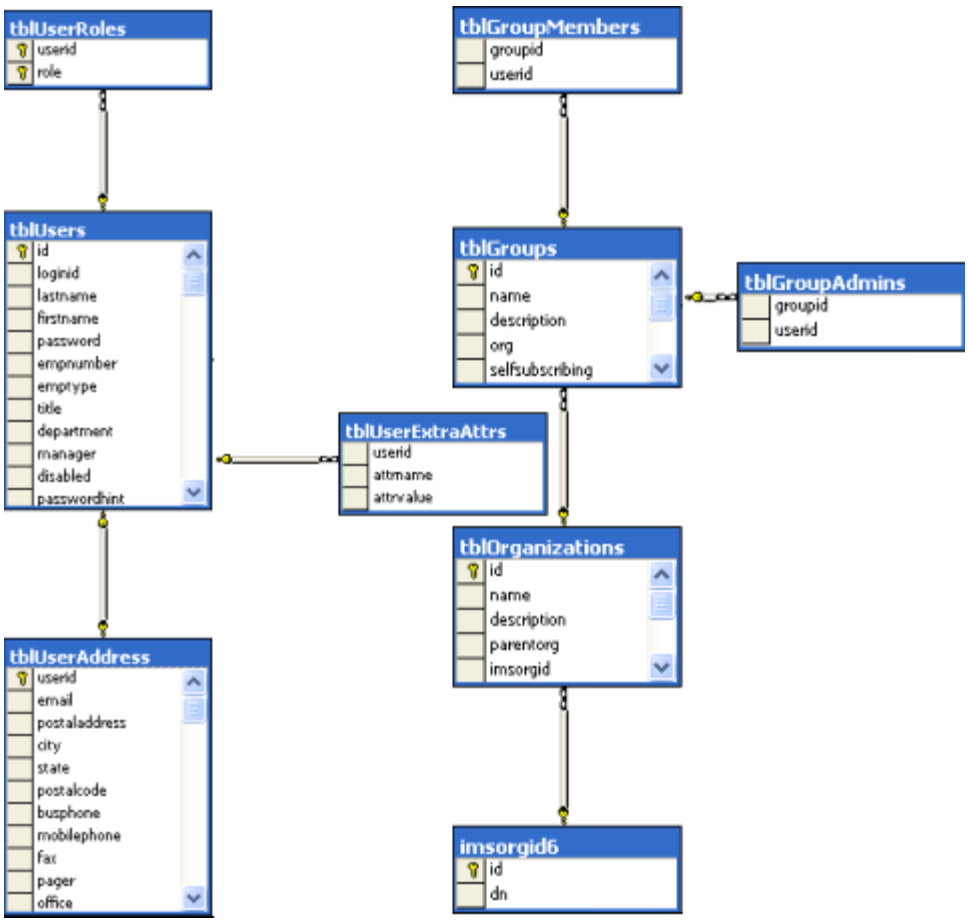
- Superadministrateur est le compte d'administrateur disposant du rôle de responsable du système pour cet environnement CA Identity Manager. Le superadministrateur peut effectuer toutes les tâches d'administration par défaut.

  Remarque : Pour obtenir une description des tâches d'administration par défaut, consultez le *Manuel d'administration*.

- SelfRegUser est le compte d'administrateur que CA Identity Manager utilise pour activer l'auto-enregistrement pour cet environnement CA Identity Manager.
- Lors de l'installation de l'environnement NeteAuto, l'administrateur NeteAuto ne dispose d'aucun droit. Toutefois, vous pouvez affecter un gestionnaire de groupes comme rôle d'utilisateur, comme décrit à la section Affectation du rôle de gestionnaire de groupes.

Base de données relationnelles pour NeteAuto

Le schéma suivant illustre la base de données relationnelles de l'exemple NeteAuto comprenant une table d'organisations :



Logiciel requis pour NeteAuto

Configuration requise pour l'environnement CA Identity Manager pour NeteAuto :

- Installez CA Identity Manager comme décrit dans le *Manuel d'installation*. Assurez-vous d'installer les outils d'administration CA Identity Manager.
- Vous devez avoir accès à un serveur d'annuaires Sun Java System (Sun One ou iPlanet) ou une base de données Microsoft SQL Server.

Fichiers d'installation pour l'environnement NeteAuto

CA Identity Manager inclut un ensemble de fichiers que vous pouvez utiliser pour configurer un exemple d'environnement CA Identity Manager. L'environnement CA Identity Manager est une vue d'espace de noms de gestion qui permet aux administrateurs CA Identity Manager de gérer des objets tels que des utilisateurs, des groupes et des organisations. Ces objets sont gérés avec un ensemble de rôles et de tâches associés. L'environnement CA Identity Manager contrôle la gestion et la présentation graphique d'un annuaire.

L'exemple d'environnement CA Identity Manager comprend :

- Des exemples d'objets, tels que des utilisateurs et des organisations
- Des définitions de rôles, de tâches et de fenêtres

  Les tâches apparaissent dans la console d'utilisateur lorsque vous cliquez sur un onglet, tel que Utilisateurs ou Groupes. En fonction des rôles affectés, les tâches associées s'affichent lorsque l'utilisateur se connecte.

  Remarque : Pour plus d'informations sur les tâches et les rôles, reportez-vous au *Manuel d'administration*.
- Un exemple d'apparence permettant de personnaliser la console d'utilisateur pour les utilisateurs NeteAuto
- Un fichier de configuration d'annuaire que vous utilisez pour créer un annuaire CA Identity Manager

Les fichiers destinés à la création de l'exemple d'environnement CA Identity Manager se trouvent à l'emplacement suivant :

outils_admin\samples\NeteAuto

Dans ce chemin d'accès, *admin_tools* se réfère aux outils d'administration. Les outils d'administration sont installés aux emplacements par défaut ci-après.

- **Windows :** <chemin_d'installation>\tools
- **UNIX :** <chemin_d'installation2>/tools

Installation de l'environnement NeteAuto

Pour installer l'environnement NeteAuto, suivez la procédure suivante.

Procédez comme suit:

1. Veillez à ce que le logiciel requis soit installé (page 22).
2. Configurez le référentiel d'utilisateurs et importez des exemples de données.
   - Pour des utilisateurs LDAP : configurez un annuaire d'utilisateurs LDAP. (page 23)
   - Pour des utilisateurs de base de données relationnelles : configurez une base de données relationnelles.
3. Créez l'annuaire CA Identity Manager pour NeteAuto.
4. Créez l'environnement CA Identity Manager pour NeteAuto.
5. Configurez l'apparence de l'interface utilisateur CA Identity Manager pour les utilisateurs NeteAuto (page 39).

Configuration d'un annuaire d'utilisateurs LDAP

L'annuaire LDAP est disponible en fonction de votre installation. Pour vérifier si l'annuaire existe ou si vous devez le créer, vous pouvez procéder comme suit.

Procédez comme suit:

1. Dans la console du serveur d'annuaires, créez une instance LDAP avec la racine suivante :

   ```
   dc=security,dc=com
   ```

   Notez le numéro de port aux fins de référence ultérieure.

2. Importez le fichier NeteAuto.ldif dans le serveur d'annuaires à partir de samples\NeteAuto situé dans les outils d'administration.

   Les outils d'administration sont situés aux emplacements par défaut suivants :

   - **Windows** : <chemin_installation>\tools
   - **UNIX** : <chemin_installation2>/tools

Remarque : Si vous rencontrez des problèmes lors de l'importation du fichier LDIF ou de la création de l'annuaire CA Identity Manager, ajoutez le texte suivant au début du fichier LDIF :

```
dn : dc=security, dc=com
objectClass: top
objectClass: domain
dc: security
```

Enregistrez le fichier et répétez les étapes 1 et 2.

Configuration d'une base de données relationnelles

Pour configurer une base de données relationnelles, suivez la procédure suivante.

Procédez comme suit:

1. Créez une instance de base de données nommée NeteAuto.
2. Créez un utilisateur nommé neteautoadmin avec le mot de passe test. Accordez des droits neteautoadmin (tels que des droits publics db_owner) à NeteAuto en modifiant les propriétés de l'utilisateur.

   Remarque : Pour créer une base de données NeteAuto, le rôle neteautoadmin doit au moins disposer des autorisations minimum (sélection, insertion, mise à jour et suppression) pour toutes les tables créées à l'aide du script .sql. De même, neteautoadmin doit pouvoir exécuter toutes les procédures stockées, le cas échéant, définies dans ces scripts.
3. Lors de la modification des propriétés d'utilisateur, définissez NeteAuto comme base de données par défaut pour neteautoadmin.

4. Exécutez les scripts suivants dans l'ordre dans lequel ils sont répertoriés :
   - *db_type*-rdbuserdirectory.sql : configure les tables de l'exemple NeteAuto et crée les entrées d'utilisateur.
   - ims_*db_type*_rdb.sql : configure la prise en charge des organisations.

     db_type

     Définit Microsoft SQL ou Oracle selon le type de base de données que vous configurez.

   Ces fichiers de script se trouvent dans le dossier *admin_tools*\samples\NeteAutoRDB\Organization. Dans cet exemple, *admin_tools* se réfère aux outils d'administration, installés dans les emplacements par défaut suivants :
   - **Windows** : <chemin_installation>\tools
   - **UNIX** : <chemin_installation2>/tools
5. Définissez une source de données JDBC nommée neteautoDS qui pointe vers la base de données NeteAuto.

   La procédure de configuration d'une source de données dépend du type de serveur d'applications sur lequel CA Identity Manager est installé. La section Création d'une source de données JDBC (page 107) comprend des instructions spécifiques au serveur d'applications pour la création d'une source de données JDBC.

Création d'un annuaire CA Identity Manager

Pour créer un annuaire CA Identity Manager, suivez la procédure suivante.

Procédez comme suit:

1. Pour ouvrir la console de gestion, saisissez l'URL suivante dans un navigateur.

   http://*serveur_im*:*port*/iam/immanage

   serveur_im

   Définit le nom de domaine complet du serveur sur lequel CA Identity Manager est installé.

   port

   Définit le numéro de port du serveur d'applications.
2. Cliquez sur Annuaires.
3. Pour lancer l'assistant de création d'annuaires CA Identity Manager, cliquez sur Create from Wizard (Créer à partir de l'assistant).

4. Accédez au fichier .xml de configuration d'annuaire approprié et cliquez sur Suivant.

   Le fichier de configuration d'annuaire se trouve dans les dossiers suivants :

   - Pour les annuaires d'utilisateurs du serveur d'annuaires Sun Java System :

     admin_tools\samples\NeteAuto\Organization\directory.xml

   - Pour les bases de données relationnelles :

     admin_tools\samples\NeteAutoRDB\Organization*db_type* directory.xml

     outils_admin

     Définit l'emplacement d'installation des outils d'administration.

     Les outils d'administration sont situés aux emplacements par défaut suivants :

     Windows : <chemin_installation>\tools

     UNIX : <chemin_installation2>/tools

     db_type

     Spécifie le type de base de données que vous configurez : Microsoft SQL ou Oracle.

   Des informations sur le statut sont affichées dans la fenêtre Directory Configuration Output (Résultat de la configuration d'annuaire).

5. Dans la deuxième page de l'assistant, renseignez les valeurs suivantes :

   - Serveur d'annuaires Sun Java System

     Nom

     Répertoire de la NeteAuto

     Description

     Sample NeteAuto directory (Exemple d'annuaire NeteAuto)

     Connection Object Name (Nom d'objet de connexion)

     NeteAuto Users (Utilisateurs NeteAuto)

     Hôte

     Définit le nom d'ordinateur ou l'adresse IP du système sur lequel le référentiel d'utilisateurs est installé.

     Port

     Numéro de port du référentiel d'utilisateurs

     Rechercher la racine

     dc=security, dc=com

Nom d'utilisateur

Spécifie le nom d'utilisateur d'un compte pouvant accéder au référentiel d'utilisateurs.

Mot de passe et Confirmer le mot de passe

Mot de passe du compte d'utilisateur

- Bases de données Microsoft SQL Server et Oracle

  Nom

  Répertoire de la NeteAutoRDB

  Description

  Sample NeteAuto directory (Exemple d'annuaire NeteAuto)

  Connection Object Name (Nom d'objet de connexion)

  NeteAutoRDB

  JDBC Data Source (Source de données JDBC)

  neteautoDS

  Nom d'utilisateur

  Neteautoadmin

  Mot de passe

  Test

6. Cliquez sur Suivant.
7. Pour quitter l'assistant, cliquez sur Terminer.

Création de l'environnement CA Identity Manager pour NeteAuto

Pour créer l'environnement CA Identity Manager pour NeteAuto, suivez la procédure suivante.

Procédez comme suit:

1. Dans la console de gestion, cliquez sur Environnements.
2. Dans la fenêtre Environnements CA Identity Manager, cliquez sur Nouveau.

   L'assistant de création d'environnements CA Identity Manager s'ouvre.
3. Dans la première page de l'assistant, renseignez les valeurs suivantes :

   Environment name (Nom de l'environnement)

   Environnement NeteAuto

Description

Exemple d'environnement

Alias

Neteauto

Cet alias est ajouté à l'URL permettant d'accéder à l'environnement CA Identity Manager. Par exemple, l'URL permettant d'accéder à l'environnement NeteAuto est le suivant :

http://*nom_serveur*/iam/im/neteauto

nom_serveur

Définit le nom de domaine complet du serveur sur lequel CA Identity Manager est installé. Par exemple :

http://myserver.mycompany.org/iam/im/neteauto

Remarque : L'alias respecte la casse.

Cliquez sur Suivant.

4. Sélectionnez l'annuaire CA Identity Manager à associer à l'environnement que vous créez :
   - Pour le serveur d'annuaires Sun Java System, utilisez l'annuaire NeteAuto.
   - Pour une base de données Microsoft SQL Server ou Oracle, utilisez l'annuaire NeteAutoRDB.

   Cliquez sur Suivant.
5. Configurez la prise en charge des tâches publiques, telles que des tâches d'auto-enregistrement et de mot de passe oublié, comme suit :
   a. Saisissez l'alias suivant pour des tâches publiques :

      Neteautopublic

   b. Saisissez SelfRegUser comme compte d'utilisateur anonyme.
   c. Pour afficher l'identificateur unique de l'utilisateur, cliquez sur Valider.

   Remarque : Les utilisateurs n'ont pas besoin de se connecter pour utiliser des tâches publiques.
6. Sélectionnez les tâches et les rôles à créer pour l'environnement NeteAuto.
   a. Sélectionnez Import roles from the file (Importer des rôles à partir du fichier).
   b. Accédez à l'un des emplacements suivants :
      - Pour un référentiel d'utilisateurs de serveur d'annuaires Sun Java System :

        admin_tools\samples\NeteAuto\RoleDefinitions.xml

- Pour un référentiel d'utilisateurs Microsoft SQL Server :

  admin_tools\samples\NeteAutoRDB\Organization\mssqlRoleDefinitions.xml

- Pour un référentiel d'utilisateurs Oracle :

  admin_tools\samples\NeteAutoRDB\Organization\oracleRoleDefinitions.xml

admin_tools se réfère aux outils d'administration, situés à l'emplacement par défaut suivant :

Windows : <chemin_installation>\tools

UNIX : <chemin_installation2>/tools

7. Définissez un utilisateur pour agir en tant que responsable du système pour cet environnement et cliquez sur Suivant :
   a. Dans le champ du responsable du système, saisissez SuperAdmin.
   b. Cliquez sur Ajouter.

      CA Identity Manager ajoute l'identificateur unique du superadministrateur à la liste d'utilisateurs.
   c. Cliquez sur Suivant.
8. Vérifiez les paramètres de l'environnement, et effectuez les tâches suivantes :
   - (Facultatif) Pour apporter des modifications, cliquez sur Précédent.
   - Pour créer l'environnement CA Identity Manager avec les paramètres actuels, cliquez sur Terminer.

     La fenêtre Environment Configuration Output (Résultat de la configuration de l'environnement) affiche la progression de la création de l'environnement.
9. Pour fermer l'assistant de création d'environnements CA Identity Manager, cliquez sur Continuer.
10. Démarrez l'environnement CA Identity Manager.

Une fois l'environnement NeteAuto créé, vous pouvez :

- Créer une apparence pour cet environnement CA Identity Manager (page 39)
- Accéder à l'environnement (page 37)

Configuration de l'exemple NeteAuto sans prise en charge d'organisation

La configuration de l'exemple NeteAuto sans prise en charge d'organisations implique la procédure suivante :

- Installation du logiciel requis (page 22)
- Installation de l'exemple d'environnement CA Identity Manager
- Configuration de la base de données
- Création d'une source de données JDBC
- Création d'un annuaire CA Identity Manager
- Création de l'environnement CA Identity Manager pour NeteAuto

Description de l'exemple d'environnement CA Identity Manager

Pour les bases de données Microsoft SQL Server et Oracle, CA Identity Manager inclut une version de l'environnement NeteAuto qui n'inclut pas d'organisations. Cet environnement CA Identity Manager inclut les trois utilisateurs suivants :

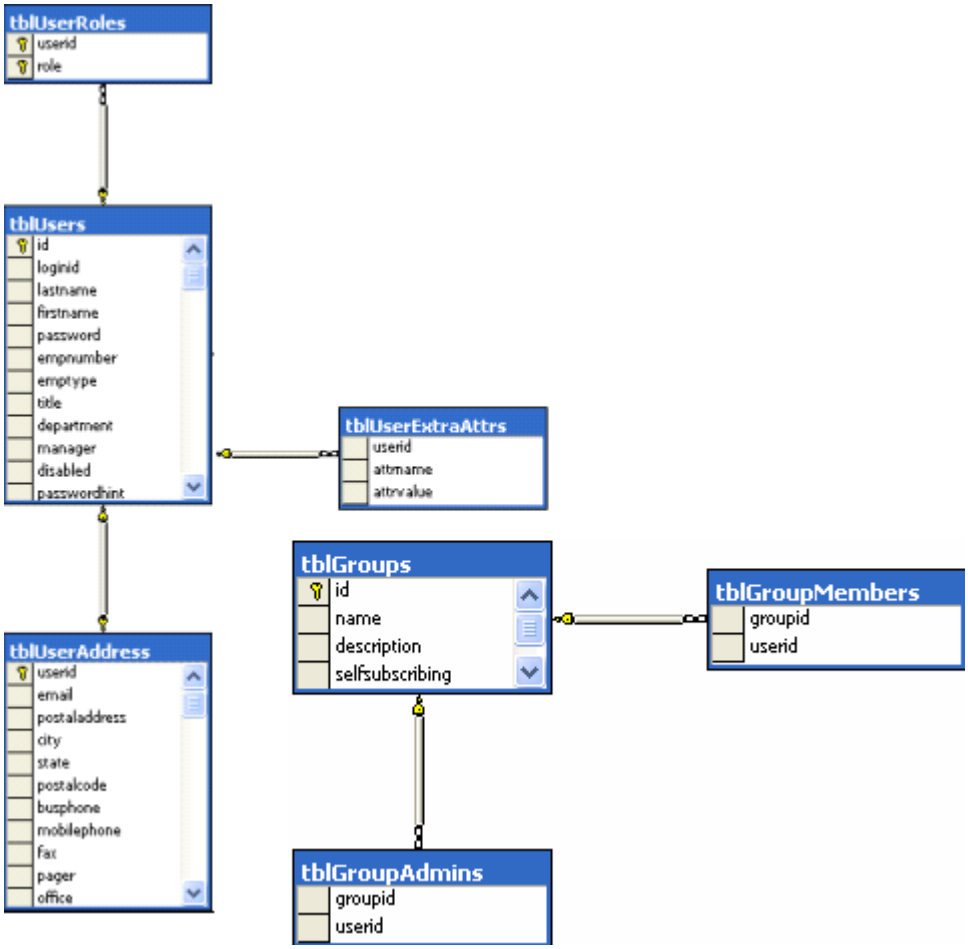
- Superadministrateur est le compte d'administrateur disposant du rôle de responsable du système pour cet environnement CA Identity Manager. Le superadministrateur peut effectuer toutes les tâches d'administration par défaut.

  Remarque : Pour obtenir une description des tâches d'administration par défaut, consultez le *Manuel d'administration*.

- SelfRegUser est le compte d'administrateur que CA Identity Manager utilise pour activer l'auto-enregistrement pour cet environnement CA Identity Manager.
- Lors de l'installation de l'environnement NeteAuto, l'administrateur NeteAuto ne dispose d'aucun droit.

  Toutefois, vous pouvez affecter le rôle de gestionnaire de groupes au compte d'administrateur NeteAuto.

Le schéma suivant illustre l'exemple NeteAuto pour une base de données relationnelles sans organisation :



Fichiers d'installation pour l'environnement NeteAuto

CA Identity Manager inclut un ensemble de fichiers que vous pouvez utiliser pour configurer un exemple d'environnement CA Identity Manager. Un environnement CA Identity Manager est une vue d'espace de noms de gestion qui permet aux administrateurs CA Identity Manager de gérer des objets. Ces objets, tels que des utilisateurs et des groupes, sont fournis avec un ensemble de rôles et de tâches associés. Un environnement CA Identity Manager contrôle la gestion et la présentation graphique d'un référentiel d'utilisateurs.

L'exemple d'environnement CA Identity Manager comprend :

- Des exemples d'utilisateurs
- Des définitions de rôles, de tâches et de fenêtres

  Les tâches apparaissent dans la console d'utilisateur lorsque vous cliquez sur une catégorie telle qu'utilisateurs ou groupes. Les tâches qui s'affichent sont basées sur les rôles affectés à l'utilisateur.

  Remarque : Pour plus d'informations sur les tâches et les rôles, reportez-vous au *Manuel d'administration*.
- Un exemple d'apparence permettant de personnaliser la console d'utilisateur pour les utilisateurs NeteAuto
- Un fichier de configuration d'annuaire que vous utilisez pour créer un annuaire CA Identity Manager

Les fichiers destinés à la création de l'exemple d'environnement CA Identity Manager se trouvent à l'emplacement suivant :

`admin_tools\samples\NeteAutoRDB\NoOrganization`

Dans ce chemin d'accès, *admin_tools* se réfère aux outils d'administration.

Les outils d'administration sont installés aux emplacements par défaut ci-après.

- **Windows :** <chemin_d'installation>\tools
- **UNIX :** <chemin_d'installation2>/tools

Installation de l'environnement NeteAuto sans prise en charge d'organisation

Pour installer l'environnement NeteAuto, suivez la procédure suivante.

Procédez comme suit:

1. Vérifiez que le logiciel requis (page 33) est installé.
2. Configurez la base de données. (page 24)
3. Créez un annuaire CA Identity Manager. (page 34)
4. Créez l'environnement CA Identity Manager pour NeteAuto (page 35).
5. Configurez l'apparence de l'interface utilisateur CA Identity Manager (page 39) pour les utilisateurs NeteAuto.

Logiciel requis

Configuration requise pour l'environnement CA Identity Manager pour NeteAuto :

- Installez CA Identity Manager comme décrit dans le *Manuel d'installation*. Veillez à installer les outils d'administration CA Identity Manager.
- Vous devez disposer de l'accès à une base de données Microsoft SQL Server ou Oracle.

Configuration d'une base de données relationnelles

Pour configurer une base de données relationnelles, suivez la procédure suivante.

Procédez comme suit:

1. Créez une instance de base de données nommée NeteAuto.
2. Créez un utilisateur nommé neteautoadmin avec le mot de passe test. Accordez des droits neteautoadmin (tels que des droits publics db_owner) à NeteAuto en modifiant les propriétés de l'utilisateur.

   Remarque : Pour créer une base de données NeteAuto, le rôle neteautoadmin doit au moins disposer des autorisations minimum (sélection, insertion, mise à jour et suppression) pour toutes les tables créées à l'aide du script .sql. De même, neteautoadmin doit pouvoir exécuter toutes les procédures stockées, le cas échéant, définies dans ces scripts.
3. Lors de la modification des propriétés d'utilisateur, définissez NeteAuto comme base de données par défaut pour neteautoadmin.
4. Exécutez les scripts suivants dans l'ordre dans lequel ils sont répertoriés :
   - *db_type*-rdbuserdirectory.sql : configure les tables de l'exemple NeteAuto et crée les entrées d'utilisateur.
   - ims_*db_type*_rdb.sql : configure la prise en charge des organisations.

     db_type

     Définit Microsoft SQL ou Oracle selon le type de base de données que vous configurez.

   Ces fichiers de script se trouvent dans le dossier *admin_tools*\samples\NeteAutoRDB\Organization. Dans cet exemple, *admin_tools* se réfère aux outils d'administration, installés dans les emplacements par défaut suivants :
   - **Windows** : <chemin_installation>\tools
   - **UNIX** : <chemin_installation2>/tools

5. Définissez une source de données JDBC nommée neteautoDS qui pointe vers la base de données NeteAuto.

   La procédure de configuration d'une source de données dépend du type de serveur d'applications sur lequel CA Identity Manager est installé. La section Création d'une source de données JDBC (page 107) comprend des instructions spécifiques au serveur d'applications pour la création d'une source de données JDBC.

Création d'un annuaire CA Identity Manager

Pour créer un annuaire CA Identity Manager, suivez la procédure suivante.

Procédez comme suit:

1. Pour ouvrir la console de gestion, saisissez l'URL suivante dans un navigateur.

   http://*serveur_im*:*port*/iam/immanage

   serveur_im

   Définit le nom de domaine complet du serveur sur lequel CA Identity Manager est installé.

   port

   Définit le numéro de port du serveur d'applications.

2. Cliquez sur Annuaires.

   La fenêtre d'annuaires CA Identity Manager s'affiche.

3. Pour lancer l'assistant de création d'annuaires CA Identity Manager, cliquez sur Nouveau.

4. Accédez à l'un des fichiers XML de configuration d'annuaire suivants et cliquez sur Suivant :

   - Sun Java System :

     admin_tools\samples\NeteAuto\NoOrganization\directory.xml

   - Bases de données SQL Server :

     admin_tools\samples\NeteAuto\NoOrganization\mssql-directory.xml

   - Bases de données Oracle :

     admin_tools\samples\NeteAuto\NoOrganization\oracle-directory.xml

   admin_tools se réfère aux outils d'administration, situés à l'emplacement par défaut suivant :

   - **Windows** : <chemin_installation>\tools
   - **UNIX** : <chemin_installation2>/tools

   Des informations sur le statut sont affichées dans la fenêtre Directory Configuration Output (Résultat de la configuration d'annuaire).

5. Dans la deuxième page de l'assistant, renseignez les valeurs suivantes :

   Nom

   Répertoire de la NeteAutoRDB

   Description

   Exemple d'annuaire NeteAuto sans prise en charge d'organisation

   Connection Object Name (Nom d'objet de connexion)

   NeteAutoRDB

   JDBC Data Source (Source de données JDBC)

   neteautoDS

   Nom d'utilisateur

   neteautoadmin

   Mot de passe

   test

6. Cliquez sur Suivant.
7. Pour quitter l'assistant, cliquez sur Terminer.

Création de l'environnement CA Identity Manager pour NeteAuto

Pour créer l'environnement CA Identity Manager pour NeteAuto, suivez la procédure suivante.

Procédez comme suit:

1. Dans la console de gestion, cliquez sur Environnements.
2. Dans la fenêtre Environnements CA Identity Manager, cliquez sur Nouveau.

   L'assistant de création d'environnements CA Identity Manager s'ouvre.
3. Dans la première page de l'assistant, saisissez les valeurs suivantes :
   - Environment name (Nom de l'environnement) : Environnement NeteAuto
   - Description : NeteAuto est un exemple d'environnement.

- Alias : NeteautoRDB

  Cet alias est ajouté à l'URL permettant d'accéder à l'environnement CA Identity Manager. Par exemple, l'URL permettant d'accéder à l'environnement NeteAuto est le suivant :

  `http://domaine/iam/im/neteautoRDB`

  Dans ce chemin d'accès, *domaine* définit le nom de domaine complet du serveur sur lequel CA Identity Manager est installé, comme dans l'exemple suivant :

  `http://myserver.mycompany.org/iam/im/neteautoRDB`

  Remarque : L'alias respecte la casse.

Cliquez sur Suivant.

4. Sélectionnez l'annuaire NeteAutoRDB CA Identity Manager à associer à l'environnement que vous créez et cliquez sur Suivant.
5. Configurez la prise en charge des tâches publiques, telles que des tâches d'auto-enregistrement et de mot de passe oublié.

   Remarque : Les utilisateurs n'ont pas besoin de se connecter pour accéder à des tâches publiques.

   a. Saisissez l'alias suivant pour des tâches publiques :

      neteautoRDBpublic

   b. Saisissez SelfRegUser comme compte d'utilisateur anonyme.

   c. Pour afficher l'identificateur unique de l'utilisateur (2, dans ce cas), cliquez sur Valider.
6. Sélectionnez les tâches et les rôles à créer pour l'environnement NeteAuto.

   - Sélectionnez Import roles from the file (Importer des rôles à partir du fichier).
   - Accédez à l'emplacement suivant :

     rép_admin_tools_im\samples\NeteAutoRDB\NoOrganizations\RoleDefinitions.xml

     Dans ce chemin d'accès, *rép_admin_tools_im* définit l'emplacement d'installation des outils d'administration CA Identity Manager.
7. Définissez un utilisateur pour agir en tant que responsable du système pour cet environnement et cliquez sur Suivant :

   a. Dans le champ du responsable du système, saisissez SuperAdmin.

   b. Cliquez sur Ajouter.

   c. Cliquez sur Suivant.

8. Révisez ces paramètres.
   - Pour apporter des modifications, cliquez sur Précédent.
   - Pour créer l'environnement CA Identity Manager avec les paramètres actuels, cliquez sur Terminer.

     La fenêtre Environment Configuration Output (Résultat de la configuration de l'environnement) affiche la progression de la création de l'environnement.
9. Pour fermer l'assistant de création d'environnements CA Identity Manager, cliquez sur Terminer.
10. Démarrez l'environnement CA Identity Manager.

Une fois l'environnement NeteAuto créé, vous pouvez :

- Créer une apparence pour cet environnement CA Identity Manager tel que décrit à la section Configuration de l'apparence de NeteAuto (page 39)
- Accéder à l'environnement comme décrit à la section Utilisation de l'environnement CA Identity Manager pour NeteAuto

Utilisation de l'environnement CA Identity Manager pour NeteAuto

Vous pouvez utiliser l'environnement CA Identity Manager pour NeteAuto pour gérer des tâches d'auto-administration et des utilisateurs.

Gestion des tâches d'auto-administration

Les tâches d'auto-administration incluent les tâches suivantes :

- Enregistrement en tant que nouvel utilisateur
- Connexion en tant qu'utilisateur auto-enregistré
- Utilisation de la fonctionnalité de mot de passe oublié

Enregistrement en tant que nouvel utilisateur

Pour vous enregistrer en tant que nouvel utilisateur, suivez la procédure suivante.

Procédez comme suit:

1. Saisissez l'URL suivante dans un navigateur :

   `http://nomhôte/iam/im/neteautopublic/index.jsp?task.tag=SelfRegistration`

   hostname

   Définit le nom de domaine complet du système sur lequel CA Identity Manager est exécuté.

   Remarque : Si vous n'avez pas configuré l'apparence de NeteAuto (page 39), vous pouvez supprimer imcss de l'URL comme suit :

   http://*nomhôte*/iam/im/neteautopublic/index.jsp?task.tag=SelfRegistration

   Cette URL vous dirige vers la console CA par défaut .

   Dans la page d'auto-enregistrement : Contrat de licence de l'utilisateur final, CA Identity Manager affiche le site Web de CA.

   Remarque : Vous pouvez configurer la tâche d'auto-enregistrement par défaut de sorte à afficher le contrat de licence de l'utilisateur final personnalisé. Pour obtenir des instructions, consultez le *Manuel d'administration*.

2. Pour continuer, cliquez sur Accepter.
3. Dans l'onglet Profil, fournissez les détails suivants :
   a. Saisissez des valeurs dans les champs obligatoires, signalés par un astérisque (*).
   b. Saisissez des indices de mot de passe et des réponses.

      En cas de mot de passe oublié, CA Identity Manager fournit l'indice de mot de passe et demande la réponse. Si la réponse est correcte, CA Identity Manager invite l'utilisateur à spécifier et à confirmer un autre mot de passe.
4. Ne modifiez pas l'onglet Groupes.
5. Cliquez sur Soumettre.

Connexion en tant qu'utilisateur auto-enregistré

Pour vous connecter en tant qu'utilisateur auto-enregistré, suivez la procédure suivante.

Procédez comme suit:

1. Saisissez l'URL suivante pour l'environnement CA Identity Manager pour NeteAuto dans un navigateur :

   `http://nomhôte/iam/im/neteauto/imcss/index.jsp`

   hostname

   Définit le nom de domaine complet du système sur lequel CA Identity Manager est exécuté.

2. Connectez-vous à l'aide du nom d'utilisateur et du mot de passe spécifiés lors de l'enregistrement.

Configuration de l'apparence de NeteAuto

Pour configurer l'apparence NeteAuto, créez une réponse SiteMinder dans le serveur de stratégies SiteMinder.

Procédez comme suit:

1. Connectez-vous à l'une des interfaces suivantes en tant qu'administrateur avec des droits de domaine :

   - Pour SiteMinder Web Access Manager r12 ou version ultérieure, connectez-vous à l'interface d'administration.
   - Pour CA eTrust SiteMinder 6.0 SP5, connectez-vous à l'interface utilisateur du serveur de stratégies.

   Remarque : Pour plus d'informations sur l'utilisation de ces interfaces, consultez la documentation de la version de SiteMinder que vous utilisez.

2. Ouvrez neteautoDomain.

3. Sous neteautoDomain, sélectionnez Domaines.

   Les domaines suivants apparaissent :

   neteauto_ims_realm

   Protège l'environnement CA Identity Manager.

   neteauto_pub_realm

   Permet la prise en charge des tâches publiques, comme les tâches d'auto-enregistrement et de mot de passe oublié.

4. Créez une règle dans chaque domaine. Spécifiez les détails suivants :
   - Ressource : *
   - Actions : GET, POST

   Pour simplifier l'administration, incluez l'apparence de NeteAuto dans le nom de la règle.
5. Créez une réponse pour le domaine avec les attributs de réponse suivants :
   - Attribut : WebAgent-HTTP-Header-Variable

     Cet attribut ajoute un nouvel en-tête HTTP à la réponse.
   - Type d'attribut : Statique
   - Nom de la variable : apparence

     Valeur de la variable : neteauto
6. Modifiez la stratégie créée par CA Identity Manager dans neteautoDomain. Spécifiez les détails suivants :
   - Utilisateurs
     - Pour LDAP : sélectionnez ou=People, ou=Employees, ou=NeteAuto dans les membres disponibles et ajoutez-le aux membres actuels. Cliquez sur OK.
     - Pour des bases de données relationnelles : recherchez des utilisateurs pour lesquels l'attribut d'ID est égal à *. Sélectionnez tous les utilisateurs dans les membres disponibles et ajoutez-les aux membres actuels. Cliquez sur OK.
   - Règles :
     - Ajoutez les règles créées à l'étape 4.
     - Pour chaque règle, cliquez sur Set Response (Définir une réponse). Associez chaque règle à la réponse créée à l'étape 5.

Remarque : L'apparence de NeteAuto est basée sur la console imcss. Pour afficher l'apparence, ajoutez /imcss/index.jsp à l'URL de l'environnement CA Identity Manager pour NeteAuto comme suit :

http://*nomhôte*/iam/im/neteauto/imcss/index.jsp

L'accès à l'environnement CA Identity Manager pour NeteAuto (page 42) fournit des instructions complètes pour accéder à l'environnement de NeteAuto.

Utilisation de la fonctionnalité de mot de passe oublié

Pour utiliser la fonctionnalité de mot de passe oublié, suivez la procédure suivante.

Procédez comme suit:

1. Saisissez l'URL suivante dans un navigateur :

   `http://nomhôte/iam/im/neteautopublic/index.jsp?task.tag=ForgottenPasswordReset`

   hostname

   Définit le nom de domaine complet du système sur lequel CA Identity Manager est exécuté.

2. Saisissez l'identificateur unique de l'utilisateur auto-enregistré créé à l'étape d'enregistrement en tant que nouvel utilisateur (page 38) et cliquez sur Suivant.

3. Chaque fois que vous y êtes invité, répondez à la question de vérification. La réponse est celle que vous avez fournie lors de l'enregistrement.

   Remarque : Une réponse correcte est requise pour chaque question. L'annulation de la tâche ou la fermeture du navigateur est considérée comme un échec de tentative.

4. Cliquez sur Soumettre.

   CA Identity Manager vous invite à fournir un nouveau mot de passe.

Gestion des utilisateurs

La gestion des utilisateurs inclut les opérations suivantes :

- Accès à l'environnement CA Identity Manager pour NeteAuto
- Modification d'un utilisateur
- Affectation du rôle de gestionnaire de groupes
- Création d'un groupe
- Gestion des utilisateurs auto-enregistrés

Accès à l'environnement CA Identity Manager pour NeteAuto

Pour accéder à l'environnement CA Identity Manager pour NeteAuto, suivez la procédure suivante.

Procédez comme suit:

1. Saisissez l'URL suivante dans un navigateur :

   `http://nomhôte/iam/im/neteauto/imcss/index.jsp`

   hostname

   Définit le nom de domaine complet, comme dans l'exemple suivant :

   http://myserver.mycompany.com/iam/im/neteauto/imcss/index.jsp.

   Remarque : Si vous n'avez pas configuré l'apparence de NeteAuto, vous pouvez utiliser l'URL suivante pour accéder à l'environnement NeteAuto :

   http://*nomhôte*/iam/im/neteauto

2. Dans la fenêtre de connexion, saisissez les informations d'identification suivantes :

   Nom d'utilisateur

   SuperAdmin

   Mot de passe

   test

Modification d'un utilisateur

Pour modifier un utilisateur, suivez la procédure suivante.

Procédez comme suit:

1. Connectez-vous à l'environnement NeteAuto en tant que SuperAdmin à l'aide du mot de passe test.
2. Sélectionnez Utilisateurs, Gérer les utilisateurs, Modifier un utilisateur.

   La boîte de dialogue Sélection de l'utilisateur s'affiche.
3. Cliquez sur Rechercher.

   CA Identity Manager affiche une liste d'utilisateurs dans l'environnement NeteAuto.
4. Sélectionnez l'administrateur NeteAuto, comme suit :
   - Pour des annuaires LDAP : Administrateur NeteAuto
   - Pour des bases de données relationnelles : Admin NeteAuto

   Cliquez sur Sélectionner. CA Identity Manager affiche le profil de l'administrateur NeteAuto.

5. Dans le champ Titre, saisissez Gestionnaire. Cliquez sur Soumettre.

   CA Identity Manager confirme la soumission de la tâche.

6. Pour revenir à l'écran principal, cliquez sur OK.

Affectation du rôle de gestionnaire de groupes

Il est nécessaire d'affecter un rôle de gestionnaire de groupes. Pour affecter un gestionnaire de groupes, suivez la procédure suivante.

Procédez comme suit:

1. En tant que SuperAdmin, sélectionnez l'onglet Rôles et tâches, puis sélectionnez Rôles d'administration, Modifier un rôle d'administration.
2. Sélectionnez le rôle Gestionnaire de groupes et cliquez sur Sélectionner.

   Le profil du rôle de gestionnaire de groupes s'affiche.

3. Cliquez sur l'onglet Membres, puis sur Ajouter sous Stratégie de membre.

   La fenêtre Stratégie de membre s'ouvre.

4. Sous Règle du membre, cliquez sur la flèche vers le bas dans le champ Utilisateurs.

   Dans la liste déroulante, sélectionnez <user-filter>.

   Le champ Utilisateurs est modifié et permet de saisir un filtre pour la règle.

5. Saisissez une règle d'appartenance comme suit :
   a. Dans le premier champ, sélectionnez Titre dans la liste déroulante.
   b. Dans le deuxième champ, veillez à ce que le signe égal (=) soit sélectionné.
   c. Dans le troisième champ, saisissez Gestionnaire.
6. Dans la section Règle de portée, définissez des règles pour les utilisateurs, les groupes et les organisations (si elles sont prises en charge) comme suit :
   a. Dans le champ Utilisateurs, cliquez sur la flèche vers le bas pour afficher une liste d'options. Sélectionnez (Tout) dans la liste.
   b. Répétez l'étape a. pour les champs Groupe et Organisation (si elle sont prises en charge).
   c. Laissez le champ Tâche d'accès vide.
7. Cliquez sur OK.

   CA Identity Manager affiche la stratégie de membre que vous avez créée.

8. Cliquez sur Soumettre.

   CA Identity Manager confirme la soumission de la tâche.

9. Pour revenir à l'écran principal, cliquez sur OK.
10. Fermez CA Identity Manager.

Création d'un groupe

Pour créer un groupe, suivez la procédure suivante.

Procédez comme suit:

1. Connectez-vous à CA Identity Manager en tant qu'administrateur NeteAuto, comme suit :
   - Pour des annuaires LDAP, saisissez le nom d'utilisateur Administrateur NeteAuto et le mot de passe test.
   - Pour des bases de données relationnelles, saisissez le nom d'utilisateur Admin NeteAuto et le mot de passe test.

   La liste des tâches que l'administrateur NeteAuto peut effectuer s'affiche. L'administrateur NeteAuto peut uniquement effectuer un nombre de tâches limité ; c'est pourquoi CA Identity Manager répertorie les tâches au lieu de catégories.
2. Cliquez sur Créer un groupe.
3. Vérifiez que l'option Créer un groupe est sélectionnée, puis cliquez sur OK.
4. Implémentez l'une des étapes suivantes correspondant à votre cas :
   - Si l'environnement NeteAuto prend en charge les organisations :
     a. Dans le champ Nom de l'organisation, cliquez sur le symbole d'ellipse (...) pour sélectionner l'organisation dans laquelle CA Identity Manager crée le groupe.
     b. Au bas de la fenêtre Sélectionner une organisation, développez NeteAuto.
     c. Sélectionnez l'organisation Dealer (Grossiste).
   - Si l'environnement NeteAuto ne prend pas en charge les organisations, passez à l'étape suivante.
5. Saisissez les informations suivantes pour le groupe :
   - Nom du groupe : Administrateurs de grossiste
   - Description du groupe : Administrateurs de concessions NeteAuto
6. Cliquez sur l'onglet Appartenance et cliquez sur Ajouter un utilisateur.

   La boîte de dialogue Sélection de l'utilisateur s'affiche.
7. Cliquez sur Rechercher.
8. Sélectionnez l'administrateur NeteAuto et cliquez sur Sélectionner.
9. Cliquez sur Soumettre pour créer le groupe.

Gestion des utilisateurs auto-enregistrés

Lorsque vous voulez gérer des utilisateurs auto-enregistrés, suivez la procédure suivante.

Procédez comme suit:

1. Connectez-vous à CA Identity Manager en tant qu'administrateur NeteAuto, à l'aide des informations d'identification suivantes :

   - Pour des annuaires LDAP :

     Nom d'utilisateur

     Administrateur NeteAuto

     Mot de passe

     test

   - Pour les bases de données relationnelles :

     Nom d'utilisateur

     Admin NeteAuto

     Mot de passe

     test

   La liste des tâches que l'administrateur NeteAuto peut effectuer apparaît sur le côté gauche de la console d'utilisateur. L'administrateur NeteAuto peut uniquement effectuer un nombre de tâches limité ; c'est pourquoi CA Identity Manager répertorie les tâches au lieu de catégories.

2. Cliquez sur Modifier un groupe.
3. Cliquez sur Rechercher.

   CA Identity Manager affiche une liste de groupes.

4. Sélectionnez Dealer Administrators (Administrateurs de grossistes) et cliquez sur Sélectionner.
5. Cliquez sur l'onglet Appartenance et cliquez sur Ajouter un utilisateur.

   La boîte de dialogue Sélection de l'utilisateur s'affiche.

6. Cliquez sur Rechercher.
7. Dans la fenêtre User Search (Recherche d'utilisateurs), sélectionnez l'utilisateur que vous avez saisi à l'étape d'enregistrement en tant que nouvel utilisateur (page 38). Cliquez sur Sélectionner.

8. Cliquez sur Soumettre.

   CA Identity Manager confirme la soumission de la tâche.

9. Pour revenir à l'écran principal, cliquez sur OK.

Pour confirmer que l'utilisateur est membre du groupe créé, utilisez la tâche Afficher un groupe.

Configuration de fonctionnalités supplémentaires

Une fois l'exemple NeteAuto installé et après avoir testé la fonctionnalité CA Identity Manager de base, utilisez l'environnement NeteAuto pour tester des fonctionnalités CA Identity Manager supplémentaires, notamment des notifications par courriel et le flux de travaux.

Remarque : Pour plus d'informations sur ces fonctionnalités, reportez-vous au *Manuel d'administration*.

Limitation liée au nom de connexion SiteMinder pour le nom d'utilisateur global

Les chaînes de caractères ou caractères suivants ne peuvent pas figurer dans un nom d'utilisateur global si cet utilisateur doit se connecter au serveur de stratégies SiteMinder :

&
*
:
( )

Solution

N'utilisez pas ces caractères dans les noms d'utilisateurs globaux.

Chapitre 3: Gestion de référentiel d'utilisateurs LDAP

Ce chapitre traite des sujets suivants :

Annuaires CA Identity Manager

Un *annuaire CA Identity Manager* décrit le stockage d'objets tels que des utilisateurs, des groupes et des organisations dans l'annuaire d'utilisateurs et leur représentation dans CA Identity Manager. Un annuaire CA Identity Manager est associé à un ou plusieurs environnements CA Identity Manager.

Création d'un annuaire CA Identity Manager

La création d'un annuaire CA Identity Manager pour un référentiel d'utilisateurs LDAP implique les étapes suivantes :

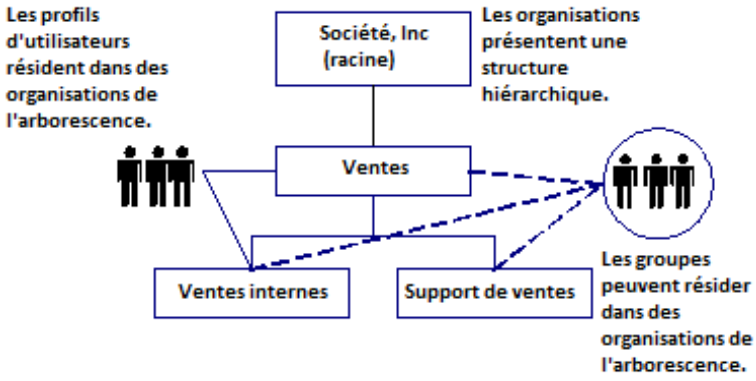
1. Définition de la structure d'annuaires
2. Description des objets dans le référentiel d'utilisateurs en modifiant un fichier de configuration d'annuaire (directory.xml) (page 53)
3. Importation du fichier de configuration d'annuaire et création de l'annuaire (page 157)

Remarque : Lors de l'utilisation de SiteMinder, vérifiez que vous avez appliqué le schéma de référentiel de stratégies avant de créer un annuaire CA Identity Manager. Pour plus d'informations sur les schémas de référentiel de stratégies spécifiques et leur application, consultez le *Manuel d'installation*.

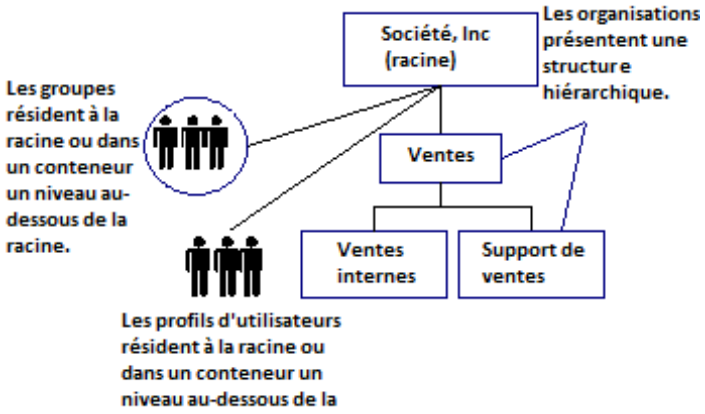
Structure des annuaires

CA Identity Manager prend en charge les structures d'annuaires suivantes :

- Hiérarchique : contient une organisation parente (racine) et des sous-organisations. Les sous-organisations peuvent également avoir des sous-organisations, ce qui crée une structure multiniveau, tel qu'illustré dans le schéma suivant :

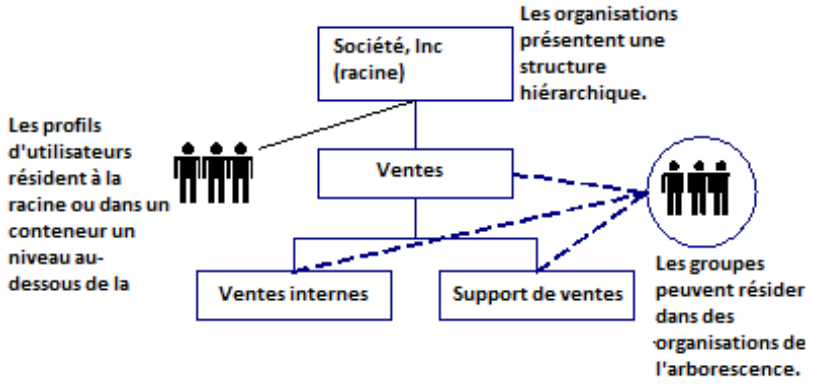


- Non hiérarchique : les utilisateurs et les groupes sont stockés au niveau de la racine de recherche ou dans un conteneur un niveau sous la racine de recherche. Les organisations ont une structure hiérarchique, comme illustré dans le schéma suivant d'une structure d'annuaires non hiérarchique :



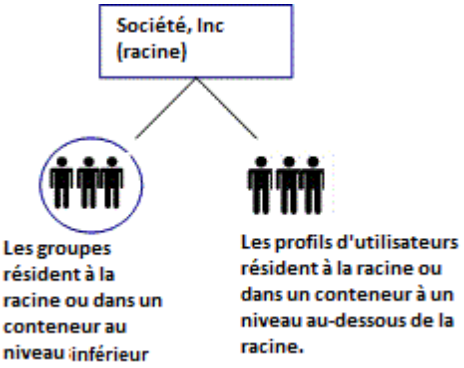
Pour faciliter la gestion des utilisateurs et la délégation dans les structures d'annuaires non hiérarchiques, les utilisateurs et les groupes appartiennent à des organisations logiques. L'organisation logique est stockée comme attribut dans des profils d'utilisateur et de groupe.

- Utilisateur non hiérarchique : les organisations et les groupes sont stockés hiérarchiquement, mais les utilisateurs sont stockés au niveau de la racine de recherche ou dans un conteneur un niveau sous la racine de recherche. Le graphique suivant illustre une structure d'annuaires d'utilisateurs non hiérarchique :



Dans les structures d'annuaires d'utilisateurs non hiérarchiques, les utilisateurs appartiennent à des organisations logiques. L'organisation logique d'un utilisateur est stockée comme attribut dans un profil d'utilisateur.

- Aucune organisation : l'annuaire n'inclut aucune organisation. Les utilisateurs et les groupes sont stockés au niveau de la racine de recherche ou dans un conteneur un niveau sous la racine de recherche. Le graphique suivant illustre une structure d'annuaires sans organisation :



Remarque : Un annuaire peut contenir plusieurs types de structure. Par exemple, vous pouvez stocker des profils d'utilisateur dans une structure non hiérarchique dans une section de l'annuaire et dans une structure hiérarchique dans une autre. Pour prendre en charge une structure d'annuaires hybride, créez plusieurs environnements CA Identity Manager.

Fichier de configuration d'annuaire

Pour décrire la structure d'un annuaire d'utilisateurs dans CA Identity Manager, créez un fichier de configuration d'annuaire.

Le fichier de configuration d'annuaire contient l'une ou plusieurs des sections suivantes :

Informations de l'annuaire CA Identity Manager

Contient des informations sur l'annuaire CA Identity Manager.

Remarque : Ne modifiez pas les informations de cette section. CA Identity Manager vous invite à les fournir lors de la création d'un annuaire CA Identity Manager dans la console de gestion.

Validation de l'attribut

Définit les règles de validation qui s'appliquent à l'annuaire CA Identity Manager.

Informations sur le fournisseur

Décrit le référentiel d'utilisateurs géré par CA Identity Manager.

Informations de recherche d'annuaire

Permet de spécifier la méthode de recherche du référentiel d'utilisateurs utilisée par CA Identity Manager.

Objet utilisateur

Décrit la méthode de stockage des utilisateurs dans le référentiel d'utilisateurs et leur représentation dans CA Identity Manager.

Objet groupe

Décrit la méthode de stockage des groupes dans le référentiel d'utilisateurs et leur représentation dans CA Identity Manager.

Objet organisation

Décrit la méthode de stockage des organisations et leur représentation dans CA Identity Manager. L'objet organisation fournit des détails uniquement lorsque le référentiel d'utilisateurs inclut des organisations.

Objet Self-Subscribing

Configure la prise en charge des groupes que les utilisateurs auto-enregistrés peuvent rejoindre.

Comportement des groupes d'annuaires

Spécifie si l'annuaire CA Identity Manager prend en charge les groupes dynamiques et imbriqués.

Pour créer un fichier de configuration d'annuaire, modifiez un modèle de configuration.

Sélection d'un modèle de configuration d'annuaire

CA Identity Manager fournit des modèles de configuration d'annuaire qui prennent en charge différents types et structures d'annuaire. Pour créer un annuaire CA Identity Manager, modifiez le modèle qui correspond le mieux à votre structure d'annuaires.

Les modèles décrits dans le tableau suivant sont installés avec les outils d'administration :

admin_tools\directoryTemplates*directory_type*\

Les outils d'administration sont installés aux emplacements par défaut ci-après.

- **Windows :** <chemin_d'installation>\tools
- **UNIX :** <chemin_d'installation2>/tools

Les types d'annuaire et les modèles de configuration correspondants figurent dans le tableau suivant :

Type d'annuaire	Modèle
Annuaire LDAP Active Directory (ADSI) avec structure hiérarchique	ActiveDirectory\directory.xml
Annuaire Microsoft ADAM avec structure hiérarchique	ADAM\directory.xml
Annuaire de serveur d'annuaires IBM avec structure hiérarchique	IBMDirectoryServer\directory.xml
Annuaire d'utilisateurs Novell eDirectory avec structure hiérarchique	eDirectory\directory.xml
Annuaire Internet Oracle avec structure hiérarchique	OracleInternetDirectory\directory.xml
Annuaire LDAP Sun Java System (SunOne ou iPlanet) avec structure hiérarchique	IPlanetHierarchical\directory.xml
Annuaire LDAP Sun Java System (SunOne ou iPlanet) avec structure non hiérarchique	IPlanetFlat\directory.xml
Annuaire LDAP Sun Java System (SunOne ou iPlanet) sans organisation	IPlanetNoOrganizations\directory.xml
Référentiel d'utilisateurs CA Directory avec structure hiérarchique	eTrustDirectory\directory.xml
Annuaire de provisionnement Ce modèle configure l'annuaire de provisionnement pour un environnement CA Identity Manager. **Remarque :** Vous pouvez utiliser ce modèle de configuration tel quel. Vous n'avez pas besoin de le modifier.	ProvisioningServer\directory.xml

Type d'annuaire	Modèle
Annuaire personnalisé	Utilisez le modèle le plus proche de votre annuaire.

Copiez le modèle de configuration vers un nouvel annuaire ou enregistrez-le sous un nom différent pour éviter de l'écraser.

Description d'un annuaire d'utilisateurs dans CA Identity Manager

Pour gérer un annuaire, CA Identity Manager doit connaître sa structure et son contenu. Pour décrire l'annuaire dans CA Identity Manager, modifiez le fichier de configuration d'annuaire (directory.xml) dans l'annuaire modèle approprié.

Le fichier de configuration d'annuaire contient les conventions importantes suivantes :

- ## : indique les valeurs requises.

  Pour fournir toutes les informations requises, recherchez tous les symboles de deux dièses (##) et remplacez-les par les valeurs appropriées. Par exemple, ##DISABLED_STATE indique que vous devez fournir un attribut pour stocker le statut du compte d'un utilisateur.
- @ : indique les valeurs remplies par CA Identity Manager. Ne modifiez pas ces valeurs dans le fichier de configuration d'annuaire. CA Identity Manager vous invite à fournir les valeurs lors de l'importation du fichier de configuration d'annuaire.

Avant de modifier ce fichier de configuration d'annuaire, les informations suivantes sont nécessaires :

- Classes d'objet LDAP pour les objets utilisateur, groupe et organisation
- Liste d'attributs dans les profils d'utilisateur, de groupe et d'organisation

Modification du fichier de configuration d'annuaire

Pour modifier le fichier de configuration d'annuaire, suivez la procédure suivante.

Remarque : Les étapes requises sont signalées.

1. Limitez la taille des résultats de la recherche (page 59).
2. Modifiez les objets gérés utilisateur, organisation, ou groupe par défaut.
3. Modifiez les descriptions d'attribut par défaut.

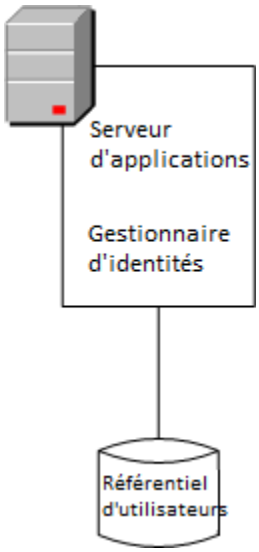
4. Modifiez des attributs connus (page 79). (requis)

   Les attributs connus identifient des attributs spéciaux, par exemple l'attribut de mot de passe, dans CA Identity Manager.

5. Configurez CA Identity Manager pour votre structure d'annuaire (page 86) (requis).
6. Permettez aux utilisateurs de s'inscrire à des groupes (page 87).

Connexion à l'annuaire d'utilisateurs

CA Identity Manager se connecte à un annuaire d'utilisateurs pour stocker des informations par exemple sur les utilisateurs, les groupes et les organisations comme illustré dans le schéma suivant :



Un nouvel annuaire ou une nouvelle base de données n'est pas nécessaire. Toutefois, l'annuaire ou la base de données qui existe doit être placé dans un système avec un nom de domaine complet.

Pour obtenir une liste de types d'annuaire et de base de données pris en charge, consultez le tableau de prise en charge CA Identity Manager sur le site du support de CA.

Configurez une connexion au référentiel d'utilisateurs lors de la création d'un annuaire CA Identity Manager dans la console de gestion.

Si vous exportez la configuration d'annuaire après la création d'un annuaire CA Identity Manager, les informations de connexion à l'annuaire d'utilisateurs apparaissent dans l'élément fournisseur du fichier de configuration d'annuaire.

Elément fournisseur

Les informations sur la configuration sont stockées dans l'élément fournisseur et ses sous-éléments dans le fichier directory.xml.

Remarque : Si vous créez un annuaire CA Identity Manager, il n'est pas nécessaire de fournir des informations de connexion à l'annuaire dans le fichier directory.xml. Indiquez les informations de connexion dans l'assistant de création d'annuaires CA Identity Manager dans la console de gestion. Modifiez l'élément fournisseur aux fins de mise à jour uniquement.

L'élément fournisseur inclut les sous-éléments suivants :

LDAP

Décrit l'annuaire d'utilisateurs auquel vous vous connectez.

Credentials (Informations d'identification)

Fournit le nom d'utilisateur et le mot de passe permettant d'accéder au référentiel d'utilisateurs LDAP.

Connexion

Spécifie le nom d'hôte et le port de l'ordinateur sur lequel le référentiel d'utilisateurs est installé.

Provisioning Domain (Domaine de provisionnement)

Définit le domaine de provisionnement géré par CA Identity Manager (aux fins de provisionnement des utilisateurs uniquement).

Un élément fournisseur renseigné est similaire au code suivant :

```
<Provider type="LDAP" userdirectory="@SMDirName">
   <LDAP searchroot="@SMDirSearchRoot" secure="@SMDirSecure" />
   <Credentials user="@SMDirUser"
     cleartext="true">@SMDirPassword</Credentials>
   <Connection host="@SMDirHost" port="@SMDirPort" />
   <eTrustAdmin domain="@SMDirETrustAdminDomain" />
</Provider>
```

L'élément fournisseur inclut les paramètres suivants :

type

Spécifie le type de base de données. Pour tous les référentiels d'utilisateurs LDAP, spécifiez LDAP (valeur par défaut).

userdirectory

Spécifie le nom de la connexion à l'annuaire d'utilisateurs.

Remarque : Ne spécifiez pas de nom pour la connexion à l'annuaire d'utilisateurs dans le fichier directory.xml. CA Identity Manager vous invite à fournir le nom lors de la création de l'annuaire CA Identity Manager dans la console de gestion.

Remarque : Les paramètres sont facultatifs.

Sous-élément LDAP

Le sous-élément LDAP inclut les paramètres suivants :

Rechercher la racine

Spécifie l'emplacement qui sert de point de départ pour l'annuaire LDAP ; en général, une organisation (o) ou une unité organisationnelle (ou).

secure

Force la connexion SSL (Secure Sockets Layer) à l'annuaire d'utilisateurs LDAP, comme suit :

- True : CA Identity Manager utilise une connexion sécurisée.
- False : CA Identity Manager se connecte à l'annuaire d'utilisateurs sans SSL (valeur par défaut).

Remarque : Les paramètres sont facultatifs.

Sous-élément informations d'identification

Pour se connecter à un annuaire LDAP, CA Identity Manager doit fournir des informations d'identification valides. Ces informations d'identification sont définies dans le sous-élément informations d'identification, similaire au code suivant :

```
<Credentials user="@SMDirUser" cleartext="true">
  "MyPassword"
</Credentials>
```

Si vous ne spécifiez aucun mot de passe dans le sous-élément informations d'identification, CA Identity Manager vous invite à le fournir lors de la création de l'annuaire dans la console de gestion.

Remarque : Il est recommandé de spécifier le mot de passe dans la console de gestion.

Ainsi, CA Identity Manager chiffre le mot de passe pour vous. Dans le cas contraire, si vous ne voulez pas que le mot de passe s'affiche en texte clair, chiffrez le mot de passe à l'aide de l'outil de modification de mots de passe fourni avec CA Identity Manager.

Remarque : Vous pouvez spécifier un seul ensemble d'informations d'identification. Si vous définissez plusieurs annuaires, comme décrit à la section Sous-élément de connexion, les informations d'identification spécifiées doivent s'appliquer à tous les annuaires.

Le sous-élément informations d'identification inclut les paramètres suivants :

utilisateur

Spécifie l'ID de connexion d'un compte pouvant accéder à l'annnuaire.

Pour le provisionnement d'utilisateurs, le compte d'utilisateur que vous spécifiez doit disposer du profil d'administrateur de domaines ou un ensemble équivalent de droits dans le serveur de provisionnement.

Remarque : Ne spécifiez aucune valeur pour le paramètre utilisateur dans le fichier directory.xml. CA Identity Manager vous invite à fournir l'ID de connexion lors de la création de l'annuaire CA Identity Manager dans la console de gestion.

cleartext

Détermine si le mot de passe est affiché en texte clair dans le fichier directory.xml, comme suit :

- True : le mot de passe est affiché en texte clair.
- False : le mot de passe est chiffré (valeur par défaut).

Remarque : Les paramètres sont facultatifs.

Sous-élément connexion

Le sous-élément connexion décrit l'emplacement du référentiel d'utilisateurs géré par CA Identity Manager. Ce sous-élément inclut les paramètres suivants :

hôte

Indique le nom d'hôte ou l'adresse IP du système sur lequel l'annuaire d'utilisateurs est installé.

Remarque : Si le système de connexion a une adresse IPv6, placez l'adresse IP entre crochets ([ ]) comme suit :

<Connection host="[2::9255:214:22ff:fe72:525a]" port="20389"

failover="[2::9255:214:22ff:fe72:525a]:20389"/>

port

Indique le numéro de port de l'annuaire d'utilisateurs.

Basculement

Spécifie le nom d'hôte et l'adresse IP du système sur lequel des référentiels d'utilisateurs redondants existent, dans le cas où le système principal est indisponible. Lorsque le système principal devient à nouveau disponible, le système de basculement est toujours utilisé. Pour réutiliser le système principal, redémarrez le système secondaire. Si plusieurs serveurs sont répertoriés, CA Identity Manager tentera de se connecter aux systèmes dans l'ordre indiqué.

Spécifiez le nom d'hôte et l'adresse IP dans l'attribut de basculement dans une liste *séparée par des espaces,* comme suit :

failover="IPaddress:port IPaddress:port"

Exemple :

<Connection host="123.456.789.001" port="20389"

failover="123,456.789,002:20389 123,456.789,003:20389"/>

Remarque : Le port 20389 est le port par défaut pour le serveur de provisionnement.

Remarque : Les paramètres sont facultatifs.

Sous-élément provisionnement

Si l'environnement CA Identity Manager inclut le provisionnement, définissez le domaine de provisionnement comme suit :

```
<eTrustadmin domain="@SMDirProvisioningDomain" />
```

Le sous-élément provisionnement inclut le paramètre suivant :

domaine

Définit le nom du domaine de provisionnement géré par CA Identity Manager.

Lors de la création de l'annuaire CA Identity Manager dans la console de gestion, vous êtes invité à fournir le nom de domaine. Par conséquent, veillez à spécifier une valeur pour le paramètre de domaine dans le fichier de configuration d'annuaire (directory.xml).

Paramètres de recherche d'annuaire

Vous pouvez définir les paramètres de recherche suivants dans l'élément DirectorySearch :

maxrows

Spécifie le nombre maximum d'objets que CA Identity Manager peut renvoyer lors d'une recherche dans un annuaire d'utilisateurs. Lorsque le nombre d'objets dépasse la limite, une erreur s'affiche.

La définition d'une valeur pour le paramètre maxrows permet de remplacer les paramètres dans l'annuaire LDAP qui limitent les résultats de la recherche. Lorsque des paramètres contradictoires sont appliqués, le serveur LDAP utilise le paramètre dont la valeur est la plus faible.

Remarque : Le paramètre maxrows ne limite pas le nombre d'objets qui sont affichés dans la fenêtre de tâche CA Identity Manager. Pour configurer les paramètres d'affichage, modifiez la définition de la fenêtre de liste dans la console d'utilisateur CA Identity Manager. Pour obtenir des instructions, consultez le Manuel *User Console Design Guide*.

maxpagesize (taille maximale de la page de recherche)

Spécifie le nombre d'objets renvoyés pour une recherche unique. Si le nombre d'objets dépasse la taille de la page, CA Identity Manager effectue plusieurs recherches.

Lors de la spécification du paramètre maxpagesize, tenez compte des points suivants :

- Pour utiliser l'option maxpagesize, le référentiel d'utilisateurs géré par CA Identity Manager doit prendre en charge la pagination. Certains types de référentiel d'utilisateurs requièrent une configuration supplémentaire pour prendre en charge la pagination. Pour plus d'informations, consultez la section Amélioration des performances des recherches volumineuses (page 97).
- Si le référentiel d'utilisateurs ne prend pas en charge la pagination et qu'une valeur pour maxrows est spécifiée, seule la valeur de maxrows est utilisée par CA Identity Manager pour contrôler la taille de la recherche.

délai d'expiration

Spécifie la durée maximum en secondes de la recherche d'un annuaire effectuée par CA Identity Manager avant de prendre fin.

Remarque : L'élément DirectorySearch est facultatif. Toutefois, l'annuaire prend en charge la pagination (page 97) ; il est donc recommandé de spécifier cet élément DirectorySearch.

Descriptions d'objets gérés utilisateur, groupe et organisation

Dans CA Identity Manager, vous gérez les types suivants d'objets correspondant à des entrées dans un annuaire d'utilisateurs :

Utilisateurs

Représentent les utilisateurs dans une entreprise. Un utilisateur appartient à une organisation unique.

Groupes

Représentent des associations d'utilisateurs ayant des éléments en commun.

Organisations

Représentent des unités commerciales. Les organisations contiennent des détails tels que des utilisateurs, des groupes et d'autres organisations.

Une description d'objet contient les informations suivantes :

- Informations sur l'objet (page 118), telles que la classe d'objet LDAP et le conteneur dans lequel il est stocké
- Les attributs qui stockent des informations sur une entrée (page 122). Par exemple, l'attribut récepteur d'appels stocke un numéro de récepteur d'appels.

Remarque : Un environnement CA Identity Manager prend en charge un seul type d'objet utilisateur, groupe et organisation. Par exemple, tous les objets utilisateur ont la même classe d'objet.

Descriptions d'objet géré

Un objet géré est décrit en spécifiant des informations dans les sections Objet utilisateur, Objet groupe et Objet organisation du fichier de configuration d'annuaire.

Remarque : Lors de l'utilisation du modèle de configuration (fichier directory.xml), la section d'objet organisation est indisponible pour les annuaires d'utilisateurs qui ne prennent pas en charge les organisations.

Chaque section contient des éléments ImsManagedObject, comme illustré par l'exemple suivant :

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson" objecttype="USER">
```

De même, l'élément ImsManagedObject peut inclure un élément conteneur, comme illustré par l'exemple suivant :

```
<Container objectclass="top,organizationalUnit" attribute="ou" value="people" />
```

Spécification d'informations d'objet

Les informations d'objet sont spécifiées par des valeurs de différents paramètres.

Procédez comme suit:

1. Recherchez l'élément ImsManagedObject dans la section d'objet utilisateur, d'objet organisation, ou d'objet groupe.
2. Fournissez des valeurs pour les paramètres suivants :

   name

   Spécifie un nom unique pour l'objet géré.

   Remarque : Ce paramètre est obligatoire.

   description

   Contient une description de l'objet géré.

   objectclass

   Spécifie le nom de la classe d'objet LDAP pour le type d'objet (utilisateur, groupe, ou organisation). La classe d'objets détermine la liste d'attributs disponibles pour un objet.

   Si des attributs de différentes classes d'objet s'appliquent à un type d'objet, répertoriez les classes d'objets dans une liste séparée par des virgules. Par exemple, si un objet contient des attributs des classes d'objets person, organizationalperson et inetorgperson, ajoutez ces classes d'objets comme suit :

   objectclass="top,person,organizationalperson,inetorgperson"

   Chaque annuaire LDAP inclut un ensemble de classes d'objets prédéfinies. Pour plus d'informations sur les classes d'objets prédéfinies, consultez la documentation du serveur d'annuaires.

   Remarque : Ce paramètre est obligatoire.

   objecttype

   Spécifie le type de l'objet géré. Les valeurs valides sont les suivantes.

   - Utilisateur
   - Organisation
   - Groupe

   Remarque : Ce paramètre est obligatoire.

   maxrows

   Spécifie le nombre maximum d'objets que CA Identity Manager peut renvoyer lors d'une recherche dans un annuaire d'utilisateurs. Lorsque le nombre d'objets dépasse la limite, une erreur s'affiche.

La définition d'une valeur pour le paramètre maxrows permet de remplacer les paramètres dans l'annuaire LDAP qui limitent les résultats de la recherche. Lorsque des paramètres contradictoires sont appliqués, le serveur LDAP utilise le paramètre dont la valeur est la plus faible.

Remarque : Le paramètre maxrows ne limite pas le nombre d'objets qui sont affichés dans la fenêtre de tâche CA Identity Manager. Pour configurer les paramètres d'affichage, modifiez la définition de la fenêtre de liste dans la console d'utilisateur CA Identity Manager. Pour obtenir des instructions, consultez le Manuel *User Console Design Guide*.

maxpagesize (taille maximale de la page de recherche)

Spécifie le nombre d'objets renvoyés pour une recherche unique. Si le nombre d'objets dépasse la taille de la page, CA Identity Manager effectue plusieurs recherches.

Lors de la spécification de la taille de la page de recherche, tenez compte des points suivants :

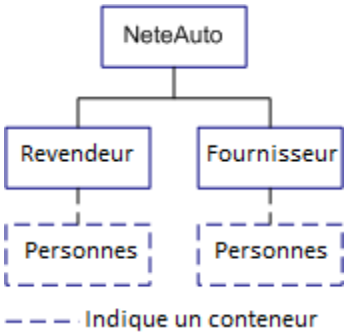
- Pour utiliser l'option Search Page Size (Taille de la page de recherche), le référentiel d'utilisateurs géré par CA Identity Manager doit prendre en charge la pagination. Certains types de référentiel d'utilisateurs requièrent une configuration supplémentaire pour prendre en charge la pagination. Pour plus d'informations, consultez la section Amélioration des performances de recherche (page 97).
- Si le référentiel d'utilisateurs ne prend pas en charge la pagination et qu'une valeur pour maxrows est spécifiée, seule la valeur de maxrows est utilisée par CA Identity Manager pour contrôler la taille de la recherche.

3. Vous pouvez également fournir des informations sur le conteneur.

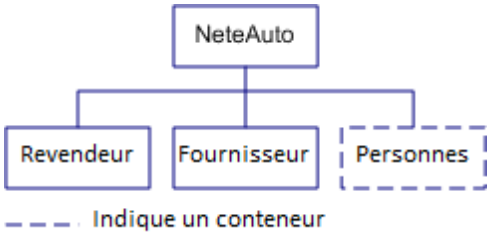
Conteneurs

Pour simplifier l'administration, vous pouvez grouper des objets de type spécifique dans un conteneur. Lorsque vous spécifiez un conteneur dans le fichier de configuration d'annuaire, CA Identity Manager gère uniquement les entrées dans le conteneur. Par exemple, si vous spécifiez un conteneur d'utilisateurs appelés People, CA Identity Manager gère les utilisateurs dans le conteneur People, comme illustré dans les exemples suivantes :

- Annuaire hiérarchique



- Annuaire non hiérarchique



Dans ces exemples, tous les utilisateurs existent dans les conteneurs People.

Lorsque vous spécifiez un conteneur, tenez compte des points suivants :

- Si aucun conteneur n'existe dans une organisation, CA Identity Manager créera le conteneur dès l'ajout de la première entrée. Dans le cas d'un annuaire hiérarchique, CA Identity Manager créera le conteneur dans l'organisation dans laquelle l'entrée est ajoutée. Dans le cas d'annuaires non hiérarchique et ne prenant pas en charge les organisations, CA Identity Manager créera le conteneur sous la racine de recherche, que vous spécifiez lors de la création de l'annuaire CA Identity Manager.
- CA Identity Manager ignore les entrées non comprises dans le conteneur spécifié. Par exemple, si vous spécifiez le conteneur People, vous ne pouvez pas gérer les utilisateurs existant à l'extérieur de ce conteneur People.

  Remarque : Pour gérer des utilisateurs non inclus dans le conteneur spécifié, vous pouvez créer un autre environnement CA Identity Manager.

Conteneurs et attributs connus

Les attributs connus sont des attributs qui ont signification spéciale dans CA Identity Manager. Lorsque CA Identity Manager gère un référentiel d'utilisateurs comprenant des conteneurs, les attributs connus suivants identifient les informations sur le conteneur :

%ORG_MEMBERSHIP%

Identifie l'attribut qui stocke le nom complet (nom unique) du conteneur.

Par exemple, le nom complet peut être similaire au suivant :

ou=People, ou=Employee, ou=NeteAuto, dc=security, dc=com

%ORG_MEMBERSHIP_NAME%

Identifie l'attribut qui stocke le nom convivial de l'attribut.

Par exemple, le nom convivial du conteneur dans l'exemple précédent est People.

Ces attributs connus s'affichent dans les descriptions d'attribut des sections d'objets utilisateur et groupe du fichier directory.xml, comme suit :

```
 <ImsManagedObjectAttr physicalname="someattribute" description="Organization"
displayname="Organization" valuetype="String" required="true"
wellknown="%ORG_MEMBERSHIP%" maxlength="0" permission="WRITEONCE"
searchable="false" />
```

Dans le cas de structures de référentiel d'utilisateurs hiérarchiques, les paramètres physicalname et wellknown sont mappés vers l'attribut connu comme suit :

```
<ImsManagedObjectAttr physicalname="%ORG_MEMBERSHIP%" description="Organization"
displayname="Organization" valuetype="String" required="true"
wellknown="%ORG_MEMBERSHIP%" maxlength="0" permission="WRITEONCE"
searchable="false" />
```

L'exemple indique que CA Identity Manager dérive automatiquement le nom unique et le nom convivial du conteneur d'autres informations dans le fichier directory.xml.

Dans le cas de structures de référentiel d'utilisateurs non hiérarchiques, fournissez les noms d'attributs physiques.

Remarque : Pour obtenir des instructions, consultez la section Description d'une structure d'annuaires d'utilisateurs non hiérarchiques (page 87).

Spécification d'un conteneur d'utilisateurs ou de groupes

Pour spécifier un conteneur d'utilisateurs ou de groupes, suivez la procédure suivante.

Procédez comme suit:

1. Recherchez l'élément conteneur dans la section d'objet utilisateur, d'objet organisation, ou d'objet groupe.
2. Fournissez des valeurs pour les paramètres suivants :

   objectclass

   Spécifie la classe d'objet LDAP du conteneur dans lequel les objets d'un certain type sont créés. Par exemple, la valeur par défaut pour le conteneur d'utilisateurs est top,organizationalUnit, ce qui indique que les utilisateurs sont créés dans des unités organisationnelles LDAP (ou).

   Lors de la gestion de groupes dynamiques ou imbriqués, veillez à spécifier un objectclass prenant en charge ces types de groupe (page 88).

   Remarque : Ce paramètre est obligatoire.

   attribute

   Spécifie l'attribut qui référence le nom de conteneur, par exemple, ou.

   L'attribut est associé à la valeur pour former le nom unique relatif du conteneur, comme dans l'exemple suivant :

   ou=People

   Remarque : Ce paramètre est obligatoire.

   value

   Spécifie le nom du conteneur.

   Remarque : Ce paramètre est obligatoire.

Remarque : Vous ne pouvez pas spécifier de conteneurs pour les organisations.

Descriptions d'attribut

Un attribut stocke des informations concernant une entrée, telles qu'un numéro de téléphone ou une adresse. Un attribut d'entrée détermine son profil.

Dans le fichier de configuration d'annuaire, les attributs sont décrits dans les éléments ImsManagedObjectAttr. Dans les sections d'objet utilisateur, d'objet groupe et d'objet organisation du fichier de configuration d'annuaire, vous pouvez réaliser les actions suivantes :

- Modification de descriptions d'attribut par défaut pour décrire les attributs de votre référentiel d'utilisateurs
- Création de descriptions d'attribut en copiant une description existante et en modifiant des valeurs le cas échéant

Pour chaque attribut dans les profils d'utilisateur, de groupe et d'organisation, il existe un élément ImsManagedObjectAttr. Par exemple, un élément ImsManagedObjectAttr est décrit comme ID d'utilisateur.

Un élément ImsManagedObjectAttr est similaire au code suivant :

```
<ImsManagedObjectAttr physicalname="uid" displayname="User ID" description="User ID" valuetype="String" required="true" multivalued="false" wellknown="%USER_ID%" maxlength="0" />
```

ImsManagedObjectAttr possède les paramètres suivants :

physicalname

Ce paramètre doit contenir l'un des éléments suivants :

- Le nom de l'attribut LDAP où la valeur de profil est stockée. Par exemple, l'ID d'utilisateur est stocké dans l'attribut uid dans l'annuaire d'utilisateurs.

  Remarque : Pour améliorer les performances, indexez les attributs LDAP utilisés dans des requêtes de recherche dans la console d'utilisateur.

- Un attribut connu (page 79). Lorsque vous fournissez un attribut connu, CA Identity Manager calcule la valeur automatiquement. Par exemple, si vous spécifiez un attribut connu %ORG_MEMBERSHIP%, CA Identity Manager déterminera l'organisation à laquelle l'entrée appartient, en fonction du nom unique d'une entrée.

description

Contient la description de l'attribut.

displayName

Spécifie un nom unique pour l'attribut.

Dans la console d'utilisateur, le nom d'affichage s'affiche dans la liste d'attributs disponibles pour être ajoutés à une fenêtre de tâche. Ce paramètre est obligatoire.

Remarque : Ne modifiez pas le nom d'affichage d'un attribut dans le fichier de configuration d'annuaire (directory.xml). Pour modifier le nom de l'attribut dans une fenêtre de tâche, vous pouvez spécifier une étiquette pour l'attribut dans la définition de la fenêtre de tâche. Pour plus d'informations, consultez le *Manuel d'administration*.

valuetype

Spécifie le type de données de l'attribut. Les valeurs valides sont les suivantes.

Chaîne

La valeur peut être une chaîne.

C'est la valeur par défaut.

Integer

La valeur doit être un nombre entier.

Remarque : Le nombre entier ne prend pas en charge les nombres décimaux.

Number

La valeur doit être un nombre entier. L'option de nombre prend en charge les nombres décimaux.

Date

La valeur doit analyser une date valide à l'aide du modèle suivant :

MM/JJ/AAAA

ISODate

La valeur doit analyser une date valide à l'aide du modèle MM-JJ-AAAA.

UnicenterDate

La valeur doit analyser une date valide à l'aide du modèle YYYYYYYDDD où :

YYYYYYY est une représentation à 7 chiffres pour une année commençant par 3 zéros. Par exemple : 0002008

DDD est la représentation à 3 chiffres du jour commençant par des zéros, le cas échéant. Les valeurs valides sont comprises dans la plage de 001 à 366.

Structuré

Ce type d'attribut est composé de données structurées qui permettent à une valeur d'attribut unique de stocker plusieurs valeurs liées. Par exemple, un attribut structuré contient des valeurs telles que le prénom, le nom et l'adresse électronique.

Certains types de terminal utilisent ces attributs, mais sont gérés à travers CA Identity Manager.

Remarque : CA Identity Manager peut afficher des attributs structurés dans une table de la console d'utilisateur. Lorsque des utilisateurs modifient des valeurs dans la table, ces valeurs sont stockées dans le référentiel d'utilisateurs et propagées vers le terminal. Pour plus d'informations sur l'affichage des attributs à valeurs multiples, reportez-vous au *Manuel d'administration*.

required

Indique si l'attribut est requis, comme suit :

- True : l'attribut est requis.
- False : l'attribut est facultatif (valeur par défaut).

Remarque : Si un attribut est requis pour un serveur d'annuaires LDAP, définissez le paramètre required sur True.

multivalued (valeurs multiples)

Indique si l'attribut peut posséder plusieurs valeurs. Par exemple, l'attribut d'appartenance au groupe a plusieurs valeurs pour stocker le nom unique d'utilisateur de chaque membre de groupe. Les valeurs valides sont les suivantes.

- True : l'attribut peut posséder plusieurs valeurs.
- False : l'attribut doit posséder une seule valeur (valeur par défaut).

Important : Les attributs d'appartenance au groupe et de rôles d'administration dans la définition de l'objet utilisateur doivent posséder plusieurs valeurs.

wellknown (connu)

Définit le nom de l'attribut connu.

Les attributs connus ont une signification spécifique dans CA Identity Manager (page 79). Ils sont identifiés dans la syntaxe suivante :

%ATTRIBUTENAME%

maxlength (longueur maximum)

Définit la longueur maximum d'une valeur d'attribut. Pour spécifier une longueur illimitée, définissez le paramètre maxlength sur 0.

Remarque : Ce paramètre est obligatoire.

permission

Indique si vous pouvez modifier la valeur d'un attribut dans une fenêtre de tâche. Les valeurs valides sont les suivantes.

READONLY (lecture seule)

La valeur est affichée, mais ne peut pas être modifiée.

WRITEONCE (écriture unique)

La valeur peut être modifiée une fois l'objet créé. Par exemple, un ID d'utilisateur peut être modifié uniquement après la création de l'utilisateur.

READWRITE (lecture et écriture)

Vous pouvez modifier la valeur (valeur par défaut).

hidden

Indique si un attribut apparaît dans des formulaires de tâche CA Identity Manager. Les valeurs valides sont les suivantes.

- True : l'attribut n'est pas affiché pour les utilisateurs.
- False : l'attribut est affiché pour les utilisateurs (valeur par défaut).

Les attributs logiques utilisent des attributs masqués.

Remarque : Pour plus d'informations, reportez-vous au manuel *Programming Guide for Java*.

system

Spécifie uniquement des attributs utilisés par CA Identity Manager. Les utilisateurs dans la console d'utilisateur ne peuvent pas modifier les attributs. Les valeurs valides sont les suivantes.

- True : les utilisateurs ne peuvent pas modifier l'attribut. L'attribut est masqué dans l'interface utilisateur CA Identity Manager.
- False : les utilisateurs peuvent modifier cet attribut. L'attribut est disponible pour être ajouté à des fenêtres de tâche dans l'interface utilisateur CA Identity Manager. (action par défaut).

validationruleset

Associe un ensemble de règles de validation à l'attribut.

Vérifiez que l'ensemble de règles de validation spécifié est défini dans un élément ValidationRuleSet du fichier de configuration d'annuaire.

objectclass

Indique la classe auxiliaire LDAP d'un attribut utilisateur, groupe, ou organisation lorsque cet attribut ne fait pas partie de l'objectclass principal spécifié dans l'élément ImsManagedObject.

Par exemple, supposons que la classe d'objet principal des utilisateurs est top, person et organizationalperson, qui définit les attributs utilisateur suivants :

- nom commun (cn)
- nom de famille (sn)
- ID d'utilisateur (uid)
- mot de passe (userPassword)

Pour inclure l'attribut employeeID, qui est défini dans la classe d'auxiliaire Employee, vous ajoutez la description d'attribut suivante :

```
<ImsManagedObjectAttr physicalname="employeeID" displayname="Employee ID"
description="Employee ID" valuetype="String" required="true" multivalued="false"
maxlength="0" objectclass="Employee"/>
```

Spécification de descriptions d'attributs

La description d'attributs implique les étapes suivantes :

1. Lisez les sections pertinentes parmi les rubriques suivantes :
   - Remarques relatives à CA Directory (page 77)
   - Remarques relatives à Microsoft Active Directory (page 78)
   - Remarques relatives au serveur d'annuaires IBM (page 78)
   - Remarques relatives à l'annuaire Internet Oracle (page 79)
2. Dans les sections d'objet utilisateur, d'objet groupe et d'objet organisation du fichier de configuration d'annuaire, effectuez les actions suivantes :
   - Modifiez des descriptions d'attributs par défaut et décrivez vos attributs d'annuaire.
   - Créez des descriptions d'attributs en copiant une description existante et en modifiant des valeurs le cas échéant.

   Remarque : Supposons qu'une nouvelle description d'attribut est créée et qu'un attribut physique est spécifié. Veillez à ce que l'attribut physique existe dans la ou les classes d'objets spécifiées pour le type d'objet.
3. (Facultatif) Modifiez les paramètres d'affichage (page 74) de l'attribut pour éviter l'affichage d'informations confidentielles, telles que les mots de passe ou les salaires, dans la console d'utilisateur.
4. (Facultatif) Configurez un ordre de tri par défaut.
5. Si vous gérez un annuaire avec une structure d'utilisateur hiérarchique ou non hiérarchique, ou un annuaire sans organisation, consultez la section Description de la structure d'annuaire d'utilisateurs (page 86).

Gestion des attributs sensibles

CA Identity Manager fournit les méthodes suivantes pour la gestion des attributs sensibles :

- Classifications de données des attributs

  Les classifications de données permettent de spécifier des propriétés d'affichage et de chiffrement pour des attributs dans le fichier de configuration d'annuaire (directory.xml).

  Vous pouvez définir des classifications de données qui gèrent des attributs sensibles comme suit :

  - Dans les fenêtres de tâche CA Identity Manager, affichez la valeur d'un attribut sous forme d'une série d'astérisques.

    Par exemple, vous pouvez afficher des mots de passe sous forme d'astérisques au lieu de les afficher en texte clair.

  - Dans les fenêtres Afficher les tâches soumises, masquez la valeur d'attribut.

    Cette option permet de masquer des attributs pour les administrateurs. Par exemple, vous pouvez masquer les détails des salaires pour des administrateurs qui consultent le statut des tâches dans CA Identity Manager, mais n'ont pas besoin de connaître les détails des salaires.

  - Ignorez certains attributs lors de la création d'une copie d'un objet existant.

  - Chiffrez un attribut.

- Styles de champ dans les fenêtres de profil de tâche

  Si vous ne voulez pas modifier d'attributs dans le fichier directory.xml, définissez la propriété d'affichage de l'attribut dans les définitions de fenêtres dans lesquelles l'attribut sensible apparaît.

  Le style de champ permet d'afficher des attributs, tels que des mots de passe, sous forme de série d'astérisques au lieu du texte clair.

  Remarque : Pour plus d'informations sur le style de champ des attributs sensibles, recherchez les styles de champ dans l'aide de la console d'utilisateur.

Attributs de classification de données

L'élément de classification des données fournit une méthode permettant d'associer des propriétés supplémentaires à une description d'attribut. Les valeurs de cet élément déterminent la gestion par CA Identity Manager de l'attribut. Cet élément prend en charge les paramètres suivants :

- sensitive

  CA Identity Manager affichera l'attribut sous forme d'une série d'astérisques (*) dans les fenêtres Afficher les tâches soumises. Ce paramètre empêche les valeurs anciennes et nouvelles de l'attribut de s'afficher en texte clair dans les fenêtres Afficher les tâches soumises.

  En outre, si vous créez une copie d'un utilisateur existant dans la console d'utilisateur, ce paramètre empêchera l'attribut d'être copié vers le nouvel utilisateur.

- vst_hide

  Masque l'attribut dans la fenêtre Détails de l'événement de l'onglet Afficher les tâches soumises. Contrairement aux attributs sensibles, qui sont affichés sous forme d'astérisques, les attributs vst_hidden ne sont pas affichés.

  Vous pouvez utiliser ce paramètre pour éviter que les modifications apportées à un attribut, tel que le salaire, ne s'affichent dans Afficher les tâches soumises.

- ignore_on_copy

  CA Identity Manager ignore un attribut lorsqu'un administrateur crée une copie d'un objet dans la console d'utilisateur. Par exemple, supposons que vous avez spécifié ignore_on_copy pour l'attribut de mot de passe sur un objet d'utilisateur. Lors de la copie d'un profil d'utilisateur, CA Identity Manager n'appliquera pas le mot de passe de l'utilisateur actuel au nouveau profil d'utilisateur.

- AttributeLevelEncrypt

  Chiffre les valeurs d'attribut si elles sont stockées dans le référentiel d'utilisateurs. Si la norme FIPS 140-2 est activée pour CA Identity Manager, CA Identity Manager utilisera le chiffrement RC2 ou FIPS 140-2.

  Pour plus d'informations sur la prise en charge de FIPS 140-2 dans CA Identity Manager, consultez le *Manuel de configuration*.

  Les attributs s'affichent en texte clair pendant l'exécution.

  Remarque : Pour éviter que des attributs s'affichent en texte clair dans des fenêtres, vous pouvez également ajouter un élément de classification de données sensibles à des attributs chiffrés. Pour plus d'informations, consultez la section Ajout du chiffrement de niveau attribut (page 75).

- PreviouslyEncrypted

  CA Identity Manager détecte et déchiffre toute valeur chiffrée dans l'attribut lors de l'accès à l'objet dans le référentiel d'utilisateurs.

  Utilisez cette classification de données pour déchiffrer toute valeur préalablement chiffrée.

  La valeur du texte clair est enregistrée dans le référentiel lors de l'enregistrement de l'objet.

Configuration des attributs de classification de données

Procédez comme suit:

1. Recherchez l'attribut dans le fichier de configuration d'annuaire.
2. Après la description d'attribut, ajoutez l'attribut suivant :

   <DataClassification name="*parameter*">

   parameter

   Représente l'un des paramètres suivants :

   sensitive

   vst_hide

   ignore_on_copy

   AttributeLevelEncrypt

   PreviouslyEncrypted

   Par exemple, une description d'attribut qui inclut l'attribut de classification de données vst_hide est similaire au code suivant :

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false" multivalued="false"
maxlength="0">
    <DataClassification name="vst_hide"/>
```

Chiffrement de niveau attribut

Vous pouvez chiffrer un attribut dans le référentiel d'utilisateurs en spécifiant la classification de données AttributeLevelEncypt pour cet attribut dans le fichier de configuration d'annuaire (directory.xml). Lorsque le chiffrement de niveau attribut est activé, CA Identity Manager chiffre la valeur de cet attribut avant de la stocker dans le référentiel d'utilisateurs. L'attribut est affiché en texte clair dans la console d'utilisateur.

Remarque : Pour éviter que des attributs s'affichent en texte clair dans des fenêtres, vous pouvez également ajouter un élément de classification de données sensibles à des attributs chiffrés. Pour plus d'informations, consultez la section Ajout du chiffrement de niveau attribut (page 75).

Si la prise en charge de FIPS 140-2 est activée, l'attribut sera chiffré à l'aide du chiffrement RC2 ou FIPS 140-2.

Avant d'implémenter le chiffrement de niveau attribut, tenez compte des points suivants :

- CA Identity Manager ne peut pas détecter les attributs chiffrés dans une recherche.

  Supposons qu'un attribut chiffré est ajouté à une stratégie de membre, d'administration, de propriété, ou d'identités. CA Identity Manager ne peut pas résoudre correctement la stratégie, car il ne peut pas rechercher l'attribut.

  Prévoyez de définir l'attribut sur searchable="false" dans le fichier directory.xml. Par exemple :

  <ImsManagedObjectAttr physicalname="title" description="Title" displayname="Title" valuetype="String" maxlength="0" searchable="false">

  <DataClassification name="AttributeLevelEncrypt"/>

  </ImsManagedObjectAttr>

- Si CA Identity Manager utilise un référentiel d'utilisateurs partagé et un annuaire de provisionnement, ne chiffrez pas les attributs du serveur de provisionnement.
- N'activez pas AttributeLevelEncrypt pour les mots de passe d'utilisateur dans les environnements conformes aux critères suivants :
  - Intégration de CA SiteMinder
  - Stockage d'utilisateurs dans une base de données relationnelles

  Lorsque CA Identity Manager comprend CA SiteMinder, les mots de passe chiffrés entraînent des problèmes lorsque des utilisateurs nouveaux tentent de se connecter et saisissent leur mot de passe en texte clair.
- Si vous activez le chiffrement de niveau attribut pour un référentiel d'utilisateurs utilisé par d'autres applications que CA Identity Manager, elles ne pourront pas utiliser l'attribut chiffré.

Ajout du chiffrement de niveau attribut

Supposons que vous avez ajouté un chiffrement de niveau attribut à un annuaire CA Identity Manager. CA Identity Manager chiffre automatiquement les valeurs d'attributs en texte clair existants lors de l'enregistrement de l'objet associé à l'attribut. Par exemple, le chiffrement de l'attribut de mot de passe permet de chiffrer le mot de passe lors de l'enregistrement du profil de l'utilisateur.

Remarque : Pour chiffrer la valeur d'un attribut, la tâche utilisée pour enregistrer l'objet doit inclure cet attribut. Pour chiffrer l'attribut de mot de passe dans l'exemple précédent, veillez à ce que le champ de mot de passe soit ajouté à la tâche utilisée pour enregistrer l'objet, telle que la tâche Modifier un utilisateur.

Tous les nouveaux objets sont créés avec des valeurs chiffrées dans le référentiel d'utilisateurs.

Procédez comme suit:

1. Effectuez l'une des tâches suivantes :
   - Création d'un annuaire CA Identity Manager
   - Mise à jour d'un annuaire existant via l'exportation des paramètres d'annuaire
2. Ajout des attributs de classification de données suivants à l'attribut que vous voulez chiffrer dans le fichier directory.xml :

   AttributeLevelEncrypt

   Conserve la valeur de l'attribut sous forme chiffré dans le référentiel d'utilisateurs.

   sensitive (facultatif)

   Masque la valeur de l'attribut dans les fenêtres CA Identity Manager. Par exemple, un mot de passe s'affiche sous forme d'astérisques (*).

   Exemple :

```
<ImsManagedObjectAttr physicalname="salary"
displayname="Salary" description="salary" valuetype="String"
required="false" multivalued="false" maxlength="0"
searchable="false">
<DataClassification name="AttributeLevelEncrypt"/>
<DataClassification name="sensitive"/>
```

3. Si vous avez créé un annuaire CA Identity Manager, associez-le à un environnement.
4. Pour forcer CA Identity Manager à chiffrer toutes les valeurs immédiatement, modifiez tous les objets à l'aide du chargeur en bloc.

   Remarque : Pour plus d'informations sur le chargeur en bloc, consultez le *Manuel d'administration*.

Suppression du chiffrement de niveau attribut

Si vous avez un attribut chiffré dans l'annuaire CA Identity Manager, stocké avec la valeur en texte clair, vous pouvez supprimer la classification de données AttributeLevelEncrypt.

Une fois la classification de données supprimée, CA Identity Manager arrête de chiffrer les nouvelles valeurs d'attribut. Les valeurs existantes sont déchiffrées lors de l'enregistrement de l'objet à l'attribut.

Remarque : Pour déchiffrer la valeur d'un attribut, la tâche utilisée pour enregistrer l'objet doit inclure cet attribut. Par exemple, pour déchiffrer le mot de passe d'un utilisateur existant, enregistrez l'objet d'utilisateur avec une tâche qui inclut le champ de mot de passe, telles que la tâche Modifier un utilisateur.

Pour forcer CA Identity Manager à détecter et déchiffrer toute valeur de l'attribut chiffrée conservée dans le référentiel d'utilisateurs, vous pouvez spécifier une autre classification de données : PreviouslyEncrypted. La valeur du texte clair est enregistrée dans le référentiel d'utilisateurs lors de l'enregistrement de l'objet.

Remarque : L'ajout de la classification de données PreviouslyEncrypted ajoute un traitement supplémentaire sur chaque chargement d'objet. Pour éviter tout problème de performance, envisagez d'ajouter la classification de données PreviouslyEncrypted, en chargeant et en enregistrant chaque objet associé à cet attribut, puis en supprimant la classification de données. Cette méthode convertit automatiquement toutes les valeurs chiffrées stockées en texte clair stocké.

Procédez comme suit:

1. Exportez les paramètres de l'annuaire CA Identity Manager approprié.
2. Dans le fichier directory.xml, supprimez la classification de données AttributeLevelEncrypt des attributs que vous voulez déchiffrer.
3. Si vous voulez forcer CA Identity Manager à supprimer préalablement des valeurs chiffrées, ajoutez l'attribut de classification de données PreviouslyEncrypted.

   Exemple :

   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false" multivalued="false"
   maxlength="0" searchable="false">
   <DataClassification name="PreviouslyEncrypted"/>
   ```

4. Pour forcer CA Identity Manager à déchiffrer toutes les valeurs immédiatement, modifiez tous les objets à l'aide du chargeur en bloc.

   Remarque : Pour plus d'informations sur le chargeur en bloc, consultez le *Manuel d'administration*.

Remarques relatives à CA Directory

Lorsque vous décrivez des attributs d'un référentiel d'utilisateurs CA Directory, tenez compte des points suivants :

- Les noms d'attribut sont sensibles à la casse.
- L'utilisation de l'attribut seeAlso comme attribut indiquant un groupe avec auto-abonnement peut entraîner des erreurs lorsque les administrateurs créent des groupes.

L'utilisation de l'attribut photo comme attribut indiquant le statut d'un compte d'utilisateur (activé ou désactivé) peut entraîner des erreurs lorsqu'un administrateur crée un utilisateur.

Remarque : Pour des informations supplémentaires sur la configuration requise de CA Directory, consultez la documentation CA Directory.

Remarques relatives à Microsoft Active Directory

Lorsque vous décrivez des attributs pour Active Directory, tenez compte des points suivants :

- La casse des attributs spécifiés dans les descriptions doit correspondre à la casse des attributs dans Active Directory. Par exemple, lorsque vous sélectionnez l'attribut unicodePwd comme attribut de stockage de mots de passe d'utilisateur, spécifiez unicodePwd (avec un P majuscule) dans le fichier de configuration d'annuaire.
- Pour des objets utilisateur et groupe, veillez à inclure l'attribut sAMAccountName.

Remarques relatives au serveur d'annuaires IBM

Lorsque vous décrivez des attributs d'un annuaire d'utilisateurs de serveur d'annuaires IBM, consultez les sections suivantes :

- Groupes inclus dans les annuaires de serveur d'annuaires (page 78)
- Objectclass Top dans la description d'objet organisation (page 79)

Groupes inclus dans les annuaires de serveur d'annuaires

Le serveur d'annuaires IBM requiert que les groupes contiennent au moins un membre. Pour répondre à cette condition, CA Identity Manager ajoute un *utilisateur factice* comme membre d'un groupe lors de sa création.

Configuration d'un utilisateur factice

Procédez comme suit:

1. Dans la section d'objet groupe du fichier de configuration d'annuaire, recherchez les éléments suivants :

   ```
   <PropertyDict name="DUMMY_USER">
       <Property name="DUMMY_USER_DN">##DUMMY_USER_DN</Property>
   </PropertyDict>
   ```

   Remarque : Si ces éléments n'existent pas dans le fichier de configuration d'annuaire, ajoutez-les exactement tels qu'ils apparaissent ici.

2. Remplacez ##DUMMY_USER_DN par un nom unique d'utilisateur. CA Identity Manager ajoute ce nom unique comme membre de tous les nouveaux groupes.

   Remarque : Si vous spécifiez le nom unique d'un utilisateur existant, cet utilisateur s'affichera comme membre de tous les groupes CA Identity Manager. Pour éviter que l'*utilisateur factice* apparaisse comme membre d'un groupe, spécifiez un nom unique qui n'existe pas dans l'annuaire.

3. Enregistrez le fichier de configuration d'annuaire.

Objectclass Top dans la description d'objet organisation

Important : Dans la description de l'objet organisation dans le fichier de configuration d'annuaire, n'incluez pas l'objectclass top.

Par exemple, lorsque l'objectclass de l'objet organisation est top, organizationalUnit, spécifiez l'objectclass comme suit :

```
<ImsManagedObject name="Organization" description="My Organizations"
objectclass="organizationalUnit" objecttype="ORG">
```

L'inclusion de top peut entraîner des résultats de recherche inattendus.

Remarques relatives à l'annuaire Internet Oracle

Lorsque vous décrivez des attributs d'un référentiel d'utilisateurs d'annuaire Internet Oracle (ID d'objet), spécifiez des attributs LDAP en minuscule uniquement.

Attributs connus pour un référentiel d'utilisateurs LDAP

Les attributs connus ont une signification spécifique dans CA Identity Manager. Ils sont identifiés comme illustré dans la syntaxe suivante :

%ATTRIBUTENAME%

Dans cette syntaxe, *ATTRIBUTENAME* doit être en majuscule.

Un attribut connu est mappé vers un attribut physique, à l'aide d'une description d'attribut (page 122).

Dans la description d'attribut suivante, l'attribut userpassword est mappé vers l'attribut connu %PASSWORD% de sorte que CA Identity Manager traite la valeur dans userpassword comme mot de passe, de la manière suivante :

```
<ImsManagedObjectAttr
        physicalname="userpassword"
        displayname="Password"
        description="Password"
        valuetype="String"
        required="false"
        multivalued="false"
        wellknown="%PASSWORD%"
        maxlength="0" />
```

Certains attributs connus sont requis ; d'autres sont facultatifs.

Attributs connus d'utilisateur

Voici une liste d'attributs connus d'utilisateur et les éléments vers lesquels ils sont mappés :

%ADMIN_ROLE_CONSTRAINT%

Mappe vers la liste de rôles d'administration d'un administrateur.

L'attribut physique mappé vers %ADMIN_ROLE_CONSTRAINT% doit posséder plusieurs valeurs pour prendre en charge plusieurs rôles.

Il est recommandé d'indexer l'attribut LDAP mappé vers %ADMIN_ROLE_CONSTRAINT%.

%CERTIFICATION_STATUS%

Mappe vers le statut de certification d'un utilisateur.

Cet attribut est requis pour l'utilisation de la fonctionnalité de certification d'utilisateur.

Remarque : Pour plus d'informations sur la certification d'utilisateur, consultez le *Manuel d'administration*.

%DELEGATORS%

Mappe vers une liste d'utilisateurs ayant délégué des tâches à l'utilisateur actuel.

Cet attribut est requis pour utiliser la délégation. L'attribut physique de mappage vers %DELEGATORS% doit être de valeurs multiples et en mesure de stocker des chaînes.

Important : La modification de ce champ directement à l'aide de tâches CA Identity Manager ou d'un outil externe peut affecter la sécurité de manière significative.

%EMAIL%

Mappe vers l'adresse électronique d'un utilisateur.

Requis pour l'utilisation de la fonctionnalité de notification par courriel.

%ENABLED_STATE%

(requis)

Mappe vers le statut d'un utilisateur.

Remarque : Cet attribut doit correspondre à l'attribut d'annuaire d'utilisateurs Indicateur désactivé dans la connexion à l'annuaire d'utilisateurs SiteMinder.

%FIRST_NAME%

Mappe vers le prénom d'un utilisateur.

%FULL_NAME%

Mappe vers les nom et prénom d'un utilisateur.

%IDENTITY_POLICY%

Spécifie la liste de stratégies d'identité appliquées à un compte d'utilisateur et une liste d'ID de stratégie Policy Xpress uniques qui ont réalisé des actions d'ajout ou de suppression sur l'objet utilisateur.

CA Identity Manager utilise cet attribut pour déterminer si l'application d'une stratégie d'identité à un utilisateur est requise ou non. Supposons que le paramètre Apply Once (Appliquer une fois) de la stratégie est activé et que la stratégie est répertoriée dans l'attribut %IDENTITY_POLICY%. CA Identity Manager n'applique pas les modifications de la stratégie à l'utilisateur.

Remarque : Pour plus d'informations sur les stratégies d'identité, consultez le *Manuel d'administration*.

%LAST_CERTIFIED_DATE%

Mappe vers la date lorsque les rôles sont certifiés pour un utilisateur.

Requis pour l'utilisation de la fonctionnalité de certification d'utilisateur.

Remarque : Pour plus d'informations sur la certification d'utilisateur, consultez le *Manuel d'administration*.

%LAST_NAME%

Mappe vers le nom d'un utilisateur.

%MEMBER_OF%

Mappe vers la liste de groupes dont l'utilisateur est membre.

L'attribut physique mappé vers %MEMBER_OF% doit posséder plusieurs valeurs pour prendre en charge plusieurs groupes.

Cet attribut permet de gagner du temps de réponse lors de la recherche de groupes d'un utilisateur.

Vous pouvez utiliser cet attribut avec Active Directory ou un autre schéma d'annuaire qui gère l'appartenance à un groupe d'un utilisateur sur l'objet utilisateur.

%ORG_MEMBERSHIP%

(requis)

Mappe vers le nom unique de l'organisation à laquelle l'utilisateur appartient.

CA Identity Manager utilise cet attribut connu pour déterminer la structure d'un annuaire (page 86).

Cet attribut n'est pas requis si l'annuaire d'utilisateurs n'inclut pas d'organisations.

%ORG_MEMBERSHIP_NAME%

(requis)

Mappe vers le nom convivial de l'organisation dans laquelle le profil de l'utilisateur existe.

Cet attribut n'est pas requis si l'annuaire d'utilisateurs n'inclut pas d'organisations.

%PASSWORD%

Mappe vers le mot de passe d'un utilisateur.

Cet attribut doit correspondre à l'attribut Password dans la connexion à l'annuaire d'utilisateurs SiteMinder.

Remarque : La valeur de l'attribut %PASSWORD% apparaît toujours sous forme de série d'astérisque (*) dans les fenêtres CA Identity Manager, même lorsque l'attribut ou le champ n'est pas défini pour masquer les mots de passe.

%PASSWORD_DATA%

(requis pour la prise en charge de la stratégie de mot de passe)

Spécifie l'attribut de suivi des informations de stratégie de mot de passe.

Remarque : La valeur de l'attribut %PASSWORD_DATA% apparaît toujours sous forme de série d'astérisque (*) dans les fenêtres CA Identity Manager, même lorsque l'attribut ou le champ n'est pas défini pour masquer les mots de passe.

%PASSWORD_HINT%

(requis)

Mappe vers une paire de question/réponse spécifiée par l'utilisateur. La paire de question/réponse est utilisée lorsque l'utilisateur oublie son mot de passe.

Pour prendre en charge plusieurs paires de question/réponse, veillez à ce que l'attribut %PASSWORD_HINT% possède plusieurs valeurs.

Si vous utilisez la fonctionnalité de services de mot de passe de SiteMinder pour gérer des mots de passe, l'attribut Password Hint (Indice de mot de passe) doit correspondre à l'attribut Challenge/Response (Demande d'accès/réponse) dans l'annuaire d'utilisateurs SiteMinder.

Remarque : La valeur de l'attribut %PASSWORD% apparaît toujours sous forme de série d'astérisque (*) dans les fenêtres CA Identity Manager, même lorsque l'attribut ou le champ n'est pas défini pour masquer les mots de passe.

%USER_ID%

(requis)

Mappe vers l'ID d'un utilisateur.

Attributs connus de groupe

Voici la liste d'attributs connus de groupe :

%GROUP_ADMIN_GROUP%

Indique l'attribut contenant une liste de groupes qui sont des administrateurs du groupe. Par exemple, si le groupe 1 est un administrateur du groupe A, le groupe 1 est stocké dans l'attribut %GROUP_ADMIN_GROUP%.

Remarque : Si vous ne spécifiez pas d'attribut %GROUP_ADMIN_GROUP%, CA Identity Manager stocke les groupes d'administrateurs dans l'attribut %GROUP_ADMIN%.

Remarque : Pour ajouter un groupe comme administrateur d'un autre groupe, consultez le *Manuel d'administration*.

%GROUP_ADMIN%

Indique l'attribut contenant les noms uniques d'administrateurs d'un groupe.

L'attribut physique mappé vers %GROUP_ADMIN% doit posséder plusieurs valeurs.

%GROUP_DESC%

Indique l'attribut contenant la description d'un groupe.

%GROUP_MEMBERSHIP%

(requis)

Indique l'attribut contenant une liste du membre d'un groupe.

L'attribut physique mappé vers %GROUP_MEMBERSHIP% doit posséder plusieurs valeurs.

L'attribut connu %GROUP_MEMBERSHIP% n'est pas requis pour le provisionnement d'annuaires d'utilisateurs.

%GROUP_NAME%

(requis)

Indique l'attribut contenant un nom de groupe.

%ORG_MEMBERSHIP%

(requis)

Indique l'attribut contenant le nom unique de l'organisation à laquelle le groupe appartient.

CA Identity Manager utilise cet attribut connu pour déterminer la structure de l'annuaire (page 86).

Cet attribut n'est pas requis si l'annuaire d'utilisateurs n'inclut pas d'organisations.

%ORG_MEMBERSHIP_NAME%

Indique l'attribut contenant le nom convivial de l'organisation dans laquelle le groupe existe.

Cet attribut n'est pas valide pour les annuaires d'utilisateurs qui n'incluent pas les organisations.

%SELF_SUBSCRIBING%

Indique l'attribut déterminant si les utilisateurs peuvent s'abonner à un groupe (page 86).

%NESTED_GROUP_MEMBERSHIP%

Indique l'attribut contenant une liste de groupes qui sont membres du groupe. Par exemple, si le groupe 1 est un membre du groupe A, le groupe 1 est stocké dans l'attribut %NESTED_GROUP_MEMBERSHIP%.

Si vous ne spécifiez pas d'attribut %NESTED_GROUP_MEMBERSHIP%, CA Identity Manager stocke les groupes imbriqués dans l'attribut %GROUP_MEMBERSHIP%.

Pour inclure des groupes comme membres d'autres groupes, configurez la prise en charge des groupes imbriqués tel que décrit à la section Configuration de groupes dynamiques et imbriqués.

%DYNAMIC_GROUP_MEMBERSHIP%

Indique l'attribut contenant la requête LDAP qui génère un groupe dynamique (page 148).

Remarque : Pour développer les attributs disponibles pour l'objet groupe et inclure les attributs %NESTED_GROUP_MEMBERSHIP% et %DYNAMIC_GROUP_MEMBERSHIP%, vous pouvez utiliser des classes d'objets auxiliaires.

Attributs connus d'organisation

Les attributs connus suivants s'appliquent uniquement aux environnements prenant en charge des organisations :

%ORG_DESCR%

Indique l'attribut contenant la description d'une organisation.

%ORG_MEMBERSHIP%

(requis)

Indique l'attribut contenant le nom unique de l'organisation parente d'une organisation.

%ORG_MEMBERSHIP_NAME%

Indique l'attribut contenant le nom convivial de l'organisation parente d'une organisation.

%ORG_NAME%

(requis)

Indique l'attribut contenant le nom de l'organisation.

Attribut %ADMIN_ROLE_CONSTRAINT%

Lorsque vous créez un rôle d'administration, spécifiez une ou plusieurs règles d'appartenance au rôle. Les utilisateurs conformes aux règles d'appartenance ont le rôle. Par exemple, lorsque la règle d'appartenance au rôle de gestionnaire d'utilisateurs est titre=Gestionnaire d'utilisateurs, les utilisateurs qui ont le titre de gestionnaire d'utilisateurs ont le rôle de gestionnaire d'utilisateurs.

Remarque : Pour plus d'informations sur les règles, reportez-vous au *Manuel d'administration*.

%ADMIN_ROLE_CONSTRAINT% permet de désigner un attribut de profil pour stocker les rôles d'administration d'un administrateur.

Utilisation de l'attribut %ADMIN_ROLE_CONSTRAINT%

Pour utiliser %ADMIN_ROLE_CONSTRAINT% comme contrainte pour tous les rôles d'administration, procédez comme suit :

- Associez l'attribut connu %ADMIN_ROLE_CONSTRAINT% à un attribut de profil à valeurs multiples pour prendre en charge plusieurs rôles.

- Lors de la configuration d'un rôle d'administration dans la console d'utilisateur, vérifiez la contrainte suivante :

  `Rôles d'administration égal à nom_rôle`

  nom_rôle

  Définit le nom du rôle pour lequel vous fournissez la contrainte, comme illustré par l'exemple suivant :

  `Rôles d'administration égal à Gestionnaire d'utilisateurs`

Remarque : Rôles d'administration est le nom d'affichage par défaut pour l'attribut %ADMIN_ROLE_CONSTRAINT%.

Configuration des attributs connus

Pour configurer des attributs connus, suivez la procédure suivante.

Procédez comme suit:

1. Dans le fichier de configuration d'annuaire, recherchez le signe suivant :

   ##
2. Remplacez la valeur commençant par ## par l'attribut LDAP approprié.
3. Répétez les étapes 1 et 2 jusqu'à remplacer toutes les valeurs requises.
4. Mappez des attributs connus facultatifs vers des attributs physiques, selon vos besoins.
5. Enregistrez le fichier de configuration d'annuaire.

Description de la structure d'annuaire d'utilisateurs

CA Identity Manager utilise l'attribut connu %ORG_MEMBERSHIP% pour déterminer la structure d'un annuaire d'utilisateurs.

La procédure de description de la structure d'annuaire d'utilisateurs dépend du type de structure d'annuaire.

Description d'une structure d'annuaire hiérarchique

Le fichier de configuration d'annuaire est déjà configuré pour une structure d'annuaire hiérarchique. En conséquence, il n'est pas nécessaire de modifier la description de l'attribut %ORG_MEMBERSHIP%.

Description d'une structure d'annuaire d'utilisateurs non hiérarchique

Procédez comme suit:

1. Recherchez la description de l'attribut %ORG_MEMBERSHIP% dans la section d'objet utilisateur du fichier directory.xml.
2. Dans le paramètre physicalname, remplacez %ORG_MEMBERSHIP% par le nom de l'attribut contenant l'organisation à laquelle l'utilisateur appartient.

Description d'une structure d'annuaire non hiérarchique

Procédez comme suit:

1. Recherchez la description de l'attribut %ORG_MEMBERSHIP% dans la section d'objet utilisateur du fichier directory.xml.
2. Dans le paramètre physicalname, remplacez %ORG_MEMBERSHIP% par le nom de l'attribut contenant l'organisation à laquelle l'utilisateur appartient.
3. Répétez l'étape 1 dans la section d'objet groupe.
4. Dans le paramètre physicalname, remplacez %ORG_MEMBERSHIP% par le nom de l'attribut contenant l'organisation à laquelle le groupe appartient.

Description d'un annuaire d'utilisateurs qui ne prend pas en charge les organisations

Vérifiez qu'aucune description d'objet ou aucun attribut connu n'est défini pour des organisations dans directory.xml.

Configuration de groupes

Pour la configuration, vous pouvez diviser les groupes comme suit :

- Groupes avec auto-abonnement
- Groupes dynamiques et imbriqués

Configuration de groupes avec auto-abonnement

Vous pouvez permettre aux utilisateurs de l'auto-administration de rejoindre des groupes en configurant la prise en charge des groupes avec auto-abonnement dans le fichier de configuration d'annuaire.

Lorsqu'un utilisateur s'auto-enregistre, CA Identity Manager recherche les groupes dans les organisations spécifiées et affiche ceux avec auto-abonnement à l'utilisateur.

Procédez comme suit:

1. Dans la section des groupes avec auto-abonnement, ajoutez l'élément SelfSubscribingGroups comme suit :

   <SelfSubscribingGroups type=*search_type* org=*org_dn*>

2. Ajoutez des valeurs aux paramètres suivants :

   type

   Indique l'emplacement dans lequel CA Identity Manager recherche les groupes avec auto-abonnement comme suit :

   - NONE : CA Identity Manager ne recherche aucun groupe. Spécifiez NONE pour empêcher les utilisateurs de s'abonner à des groupes.
   - ALL : CA Identity Manager lance une recherche de groupes à la racine. Spécifiez ALL lorsque les utilisateurs peuvent s'abonner à des groupes dans un annuaire hiérarchique.
   - INDICATEDORG : CA Identity Manager recherche les groupes avec auto-abonnement dans l'organisation d'un utilisateur et dans ses sous-organisations. Par exemple, lorsque le profil d'un utilisateur se trouve dans l'organisation Marketing, CA Identity Manager recherche les groupes avec auto-abonnement dans l'organisation Marketing et dans toutes ses sous-organisations.
   - SPECIFICORG : CA Identity Manager effectue les recherches dans une organisation spécifique. Indiquez le nom unique de l'organisation spécifique dans le paramètre org.

   org

   Définit l'identificateur unique de l'organisation dans laquelle CA Identity Manager recherche les groupes avec auto-abonnement.

   Remarque : Veillez à spécifier le paramètre org si type=SPECIFICORG.

Une fois la prise en charge des groupes avec auto-abonnement configurée dans l'annuaire CA Identity Manager, les administrateurs CA Identity Manager peuvent spécifier ces groupes dans la console d'utilisateur.

Remarque : Pour plus d'informations sur la gestion des groupes, consultez le *Manuel d'administration*.

Configuration de groupes dynamiques et imbriqués

Si vous gérez un référentiel d'utilisateurs LDAP, vous pouvez configurer la prise en charge pour les types de groupe suivants dans le fichier de configuration d'annuaire :

Groupes dynamiques

Permet de définir l'appartenance au groupe en spécifiant une requête de filtre LDAP de façon dynamique dans la console d'utilisateur. Avec des groupes dynamiques, les administrateurs n'ont pas besoin de rechercher et d'ajouter des membres de groupe de manière individuelle.

Groupes imbriqués

Permet d'ajouter des groupes comme membres d'autres groupes.

Vous pouvez activer les groupes dynamiques et imbriqués à l'aide du fichier de configuration d'annuaire.

Procédez comme suit:

1. Mappez les attributs connus (page 83) suivants vers un attribut physique pour l'objet géré groupe en fonction de vos besoins :
   - %DYNAMIC_GROUP_MEMBERSHIP%
   - %NESTED_GROUP_MEMBERSHIP%

   Remarque : L'attribut physique sélectionné doit prendre en charge plusieurs valeurs.
2. Dans la section Directory Groups Behavior (Comportement des groupes de l'annuaire), ajoutez l'élément GroupTypes suivant :

   `<GroupTypes type=`*`group`*`>`

   Remarque : La valeur de l'élément GroupTypes doit respecter la casse.
3. Saisissez une valeur pour le paramètre suivant :

   group

   Active la prise en charge des groupes imbriqués et dynamiques. Les valeurs valides sont les suivantes.
   - NONE : CA Identity Manager ne prend pas en charge les groupes imbriqués et dynamiques.
   - ALL : CA Identity Manager prend en charge les groupes dynamiques et imbriqués.
   - DYNAMIC : CA Identity Manager prend en charge les groupes dynamiques uniquement.
   - NESTED : CA Identity Manager prend en charge les groupes imbriqués uniquement.

Une fois la prise en charge pour les groupes dynamiques et imbriqués configurée dans l'annuaire CA Identity Manager, les administrateurs CA Identity Manager peuvent spécifier les groupes dynamiques et imbriqués dans la console d'utilisateur.

Remarque : Tenez compte du fait que vous avez défini le type de groupe sur NESTED ou sur ALL *sans* définir le paramètre connu %NESTED_GROUP_MEMBERSHIP%. Dans ce cas, CA Identity Manager stocke les groupes imbriqués et les utilisateurs dans le paramètre connu %GROUP_MEMBERSHIP%. Le traitement de l'appartenance au groupe peut être légèrement ralenti.

Ajout de la prise en charge des groupes comme administrateurs de groupes

Si vous gérez un référentiel d'utilisateurs LDAP, vous pouvez permettre à des groupes d'agir en tant qu'administrateurs d'autres groupes. Lorsque vous affectez un groupe comme administrateur, seuls les administrateurs de ce groupe sont des administrateurs du groupe spécifié. Les membres du groupe d'administrateurs spécifié n'ont pas de droits de gestion du groupe.

Procédez comme suit:

1. Mappez l'attribut connu %GROUP_ADMIN_GROUP% vers un attribut physique qui stocke la liste des groupes agissant comme administrateurs.

   Remarque : L'attribut physique sélectionné doit prendre en charge plusieurs valeurs.

   Les attributs connus de groupe (page 83) fournissent davantage d'informations sur l'attribut %GROUP_ADMIN_GROUP%.

   Remarque : Si vous avez défini le type de groupe d'administrateurs sur TOUT sans définir l'attribut connu %GROUP_ADMIN_GROUP% CA Identity Manager stocke les groupes d'administrateurs dans l'attribut %GROUP_ADMIN%.

2. Dans la section AdminGroups Behavior (Comportement des groupes d'administrateurs) de l'annuaire, configurez l'élément AdminGroupTypes comme suit :

   <AdminGroupTypes type="ALL">

   La valeur par défaut d'AdminGroupTypes est NONE.

   Remarque : La valeur de l'élément AdminGroupTypes doit respecter la casse.

Une fois la prise en charge des groupes agissant en tant qu'administrateurs configurée dans l'annuaire CA Identity Manager, les administrateurs CA Identity Manager peuvent spécifier des groupes en tant qu'administrateurs d'autres groupes dans la console d'utilisateur.

Règles de validation

Une règle de validation applique des conditions aux données qu'un utilisateur saisit dans un champ de fenêtre de tâche. Les conditions peuvent appliquer un type ou format de données. Veillez donc à ce que les données soient valides dans le contexte d'autres données dans la fenêtre de tâche.

Les règles de validation sont associées à des attributs de profil. Avant de traiter une tâche, CA Identity Manager vérifie que les données saisies pour un attribut de profil respectent les règles de validation associées.

Vous pouvez définir des règles de validation et les associer à des attributs de profil dans le fichier de configuration d'annuaire.

Propriétés d'annuaire CA Identity Manager supplémentaires

Vous pouvez configurer les propriétés supplémentaires suivantes :

- Triez l'ordre des résultats de la recherche.
- Effectuez une recherche dans les classes d'objets pour vérifier qu'un nouvel utilisateur n'existe pas déjà.
- Patientez afin d'éviter que CA Identity Manager expire avant l'issue de la réplication des données, à partir de l'annuaire LDAP principal vers l'annuaire LDAP secondaire.

Configuration de l'ordre de tri

Vous pouvez spécifier un attribut de tri pour chaque objet géré, tel que des utilisateurs, des groupes, ou des organisations. CA Identity Manager utilise cet attribut pour trier des résultats de la recherche dans la logique métier personnalisée, que vous créez à l'aide des API CA Identity Manager.

Remarque : L'attribut de tri n'affecte pas l'affichage des résultats de la recherche dans la console d'utilisateur.

Par exemple, lorsque vous spécifiez l'attribut cn pour l'objet utilisateur, CA Identity Manager trie les résultats d'une recherche d'utilisateurs par ordre alphabétique en fonction de l'attribut cn.

Procédez comme suit:

1. Après le dernier élément IMSManagedObjectAttr dans la section de l'objet géré auquel l'ordre de tri s'applique, ajoutez les instructions suivantes :

```
<PropertyDict name="SORT_ORDER">
    <Property name="ATTR">your_sort_attribute
    </Property>
</PropertyDict>
```

2. Remplacez *your_sort_attribute* par l'attribut sur lequel CA Identity Manager triera les résultats de la recherche.

Remarque : Spécifiez uniquement un attribut physique. Ne spécifiez pas d'attribut connu.

Par exemple, supposons que vous devez trier des résultats de recherche d'utilisateur en fonction de la valeur de l'attribut cn. Après le dernier élément IMSManagedObjectAttr dans la section d'objet utilisateur du fichier de configuration d'annuaire, ajoutez les éléments suivants :

```
<!-- ******************** User Object ******************** -->
   <ImsManagedObject name="User" description="My Users"
      objectclass="top,person,organizationalperson,user"
      objecttype="USER">
   .
   .
   .
        <ImsManagedObjectAttr physicalname="departmentnumber"
                displayname="Department" description="Department"
                valuetype="String" required="true"
                multivalued="false" maxlength="0" />
        <PropertyDict name="SORT_ORDER">
                <Property name="ATTR">cn</Property>
        </PropertyDict>
  </ImsManagedObject>
```

Recherche dans les Objectclasses

Lorsque vous créez un utilisateur, CA Identity Manager effectue une recherche dans le référentiel d'utilisateurs pour vérifier si l'utilisateur existe ou non. Cette recherche est limitée aux utilisateurs dont les objectclasses sont spécifiées dans la définition d'objet utilisateur dans le fichier de configuration d'annuaire (directory.xml). Si aucun utilisateur existant n'est détecté dans ces objectclasses, CA Identity Manager tente de créer l'utilisateur.

Si un utilisateur avec le même identificateur unique (ID d'utilisateur) existe, mais qu'il possède un objectclass différent, la création de l'utilisateur par le serveur LDAP échoue. L'erreur est signalée dans le serveur LDAP, mais CA Identity Manager ne reconnaît pas l'erreur. CA Identity Manager semble créer l'utilisateur correctement.

Pour éviter ce problème, vous pouvez configurer une propriété SEARCH_ACROSS_CLASSES qui entraîne CA Identity Manager à rechercher des utilisateurs dans toutes les définitions d'objectclass lors de la recherche d'utilisateurs existants.

Remarque : Cette propriété affecte uniquement les recherches d'utilisateurs dupliqués lors de l'exécution de tâches telles que la création d'un utilisateur. Pour toutes les autres recherches, les contraintes d'objectclass s'appliquent.

Procédez comme suit:

1. Dans le fichier de configuration d'annuaire (directory.xml), recherchez l'élément ImsManagedObject qui décrit l'objet d'utilisateur.
2. Ajoutez l'élément PropertyDict suivant :

```
<PropertyDict name="SEARCH_ACROSS_CLASSES" description="allowing checking an
attribute across classes ">
<Property name="ENABLE">true</Property>
</PropertyDict>
```

Remarque : L'élément PropertyDict doit être le dernier dans ImsManagedObject, comme dans l'exemple suivant :

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson,customClass"
objecttype="USER">
<ImsManagedObjectAttr physicalname="departmentnumber"
displayname="Department" description="Department" valuetype="String"
required="true" multivalued="false" maxlength="0" />
.
.
.
<PropertyDict name="SEARCH_ACROSS_CLASSES" description="allow checking an
attribute across classes ">
<Property name="ENABLE">true</Property>
</PropertyDict>
```

Temps d'attente de la réplication

Dans un déploiement qui inclut la réplication entre les annuaires LDAP principal et secondaire, vous pouvez configurer le serveur de stratégies SiteMinder de sorte à ce qu'il communique avec un annuaire secondaire. Dans cette configuration, le serveur de stratégies détecte automatiquement les références qui pointent vers l'annuaire principal lors d'opérations d'écriture de données dans l'annuaire LDAP. Les données sont stockées dans l'annuaire LDAP principal et répliqué vers l'annuaire LDAP secondaire en fonction du schéma de réplication de vos ressources réseau.

Dans cette configuration, lors de la création d'un objet dans CA Identity Manager, l'objet est créé dans l'annuaire principal et également répliqué dans l'annuaire secondaire. Un retard peut se produire pendant le processus de réplication, ce qui entraîne l'échec de l'action dans CA Identity Manager.

Pour éviter ce problème, vous pouvez spécifier la durée de l'attente (en secondes) par CA Identity Manager avant d'expirer dans la propriété REPLICATION_WAIT_TIME.

Procédez comme suit:

1. Dans le fichier de configuration d'annuaire (directory.xml), recherchez l'élément ImsManagedObject qui décrit l'objet d'utilisateur.
2. Ajoutez l'élément PropertyDict suivant :

   ```
   <PropertyDict name="REPLICATION_WAIT_TIME" description="time delay in seconds
   for LDAP provider to allow replication to propagate from master to slave">
   <Property name=REPLICATION_WAIT_TIME><time in seconds></Property>
   </PropertyDict>
   ```

   Remarque : L'élément PropertyDict doit être le dernier dans ImsManagedObject, comme dans l'exemple suivant :

   ```
   <ImsManagedObject name="User" description="My Users"
   objectclass="top,person,organizationalperson,inetorgperson,customClass"
   objecttype="USER">
   <ImsManagedObjectAttr physicalname="departmentnumber"
   displayname="Department" description="Department" valuetype="String"
   required="true" multivalued="false" maxlength="0" />
   .
   .
   .
   <PropertyDict name="REPLICATION_WAIT_TIME" description="time delay in seconds
   for LDAP provider to allow replication to propagate from master to slave">
   <Property name=REPLICATION_WAIT_TIME>800</Property>
   </PropertyDict>
   ```

Lorsque le temps d'attente de réplication n'est pas défini, la valeur par défaut 0 est utilisée.

Paramètres de connexion LDAP

Pour améliorer les performances, vous pouvez spécifier les paramètres suivants dans le fichier de configuration d'annuaire (directory.xml) :

Expiration du délai de connexion

Spécifie la durée maximum en millisecondes de la recherche d'un annuaire effectuée par CA Identity Manager avant de prendre fin.

Cette propriété est spécifiée dans le fichier de configuration d'annuaire comme suit :

com.sun.jndi.ldap.connect.timeout

Connection Pool Max Size (Taille maximum du pool de connexions)

Spécifie le nombre maximum de connexions entre CA Identity Manager et l'annuaire LDAP.

Cette propriété est spécifiée dans le fichier de configuration d'annuaire comme suit :

com.sun.jndi.ldap.connect.pool.maxsize

Connection Pool Default Size (Taille par défaut du pool de connexions)

Spécifie le nombre de connexions par défaut entre CA Identity Manager et l'annuaire LDAP.

Cette propriété est spécifiée dans le fichier de configuration d'annuaire comme suit :

com.sun.jndi.ldap.connect.pool.prefsize

Procédez comme suit:

1. Dans le fichier de configuration d'annuaire (directory.xml), recherchez l'élément ImsManagedObject qui décrit l'objet d'utilisateur.
2. Ajoutez l'élément PropertyDict suivant :

```
<PropertyDict name="LDAP_CONNECTION_SETTINGS" description="LDAP Connection
Settings">
    <Property name="com.sun.jndi.ldap.connect.timeout">5000</Property>
    <Property name="com.sun.jndi.ldap.connect.pool.maxsize">200</Property>
    <Property name="com.sun.jndi.ldap.connect.pool.prefsize">10</Property>
</PropertyDict>
```

3. Enregistrez le fichier directory.xml.

   Lors de la création de l'annuaire CA Identity Manager à l'aide de ce fichier, CA Identity Manager configure ces paramètres.

Amélioration des performances de recherche dans les annuaires

Pour améliorer les performances de recherches d'utilisateurs, d'organisations et de groupes dans les annuaires, effectuez les tâches suivantes :

- Indexez les attributs que les administrateurs peuvent spécifier dans des requêtes de recherche.

  Remarque : Dans le cas d'un annuaire Oracle Internet, une recherche peut échouer lorsqu'un attribut dans une requête de recherche n'est pas indexé.

- Configurez les paramètres de taille de page et de ligne maximum (page 97) pour la gestion CA Identity Manager de recherches étendues.
- Ajustez l'annuaire d'utilisateurs. Consultez la documentation de l'annuaire d'utilisateurs que vous utilisez.

Amélioration des performances des recherches étendues

Lorsque CA Identity Manager gère un référentiel d'utilisateurs volumineux, les recherches qui renvoient un grand nombre de résultats peuvent monopoliser toutes les ressources mémoire du système. Pour éviter les problèmes de mémoire, vous pouvez définir des limites pour des recherches étendues.

Les deux paramètres suivants déterminent la méthode de gestion des recherches étendues par CA Identity Manager :

- Nombre maximum de lignes

  Spécifie le nombre maximum de résultats que CA Identity Manager peut renvoyer lors de la recherche d'un annuaire d'utilisateurs. Lorsque le nombre de résultats dépasse la limite, une erreur s'affiche.

- Taille de la page

  Spécifie le nombre d'objets renvoyés pour une recherche unique. Si le nombre d'objets dépasse la taille de la page, CA Identity Manager effectue plusieurs recherches.

  Lors de la spécification de la taille de la page, tenez compte des points suivants :

  - Pour utiliser l'option Search Page Size (Taille de la page de recherche), le référentiel d'utilisateurs géré par CA Identity Manager doit prendre en charge la pagination. Certains types de référentiel d'utilisateurs requièrent une configuration supplémentaire pour prendre en charge la pagination. Pour plus d'informations, consultez les sections suivantes :

    Configuration de la prise en charge de la pagination de serveur d'annuaires Sun Java System (page 99)

    Configuration de la prise en charge de la pagination Active Directory

  - Si le référentiel d'utilisateurs ne prend pas en charge la pagination et qu'une valeur pour maxrows est spécifiée, seule la valeur de maxrows sera utilisée par CA Identity Manager pour contrôler la taille de la recherche.

Vous pouvez configurer le nombre maximum de lignes et la taille de la page dans les emplacements suivants :

- Référentiel d'utilisateurs

  Dans la plupart des référentiels d'utilisateurs et des bases de données, vous pouvez configurer des limites de recherche.

  Remarque : Pour plus d'informations, consultez la documentation du référentiel d'utilisateurs ou de la base de données que vous utilisez.

- Annuaire CA Identity Manager

  Vous pouvez configurer l'élément DirectorySearch (page 59) dans le fichier de configuration d'annuaire (directory.xml) que vous utilisez pour créer l'annuaire CA Identity Manager.

  Par défaut, la valeur maximale pour le nombre de lignes et la taille des pages est illimitée pour les répertoires existants. Pour les nouveaux répertoires, la valeur du nombre maximum de lignes est illimitée et la valeur maximale pour la taille de page est 2000.

- Définition d'un objet géré

  Pour définir les limites de ligne et les tailles de page maximales qui s'appliquent à un seul type d'objet et non à un annuaire complet, configurez (page 61) la *définition d'objet géré* dans le fichier directory.xml que vous utilisez pour créer l'annuaire CA Identity Manager.

  La définition de limites pour un type d'objet géré permet de procéder à des ajustements en fonction des besoins métier. Par exemple, la plupart des sociétés ont plus d'utilisateurs que de groupes. Ces sociétés peuvent définir des limites pour des recherches d'objet Utilisateur uniquement.

- Fenêtres de recherche de tâche

  Vous pouvez contrôler le nombre de résultats de recherche que les utilisateurs affichent dans les fenêtres de recherche et de liste dans la console d'utilisateur. Si le nombre de résultats dépasse le nombre de résultats par page défini pour la tâche, des liens vers les pages de résultats supplémentaires sont affichés.

  Cette configuration n'affecte pas le nombre de résultats renvoyés pour une recherche.

  Remarque : Pour plus d'informations sur la définition de la taille de page dans les fenêtres de recherche et de liste, consultez le *Manuel d'administration*.

Si les limites de nombre de lignes et les tailles de page maximales sont définies dans plusieurs endroits, le paramètre le plus spécifique s'applique. Par exemple, les paramètres d'objet géré ont priorité sur les paramètres de niveau annuaire.

Configuration de la prise en charge de la pagination de serveur d'annuaires Sun Java System

Les serveurs d'annuaires Sun Java System prennent en charge l'affichage de la liste virtuelle (VLV), une méthode de remise des résultats de recherche dans un certain ordre ou dans certains sous-ensembles. Cette méthode diffère des résultats paginés simples (Simple Paged Results), attendus par CA Identity Manager.

Pour utiliser la méthode VLV, définissez des autorisations et créez des index. CA Identity Manager inclut les fichiers suivants que vous devez configurer pour la prise en charge de la pagination :

- vlvcntrl.ldif
- vlvindex.ldif
- runvlvindex.cmd, runvlvindex.sh

Ces fichiers sont inclus dans l'exemple NeteAuto,sous samples\NeteAuto dans les outils d'administration.

Les outils d'administration sont situés aux emplacements par défaut suivants :

Windows : <chemin_installation>

UNIX : <chemin_installation2>

Procédez comme suit:

1. Dans le fichier directory.xml pour l'annuaire CA Identity Manager, ajoutez le paramètre suivant à l'élément DirectorySearch (page 59)comme suit :

   ```
   minsortrules="1"
   ```

   Remarque : Si vous modifiez un annuaire CA Identity Manager existant, consultez la section Mise à jour d'un annuaire CA Ide (page 186)ntity Manager.

2. Définissez des autorisations pour le fichier vlvcntrl.ldif comme suit :
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvcntrl.ldif
   ```

3. Importez les définitions de recherche VLV et d'index comme suit :
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvindex.ldif
   ```

4. Arrêtez l'annuaire comme suit :
   ```
   stop-slapd
   ```

5. Créez les index à l'aide de runvlvindex.

6. Démarrez l'annuaire comme suit :
   ```
   start-slapd
   ```

Configuration de la prise en charge de la pagination Active Directory

Pour configurer la prise en charge de la pagination dans Active Directory, suivez la procédure de haut niveau suivante :

- Configurez la prise en charge de l'affichage de la liste virtuelle (VLV) (page 100).
- Configurez la taille maximale de la page de recherche pour Active Directory (page 101). (**Pour les annuaires créés avant CA Identity Manager r12.5 SP7 uniquement**)

Configuration de la prise en charge de l'affichage de la liste virtuelle (VLV)

Active Directory prend en charge l'affichage de la liste virtuelle (VLV), une méthode de remise des résultats de recherche dans un certain ordre ou dans certains sous-ensembles. Cette méthode diffère des résultats paginés simples (Simple Paged Results), attendus par CA Identity Manager.

Pour utiliser la méthode VLV, définissez des autorisations et créez des index. CA Identity Manager inclut les fichiers suivants que vous devez configurer pour la prise en charge de la pagination :

- vlvcntrl.ldif
- vlvindex.ldif
- runvlvindex.cmd, runvlvindex.sh

Ces fichiers sont inclus dans l'exemple NeteAuto,sous samples\NeteAuto dans les outils d'administration.

Les outils d'administration sont situés aux emplacements par défaut suivants :

Windows : <chemin_installation>

UNIX : <chemin_installation2>

Procédez comme suit:

1. Dans le fichier directory.xml pour l'annuaire CA Identity Manager, ajoutez le paramètre suivant à l'élément DirectorySearch (page 59) comme suit :

   ```
   minsortrules="1"
   ```

   Remarque : Si vous modifiez un annuaire CA Identity Manager existant, consultez la section Mise à jour d'un annuaire CA Ide (page 186)ntity Manager.

2. Définissez des autorisations pour le fichier vlvcntrl.ldif comme suit :
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvcntrl.ldif
   ```

3. Importez les définitions de recherche VLV et d'index comme suit :
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvindex.ldif
   ```

4. Arrêtez l'annuaire comme suit :
   ```
   stop-slapd
   ```

5. Créez les index à l'aide de runvlvindex.

6. Démarrez l'annuaire comme suit :
   ```
   start-slapd
   ```

Configuration de la taille maximale de la page de recherche pour Active Directory

Active Directory utilise 1 000 comme taille maximale de la page de recherche par défaut. Supposons que la valeur d'attribut de la taille maximale de la page de recherche en directory.xml est supérieure ou égale à 1 000. Dans ce cas, CA Identity Manager ne peut afficher d'avertissement lorsque le nombre de résultats de la recherche dépasse la valeur de maxrows dans directory.xml. Dans ce cas, les administrateurs qui effectuent la recherche ignorent que certains résultats de la recherche sont omis.

Pour éviter ce problème, vérifiez que la valeur de l'attribut maxpagesize pour l'annuaire et chaque objet géré est inférieure à la taille maximale de la page de recherche Active Directory.

Supposons que vous créez un annuaire CA Identity Manager à l'aide du fichier de modèle directory.xml fourni avec CA Identity Manager 12.5 SP7 ou version ultérieure. Dans ce cas, vous n'avez pas besoin d'effectuer d'étape supplémentaire pour la prise en charge de la pagination. L'attribut maxpagesize dans directory.xml est défini par défaut.

Si vous ajoutez la prise en charge de la pagination à un annuaire CA Identity Manager existant, l'attribut maxpagesize dans directory.xml doit être inférieur à 1 000.

De même, si MaxPageSize dans Active Directory est de 1 000, veillez à définir l'attribut maxpagesize de manière appropriée dans l'annuaire CA Identity Manager et tous les objets gérés.

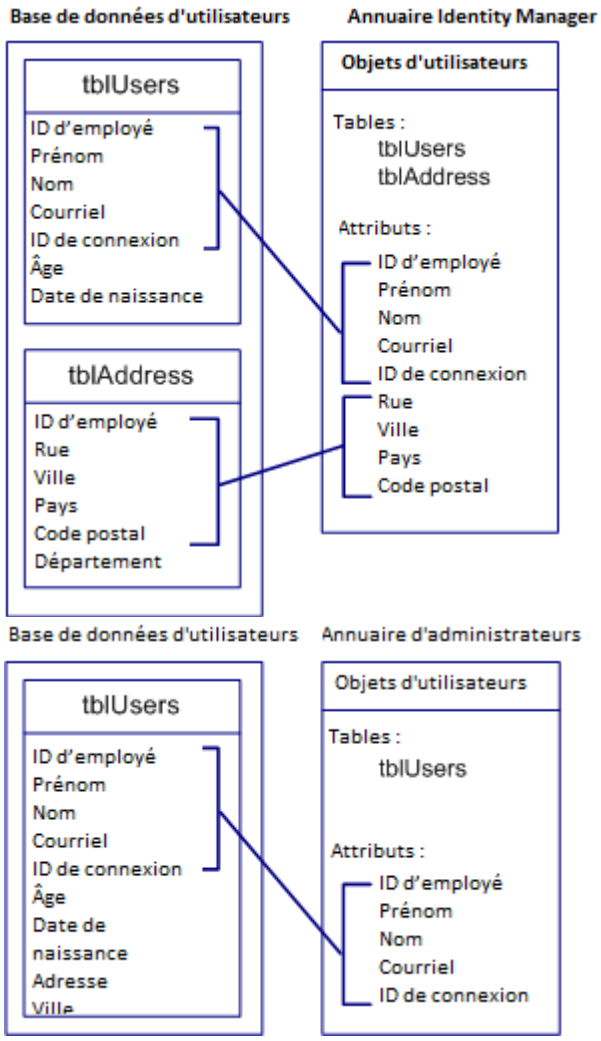
Chapitre 4: Gestion des bases de données relationnelles

Ce chapitre traite des sujets suivants :

Annuaires CA Identity Manager

Un *annuaire CA Identity Manager* décrit le stockage d'objets tels que des utilisateurs, des groupes et des organisations (facultatives) dans le référentiel d'utilisateurs et leur représentation dans CA Identity Manager. Un annuaire CA Identity Manager est associé à un ou plusieurs environnements CA Identity Manager.

Le schéma suivant illustre l'association entre un annuaire CA Identity Manager et un référentiel d'utilisateurs :



Remarque : Certains attributs utilisateur de la base de données ne font pas partie de l'annuaire CA Identity Manager. Par conséquent, CA Identity Manager ne les gère pas.

Remarques importantes concernant la configuration de CA Identity Manager pour l'utilisation de bases de données relationnelles

Avant de configurer CA Identity Manager pour la gestion d'une base de données relationnelles, veillez à ce qu'elle présente la configuration requise suivante :

- Lorsque CA Identity Manager comprend SiteMinder, la base de données doit être accessible via un pilote JDBC ou ODBC (Open Database Connectivity). Le pilote doit prendre en charge les jointures externes. Si plus de deux tables sont utilisées pour représenter un objet géré, le pilote doit également prendre en charge les jointures externes imbriquées.

  Remarque : Si le pilote ne prend pas en charge les jointures externes, CA Identity Manager utilisera des jointures intérieures lors de l'interrogation de la base de données. Cela peut entraîner des résultats de requête inattendus.

- Identifiez de manière unique chaque objet géré par CA Identity Manager, tel qu'un utilisateur, un groupe, ou une organisation (en cas de prise en charge). Par exemple, pour des utilisateurs, l'identificateur unique peut être un ID de connexion.

  Remarque : Veillez à ce que l'identificateur unique soit stocké dans une seule colonne.

- CA Identity Manager requiert des attributs à valeurs multiples, que vous pouvez stocker sous forme de liste délimitée dans une seule cellule ou dans plusieurs lignes d'une autre table. Par exemple, la table tblGroupMembers suivante stocke les membres d'un groupe :

ID	Membres
Recherche	dmason
Recherche	rsavory
Marketing	dmason
Marketing	awelch

La colonne ID contient l'identificateur unique d'un groupe et la colonne Membres contient l'identificateur unique d'un membre du groupe. Par exemple, dmason et rsavory sont membres du groupe Recherche. Lorsqu'un nouveau membre est ajouté à ce groupe, une autre ligne est ajoutée à tblGroupMembers.

- Si votre environnement inclut des organisations, procédez comme suit :
  - Pour configurer la prise en charge d'organisations (page 150), modifiez et exécutez un script SQL, fourni avec CA Identity Manager, sur la base de données.
  - CA Identity Manager requiert une organisation de niveau supérieure, appelée racine. Toutes les autres organisations sont associées à l'organisation racine.

    Pour plus d'informations sur la configuration requise des organisation, consultez la section Gestion des organisations (page 149).

Création d'une source de données Oracle pour WebSphere

Procédez comme suit:

1. Dans la console d'administration WebSphere, accédez au fournisseur JDBC créé lors de la configuration du pilote JDBC.
2. Créez une source de données avec les propriétés suivantes et cliquez sur Appliquer :

   Nom : Source de données de référentiel d'utilisateurs

   Nom JNDI : userstore

   URL : jdbc:oracle:thin:@*db_systemname*:1521:*oracle_sid*
3. Configurez une nouvelle entrée de données d'authentification J2C pour la source de données du référentiel d'utilisateurs :
   a. Entrez les propriétés suivantes :

      Alias : Référentiel d'utilisateurs

      ID d'utilisateur : *nom d'utilisateur*

      Mot de passe : *mot de passe*

      nom d'utilisateur et *mot de passe* étant le nom d'utilisateur et le mot de passe du compte spécifié lors de création de la base de données.

   b. Cliquez sur OK, puis utilisez les liens de navigation dans la partie supérieure de la fenêtre pour revenir à la source de données que vous créez.

4. Sélectionnez l'entrée de données d'authentification J2C de référentiel d'utilisateurs que vous avez créée dans la zone de liste des champs suivants :
   - Component-managed Authentication Alias (Alias d'authentification géré par composant)
   - Container-managed Authentication Alias (Alias d'authentification géré par conteneur)
5. Pour enregistrer la configuration, cliquez sur OK.

   Remarque : Pour vérifier que la source de données est configurée correctement, cliquez sur Tester la connexion dans la fenêtre de configuration de la source de données. Si la connexion de test échoue, redémarrez WebSphere et testez la connexion à nouveau.

Création d'un annuaire CA Identity Manager

Procédez comme suit:

1. Si vous utilisez SiteMinder, appliquez le schéma de référentiel de stratégies avant de créer un annuaire CA Identity Manager.

   Remarque : Pour plus d'informations sur les schémas de référentiel de stratégies spécifiques et leur application, consultez le *Manuel d'installation*.
2. Si vous utilisez SiteMinder, créez une source de données ODBC pour l'utiliser avec CA SiteMinder (page 114).
3. Créez une source de données pour la base de données d'utilisateurs gérée par CA Identity Manager.
4. Décrivez la base de données dans CA Identity Manager en modifiant un fichier de configuration d'annuaire (directory.xml). Pour plus d'informations, consultez la section Description d'une base de données dans un fichier de configuration d'annuaire.
5. Dans la console de gestion, importez le fichier de configuration d'annuaire et créez l'annuaire.

Création d'une source de données JDBC

Pour se connecter au référentiel d'utilisateurs, CA Identity Manager requiert une source de données JDBC dans le serveur d'applications sur lequel CA Identity Manager est installé. Les instructions de création de source de données sont différentes pour chaque serveur d'applications.

Création d'une source de données JDBC pour des serveurs d'applications JBoss

Procédez comme suit:

1. Créez une copie du fichier suivant :

   jboss_home\server\default\deploy\objectstore-ds.xml

   jboss home

   Emplacement d'installation du serveur d'applications Jboss sur lequel CA Identity Manager est installé

   Le nouveau fichier doit exister au même emplacement.

2. Remplacez le nom du fichier par userstore-ds.xml.

3. Modifiez userstore-ds.xml comme suit :

   a. Recherchez l'élément <jndi-name>.

   b. Modifiez la valeur jdbc/objectstore de l'élément <jndi-name> par userstore comme suit :

   <jndi-name>userstore</jndi-name>

   c. Dans l'élément <connection-url>, modifiez le paramètre DatabaseName dans le nom de la base de données qui sert de référentiel d'utilisateurs comme suit :

   <connection-url>

   jdbc:sqlserver://*adresse_ip:port*;selectMethod=cursor;DatabaseName=*nom_référentiel_utilisateurs*

   </connection-url>

   adresse ip

   Spécifie l'adresse IP de l'ordinateur sur lequel le référentiel d'utilisateurs est installé.

   port

   Spécifie le numéro de port pour la base de données.

   nom_référentiel_utilisateurs

   Spécifie le nom de la base de données qui sert de référentiel d'utilisateurs.

4. Si vous prévoyez de créer un domaine de sécurité JBoss, requis pour la prise en charge de FIPS, effectuez les étapes suivantes :
   a. Modifiez le domaine de sécurité par <security-domain>imuserstoredb</security-domain>.
   b. Enregistrez le fichier.
   c. Ignorez les étapes restantes. Effectuez plutôt les étapes décrites à la section Création d'un domaine de sécurité JBoss pour la source de données JDBC (page 110).
5. Apportez les modifications supplémentaires suivantes à userstore-ds.xml :
   a. Modifiez la valeur de l'élément <user-name> par le nom d'utilisateur d'un compte disposant de l'accès en lecture et en écriture pour le référentiel d'utilisateurs.
   b. Modifiez la valeur de l'élément <password> par le mot de passe du compte spécifié dans l'élément <user-name>.

   Remarque : Le nom d'utilisateur et le mot de passe s'affichent en texte clair dans ce fichier. Par conséquent, vous pouvez créer un domaine de sécurité de JBoss au lieu de modifier userstore-ds.xml.
6. Enregistrez le fichier.

Utilisation d'un domaine de sécurité JBoss pour la source de données JDBC

Assurez-vous de créer une source de données JDBC dans un serveur d'applications JBoss. Vous pouvez configurer la source de données pour utiliser un nom d'utilisateur et mot de passe, ou pour utiliser un domaine de sécurité.

Important : Veillez à ce que l'option du domaine de sécurité JBoss soit utilisée si la norme FIPS est utilisée.

Procédez comme suit:

1. Effectuez les étapes décrites à la section Création d'une source de données JDBC pour des serveurs d'applications JBoss (page 108).

   Ne spécifiez pas de nom d'utilisateur ni mot de passe dans le fichier userstore-ds.xml, comme décrit à l'étape 4.

2. Ouvrez login-cfg.xml dans *jboss_home*\server\default\conf.

3. Recherchez l'entrée suivante dans le fichier :

```
<application-policy name="imobjectstoredb">
  <authentication>
    <login-module
code="com.netegrity.jboss.datasource.PasswordEncryptedLogin" flag="required">
      <module-option name="userName">fwadmin</module-option>
      <module-option name="password">{PBES}:gSex2/BhDGzEKWvFmzca4w==</module-
option>
      <module-option
name="managedConnectionFactoryName">jboss.jca:name=jdbc/objectstore,service=N
oTxCM</module-option>
    </login-module>
  </authentication>
</application-policy>
```

4. Copiez l'entrée complète et collez-la dans les balises <policy> et </policy> du fichier login-cfg.xml.

5. Dans l'entrée que vous avez collée dans le fichier, appliquez les modifications suivantes :

   a. Modifiez la valeur de l'attribut nom imobjectstoredb par imuserstoredb comme suit :

      ```
      <application-policy name="imuserstoredb">
      ```

   b. Spécifiez le nom de l'utilisateur utilisé pour l'authentification dans le référentiel d'utilisateurs comme suit :

      ```
      <module-option
      name="userName">utilisateur_référentiel_utilisateurs</module-option>
      ```

   c. Spécifiez le mot de passe de l'utilisateur dans l'étape précédente comme suit :

```
<module-option
name="password">mot_passe_utilisateur_référentiel_utilisateurs</module-
option>
```

Remarque : Pour chiffrer le mot de passe du référentiel d'utilisateurs, utilisez l'outil de modification de mots de passe (pwdtools) fourni avec CA Identity Manager.

d. Dans l'élément <module-option name="managedConnectionFactoryName">, indiquez jdbc.jca:name correct comme suit :

```
<module-option name="managedConnectionFactoryName">
   jboss.jca:name=userstore,service=NoTxCM
</module-option>
```

6. Enregistrez le fichier.
7. Redémarrez le serveur d'applications.

Création d'une source de données JDBC pour WebLogic

Créez une source de données dans la console d'administration WebLogic.

Remarque : Pour des informations complètes sur les pools de connexions WebLogic, consultez la documentation d'Oracle WebLogic 11.

Procédez comme suit:

1. Dans la console d'administration WebLogic, créez une source de données JDBC avec les paramètres suivants :

   Nom : Source de données de référentiel d'utilisateurs

   Nom JNDI : userstore

2. Créez le pool de connexions pour la source de données avec les informations suivantes :

- Pour les bases de données SQL Server 2005, utilisez les valeurs suivantes :

  URL : jdbc:sqlserver://*Nomsystème_BdD*:1433

  Nom de la classe de pilote : com.microsoft.sqlserver.jdbc.SQLServerDriver

  Propriétés : user=*nom d'utilisateur*

  databaseName=*nom référentiel d'utilisateurs*

  selectMethod=cursor

  Mot de passe : *mot de passe*

- Pour les bases de données Oracle, utilisez les valeurs suivantes :

  URL : jdbc:oracle:thin:@*nomsystème_BdD_tp*:1521:*oracle_SID*

  Nom de la classe de pilote : oracle.jdbc.driver.OracleDriver

  Propriétés : user=*nom d'utilisateur*

  Mot de passe : *mot de passe*

3. A l'issue de la configuration, définissez la cible du pool dans l'instance du serveur *nom_serveur_wl*.

   A l'issue du déploiement du pool, consultez la console afin de vérifier si des erreurs se sont produites.

   Remarque : Une erreur indiquant que vous ne pouvez pas créer la source de données avec un pool non existant peut apparaître. Pour résoudre cette erreur, redémarrez WebLogic.

Sources de données WebSphere

Les sections suivantes décrivent la création d'une source de données SQL ou Oracle pour des serveurs d'applications WebSphere.

Création d'une source de données SQL Server pour WebSphere

Procédez comme suit:

1. Dans la console d'administration WebSphere, accédez au fournisseur JDBC créé lors de la configuration du pilote JDBC.
2. Dans la section Additional Properties (Propriétés supplémentaires), sélectionnez Sources de données.
3. Créez une source de données avec les propriétés suivantes et cliquez sur Appliquer :

   Nom : Source de données de référentiel d'utilisateurs

   Nom JNDI : userstore

   databaseName : *nom_référentiel_utilisateurs*

   serverName : *nomsystème_BdD*

4. Configurez la propriété selectMethod comme suit :
   a. Dans la section Additional Properties (Propriétés supplémentaires), sélectionnez Custom Properties Propriétés personnalisées).
   b. Cliquez sur la propriété personnalisée selectMethod.
   c. Dans le champ Valeur, saisissez le texte suivant :

      cursor

   d. Cliquez sur OK, puis utilisez les liens de navigation dans la partie supérieure de la fenêtre pour revenir à la source de données que vous créez.
5. Configurez une nouvelle entrée de données d'authentification J2C pour la source de données du référentiel d'utilisateurs :
   a. Dans la section Related Items (Eléments associés), sélectionnez les entrées de données d'authentification J2EE Connector Architecture (J2C).
   b. Cliquez sur Créer.
   c. Entrez les propriétés suivantes :

      Alias : Référentiel d'utilisateurs

      ID d'utilisateur : *nom d'utilisateur*

      Mot de passe : *mot de passe*

      nom d'utilisateur et *mot de passe* étant le nom d'utilisateur et le mot de passe du compte spécifié lors de création de la base de données.

   d. Cliquez sur OK, puis utilisez les liens de navigation dans la partie supérieure de la fenêtre pour revenir à la source de données que vous créez.
6. Dans la zone de liste du champ Component-managed Authentication Alias (Alias d'authentification géré par composant), sélectionnez la saisie de données d'authentification J2C de référentiel d'utilisateurs que vous avez créée.
7. Pour enregistrer la configuration, cliquez sur OK.

   Remarque : Pour vérifier que la source de données est configurée correctement, cliquez sur Tester la connexion dans la fenêtre de configuration de la source de données. Si la connexion de test échoue, redémarrez WebSphere et testez la connexion à nouveau.

Création d'une source de données Oracle pour WebSphere

Procédez comme suit:

1. Dans la console d'administration WebSphere, accédez au fournisseur JDBC créé lors de la configuration du pilote JDBC.

2. Créez une source de données avec les propriétés suivantes et cliquez sur Appliquer :

   Nom : Source de données de référentiel d'utilisateurs

   Nom JNDI : userstore

   URL : jdbc:oracle:thin:@*db_systemname*:1521:*oracle_sid*

3. Configurez une nouvelle entrée de données d'authentification J2C pour la source de données du référentiel d'utilisateurs :

   a. Entrez les propriétés suivantes :

      Alias : Référentiel d'utilisateurs

      ID d'utilisateur : *nom d'utilisateur*

      Mot de passe : *mot de passe*

      nom d'utilisateur et *mot de passe* étant le nom d'utilisateur et le mot de passe du compte spécifié lors de création de la base de données.

   b. Cliquez sur OK, puis utilisez les liens de navigation dans la partie supérieure de la fenêtre pour revenir à la source de données que vous créez.

4. Sélectionnez l'entrée de données d'authentification J2C de référentiel d'utilisateurs que vous avez créée dans la zone de liste des champs suivants :

   - Component-managed Authentication Alias (Alias d'authentification géré par composant)
   - Container-managed Authentication Alias (Alias d'authentification géré par conteneur)

5. Pour enregistrer la configuration, cliquez sur OK.

   Remarque : Pour vérifier que la source de données est configurée correctement, cliquez sur Tester la connexion dans la fenêtre de configuration de la source de données. Si la connexion de test échoue, redémarrez WebSphere et testez la connexion à nouveau.

Création d'une source de données ODBC pour l'utilisation avec CA SiteMinder

Si CA Identity Manager comprend SiteMinder, définissez une source de données ODBC dans l'ordinateur SiteMinder qui pointe vers la base de données. Notez le nom de la source de données aux fins d'utilisation ultérieure. Poursuivez comme suit :

- **Windows :** configurez la source de données ODBC comme nom unique du système. Pour plus d'informations, consultez la documentation du système d'exploitation Windows.
- **UNIX :** ajoutez une entrée spécifiant les paramètres de la source de données ODBC dans le fichier system_odbc.ini situé sous *policy_server_installation*/db.

Description d'une base de données dans un fichier de configuration d'annuaire

Pour gérer une base de données, CA Identity Manager doit comprendre la structure de la base de données et son contenu. Pour décrire base de données dans CA Identity Manager créez un fichier de configuration d'annuaire (directory.xml).

Le fichier de configuration d'annuaire contient l'une ou plusieurs des sections suivantes :

Informations de l'annuaire CA Identity Manager

Contient des informations sur l'annuaire CA Identity Manager utilisé par CA Identity Manager.

Validation de l'attribut

Définit les règles de validation qui s'appliquent à l'annuaire CA Identity Manager.

Informations sur le fournisseur

Décrit le référentiel d'utilisateurs géré par CA Identity Manager.

Informations de recherche d'annuaire

Permet de spécifier la méthode de recherche du référentiel d'utilisateurs utilisée par CA Identity Manager.

Objet utilisateur (page 117)

Décrit la méthode de stockage des utilisateurs dans le référentiel d'utilisateurs et leur représentation dans CA Identity Manager.

Objet groupe (page 117)

Décrit la méthode de stockage des groupes dans le référentiel d'utilisateurs et leur représentation dans CA Identity Manager.

Objet organisation (page 117)

Décrit la méthode de stockage des organisations et leur représentation dans CA Identity Manager.

Groupes avec auto-abonnement

Configure la prise en charge des groupes que les utilisateurs auto-enregistrés peuvent rejoindre.

Le répertoire dans lequel vous avez installé les outils d'administration CA Identity Manager inclut le modèle de fichier de configuration d'annuaire suivant pour des bases de données relationnelles :

admin_tools\directoryTemplates\RelationalDatabase\directory.xml

outils_admin

Définit l'emplacement d'installation des outils d'administration CA Identity Manager, comme dans les exemples suivants :

- **Windows** : <chemin_installation>\tools
- **UNIX** : <chemin_installation2>/tools

Remarque : Le modèle de fichier de configuration d'annuaire dans directoryTemplates\RelationalDatabase est configuré pour les environnements prenant en charge des organisations. Pour consulter un fichier de configuration d'annuaire pour un environnement qui n'inclut pas d'organisations, vous pouvez examiner le fichier directory.xml pour obtenir l'exemple NeteAuto situé sous *admin_tools*\samples\NeteAutoRDB\NoOrganization.

Copiez le modèle de configuration vers un nouvel annuaire ou enregistrez-le sous un nom différent pour éviter de l'écraser. Vous pouvez ensuite modifier le modèle pour refléter la structure de votre base de données.

Le fichier de configuration d'annuaire contient deux conventions importantes :

- ## : indique les valeurs requises.

  Pour fournir toutes les informations requises, recherchez tous les symboles de deux dièses (##) et remplacez-les par les valeurs appropriées. Par exemple, ##PASSWORD_HINT indique que vous devez fournir un attribut pour stocker une question à laquelle un utilisateur répond pour recevoir un mot de passe temporaire en cas de mot de passe oublié.

- @ : indique les valeurs remplies par CA Identity Manager. Ne modifiez pas ces valeurs dans le fichier de configuration d'annuaire. CA Identity Manager vous invite à fournir les valeurs lors de l'importation du fichier de configuration d'annuaire.

Avant de modifier ce fichier de configuration d'annuaire, les informations suivantes sont nécessaires :

- Les noms des tables pour les objets utilisateur, groupe organisation (si votre structure inclut des organisations)
- Une liste des attributs des profils d'utilisateur, de groupe et d'organisation (si votre structure inclut des organisations)

Modification du fichier de configuration d'annuaire

Pour modifier le fichier de configuration d'annuaire, suivez la procédure suivante.

Procédez comme suit:

1. Configurez une connexion à la base de données.
2. Spécifiez la durée de la recherche d'un annuaire CA Identity Manager avant de prendre fin.
3. Définissez les objets utilisateur et groupe gérés par CA Identity Manager (page 117).
4. Modifiez des attributs connus.

   Les attributs connus identifient des attributs spéciaux, par exemple l'attribut de mot de passe, dans CA Identity Manager.
5. Configurez la prise en charge des groupes avec auto-abonnement.
6. Si votre environnement inclut des organisations, configurez la prise en charge des organisations.

Descriptions d'objet géré

Dans CA Identity Manager, gérez les types d'objets suivants, correspondant à des entrées dans un référentiel d'utilisateurs :

- Utilisateurs : représentent les utilisateurs dans une entreprise.
- Groupes **:** représentent des associations d'utilisateurs ayant des éléments en commun.
- (Facultatif) Organisations : représentent des unités commerciales. Les organisations peuvent contenir des utilisateurs, des groupes et d'autres organisations.

  Remarque : La section Gestion des organisations (page 149) fournit des informations sur la configuration des organisations.

Une description d'objet contient les informations suivantes :

- Informations sur l'objet (page 118), telles que les tables dans lesquelles il est stocké
- Les attributs qui stockent des informations sur une entrée (page 122). Par exemple, l'attribut récepteur d'appels stocke un numéro de récepteur d'appels.

Important : Un environnement CA Identity Manager prend en charge un seul type d'objet utilisateur, groupe et organisation.

Description d'un objet géré

Un objet géré est décrit en spécifiant des informations dans les sections Objet utilisateur, Objet groupe et Objet organisation (si la base de donnés inclut des organisations) du fichier de configuration d'annuaire.

Chaque section contient un élément ImsManagedObject, comme le code suivant :

```
<ImsManagedObject name="User" description="My Users">
```

L'élément ImsManagedObject peut inclure les éléments suivants :

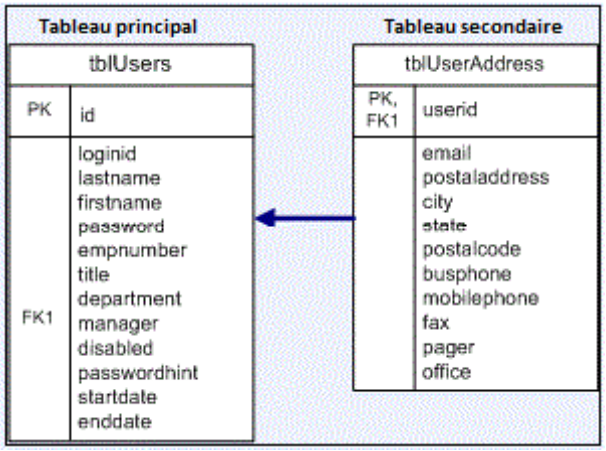
- Table (requise)
- UniqueIdentifier (requis)
- ImsManagedObjectAttr (requis)
- RootOrg (pour les objets organisation uniquement)

Database Tables

Utilisez l'élément Table dans le fichier de configuration d'annuaire pour définir les tables de stockage des informations sur un objet géré.

Chaque objet géré doit posséder une table principale qui contient l'identificateur unique de l'objet. Vous pouvez stocker des informations supplémentaires dans des tables secondaires.

Le schéma suivant illustre une base de données stockant les informations d'utilisateur dans une table principale et une table secondaire :



Si les informations d'un objet sont stockées dans plusieurs tables, créez un élément Table pour chaque table. Utilisez l'élément Reference dans l'élément Table d'une table secondaire pour définir sa relation avec la table principale.

Par exemple, si les informations de base d'un utilisateur sont stockées dans tblUsers et que les informations d'adresse sont stockées dans tblUserAddress, les définitions de table de l'objet géré utilisateur seront similaires aux entrées suivantes :

```
<Table name="tblUsers" primary="true" />
<Table name="tblUserAddress">
  <Reference childcol="userid" primarycol="id" />
</Table name>
```

Eléments Table

Les paramètres d'un élément Table se présentent comme suit :

name

(requis)

Spécifie le nom de la table qui stocke certains ou tous les attributs du profil géré d'un objet.

primary

Indique s'il s'agit de la table principale de l'objet géré. La table principale contient l'identificateur unique de l'objet, comme suit :

- True : il s'agit de la table principale.
- False : il s'agit d'une table secondaire (valeur par défaut).

Si vous ne spécifiez pas le paramètre primary, CA Identity Manager considère qu'il s'agit de table secondaire.

Remarque : Une seule table peut être principale.

filtre

Identifie un sous-ensemble des entrées de table qui s'appliquent à l'objet géré.

Le paramètre filter facultatif peut être comparable à l'exemple suivant :

```
filter="ORG=2"
```

Remarque : Le filtre s'applique uniquement aux requêtes générées par CA Identity Manager. Si vous remplacez une requête générée par une requête personnalisée, spécifiez le filtre dans la requête personnalisée.

fullouterjoin

Indique si la jointure externe est une jointure externe complète.

- True : il s'agit d'une jointure externe complète. Dans ce cas, la condition qui doit renvoyer une ligne valide figure dans les deux tables de la jointure d'une ligne renvoyée.
- False : il s'agit d'une jointure externe gauche relative à la table principale. Dans ce cas, les lignes d'une seule table de la requête doivent être conformes à la condition (valeur par défaut).

Remarque : Les paramètres sont facultatifs, sauf indication contraire.

Le paramètre Table peut contenir un ou plusieurs éléments Reference pour associer une table principale à des tables secondaires.

Elément Reference

Les paramètres de l'élément Reference se présentent comme suit :

childcol

Indique la colonne de la table secondaire (spécifiée dans l'élément Table correspondant) mappée vers la colonne de la table principale.

primarycol

Indique la colonne de la table principale mappée vers la colonne de la table secondaire.

Remarque : Les paramètres sont facultatifs, sauf indication contraire.

Spécification d'informations d'objet

Les informations d'objet sont spécifiées par des valeurs de différents paramètres.

Procédez comme suit:

1. Recherchez l'élément ImsManagedObject dans la section d'objet utilisateur, d'objet groupe, ou d'objet organisation.
2. Fournissez des valeurs pour les paramètres suivants :

   name

   (requis)

   Spécifie un nom unique pour l'objet géré.

   description

   Spécifie la description de l'objet géré.

objecttype

(requis)

Spécifie le type de l'objet géré. Les valeurs valides sont les suivantes.

- USER
- GROUP
- ORGANIZATION

L'élément ImsManagedObject doit être similaire au code suivant :

```
<ImsManagedObject name="User" description="My  Users" objecttype="USER">
```

3. Fournissez des informations sur l'élément Table, comme indiqué à la section Tables de base de données (page 118).
4. Spécifiez la colonne qui contient l'identificateur unique de l'objet (page 121).
5. Décrivez les attributs qui constituent le profil de l'objet (page 122).
6. Si vous configurez un objet organisation, consultez la section Gestion des organisations (page 149).

Spécification de l'identificateur unique d'un objet géré

Chaque objet géré par CA Identity Manager doit posséder un identificateur unique. Veillez à ce que l'identificateur unique soit stocké dans une colonne unique de la table principale de l'objet géré. Les tables principales sont décrites à la section Tables de base de données (page 118).

Utilisez les éléments UniqueIdentifier et UniqueIdentifierAttr pour définir l'identificateur unique comme suit :

```
<UniqueIdentifier>
  <UniqueIdentifierAttr name="nomtable.nomcolonne" />
</UniqueIdentifier>
```

L'élément UniqueIdentifierAttr requiert le paramètre name. La valeur du paramètre name est l'attribut dans lequel l'identificateur unique est stocké. Il peut s'agir d'un attribut physique ou d'un attribut connu (page 79).

Lorsque vous spécifiez un attribut physique, tenez compte des points suivants :

- Veillez à ce que l'attribut spécifié existe dans la base de données et qu'il soit défini dans le fichier de configuration d'annuaire, tel que décrit à la section Modification des descriptions d'attributs (page 122). Dans la description de l'attribut, veillez à spécifier l'autorisation Lecture seule ou Ecrire une fois pour éviter la modification de l'identificateur unique pendant une session.

- Pour spécifier un attribut physique, utilisez la syntaxe suivante :

  nom_table.nom_colonne

  nom_table

  Indique le nom de la table dans lequel l'attribut se trouve. Il doit s'agir de la table principale.

  nom_colonne

  Définit le nom de la colonne qui stocke l'attribut.

- Si la base de données génère l'identificateur unique, spécifiez une opération personnalisée pour l'attribut (page 133). Par exemple, vous devrez peut-être spécifier une opération d'extraction du dernier identificateur généré à partir de la base de données.

Modifier des descriptions d'attributs

Un attribut stocke des informations sur une entité utilisateur, groupe, ou organisation, telles qu'un numéro de téléphone ou une adresse. Les attributs d'une entité déterminent son profil.

Dans le fichier de configuration d'annuaire, les attributs sont décrits dans les éléments ImsManagedObjectAttr. Dans les sections d'objet utilisateur, d'objet groupe et d'objet organisation du fichier de configuration d'annuaire :

- Modifiez des descriptions d'attributs par défaut et décrivez vos attributs de base de données.
- Création de descriptions d'attribut en copiant une description existante et en modifiant des valeurs le cas échéant

Pour chaque attribut dans les profils d'utilisateur, de groupe et d'organisation, il existe un seul élément ImsManagedObjectAttr. Par exemple, un élément ImsManagedObjectAttr peut décrire un ID d'utilisateur.

Un élément ImsManagedObjectAttr est similaire au code suivant :

```
<ImsManagedObjectAttr
 physicalname="tblUsers.id"
 displayname="User Internal ID"
 description="User Internal ID"
 valuetype="Number"
 required="false"
 multivalued="false"
 maxlength="0"
 hidden="false"
 permission="READONLY">
```

Remarque : Lorsque vous utilisez une base de données Oracle, tenez compte des points suivants lors de la configuration d'attributs d'objet géré :

- Par défaut, les bases de données Oracle respectent la casse. La casse des attributs et des noms de table dans le fichier de configuration d'annuaire doit correspondre à la casse des attributs dans Oracle.

  Veillez à spécifier une longueur maximum pour les types de données de chaîne pour éviter une troncation. Pour limiter la longueur des chaînes, vous pouvez créer une règle de validation de sorte à afficher une erreur lorsqu'un utilisateur saisit une chaîne qui dépasse la longueur maximum.

Les paramètres ImsManagedObjectAttr se présentent comme suit.

Remarque : Les paramètres sont facultatifs, sauf indication contraire.

physicalname

(requis)

Spécifie le nom physique de l'attribut, qui doit contenir l'un des détails suivants :

- Nom et emplacement du stockage de la valeur

  Format : *nom_table*.*nom_colonne*

  Par exemple, lorsqu'un attribut est stocké dans la colonne ID de la table tblUsers, le nom physique de cet attribut se présentera comme suit :

  tblUsers.id

  Vous devez définir chaque table contenant un attribut dans un élément Table (page 118).

- Un attribut connu

  Un attribut connu peut représenter une valeur calculée. Par exemple, vous pouvez utiliser un attribut connu pour faire référence à un attribut calculé à l'aide d'une opération personnalisée (page 133).

displayName

(requis)

Spécifie un nom unique pour l'attribut.

Dans la console d'utilisateur, le nom d'affichage s'affiche dans la liste d'attributs disponibles pour être ajoutés à une fenêtre de tâche.

Remarque : Ne modifiez pas le nom d'affichage d'un attribut dans le fichier de configuration d'annuaire (directory.xml). Pour modifier le nom de l'attribut dans une fenêtre de tâche, vous pouvez spécifier une étiquette pour l'attribut dans la définition de la fenêtre de tâche. Pour plus d'informations, consultez le *Manuel d'administration*.

description

Contient la description de l'attribut.

valuetype

Spécifie le type de données de l'attribut. Les valeurs valides sont les suivantes.

Chaîne

La valeur peut être une chaîne.

C'est la valeur par défaut.

Integer

La valeur doit être un nombre entier.

Remarque : Le nombre entier ne prend pas en charge les nombres décimaux.

Number

La valeur doit être un nombre entier. L'option de nombre prend en charge les nombres décimaux.

Date

La valeur doit analyser une date valide à l'aide du modèle suivant :

MM/JJ/AAAA

ISODate

La valeur doit analyser une date valide à l'aide du modèle MM-JJ-AAAA.

UnicenterDate

La valeur doit analyser une date valide à l'aide du modèle YYYYYYYDDD où :

YYYYYYY est une représentation à 7 chiffres pour une année commençant par 3 zéros. Par exemple : 0002008

DDD est la représentation à 3 chiffres du jour commençant par des zéros, le cas échéant. Les valeurs valides sont comprises dans la plage de 001 à 366.

Si le type de valeur d'un attribut est incorrect, les requêtes CA Identity Manager peuvent échouer.

Pour assurer le stockage correct d'un attribut dans la base de données, vous pouvez l'associer à une règle de validation.

required

Indique si une valeur doit être spécifiée pour l'attribut, comme suit :

- True : valeur requise
- False : valeur facultative (valeur par défaut)

valeurs multiples

Indique si l'attribut peut posséder plusieurs valeurs, comme suit :

- True : un attribut peut posséder plusieurs valeurs.
- False : l'attribut doit posséder une seule valeur (valeur par défaut).

Par exemple, l'attribut d'appartenance au groupe dans un profil d'utilisateur possède plusieurs valeurs pour stocker les groupes auxquels un utilisateur appartient.

Pour stocker des attributs à valeurs multiples dans une liste délimitée au lieu d'une table contenant plusieurs lignes, vous devez définir le charactère délimiteur dans le paramètre delimiter.

Veillez à ce que le nombre de valeurs possibles et la longueur de chaque valeur activée par la colonne soient suffisants.

Important : Veillez à ce que l'attribut d'appartenance au groupe dans la définition d'objet utilisateur possède plusieurs valeurs.

wellknown (connu)

Définit le nom de l'attribut connu.

Les attributs connus ont une signification spécifique dans CA Identity Manager.

Format : %*NOM_ATTRIBUT*%

Remarque : Lorsqu'une opération personnalisée est associée à un attribut, vous devez spécifier un attribut connu (page 79).

maxlength (longueur maximum)

Détermine la taille maximum de la colonne.

permission

Indique si vous pouvez modifier la valeur d'un attribut dans une fenêtre de tâche, comme suit :

READONLY (lecture seule)

La valeur est affichée, mais ne peut pas être modifiée.

WRITEONCE (écriture unique)

La valeur peut être modifiée une fois l'objet créé. Par exemple, un ID d'utilisateur peut être modifié uniquement après la création de l'utilisateur.

READWRITE (lecture et écriture)

Vous pouvez modifier la valeur (valeur par défaut).

hidden

Indique si un attribut s'affiche dans les fenêtres de tâche CA Identity Manager, comme suit :

- True : l'attribut n'est pas affiché pour les utilisateurs.
- False : l'attribut est affiché pour les utilisateurs (valeur par défaut).

Les attributs logiques utilisent des attributs masqués.

Remarque : Pour plus d'informations sur les attributs logiques, reportez-vous au manuel *Programming Guide for Java*.

system

Indique que seul CA Identity Manager utilise des attributs. Les utilisateurs ne doivent pas modifier les attributs dans la console d'utilisateur, comme suit :

- True : les utilisateurs ne peuvent pas modifier l'attribut. L'attribut ne s'affichera pas dans la console d'utilisateur.
- False : les utilisateurs peuvent modifier cet attribut, qui peut être ajouté à des fenêtres de tâche dans la console d'utilisateur (valeur par défaut).

validationruleset

Associe un ensemble de règles de validation à l'attribut.

Vérifiez que l'ensemble de règles de validation spécifié est défini dans un élément ValidationRuleSet du fichier de configuration d'annuaire.

delimiter

Définit le caractère de séparation lorsque plusieurs valeurs sont stockées dans une seule colonne.

Important : Veillez à définir le paramètre valeurs multiples sur True pour appliquer le paramètre delimiter.

Remarque : Pour éviter l'affichage d'informations confidentielles, telles que les mots de passe ou les salaires, dans la console d'utilisateur, vous pouvez spécifier des paramètres DataClassification. (page 74)

Gestion des attributs sensibles

CA Identity Manager fournit les méthodes suivantes pour la gestion des attributs sensibles :

- Classifications de données des attributs

  Les classifications de données permettent de spécifier des propriétés d'affichage et de chiffrement pour des attributs dans le fichier de configuration d'annuaire (directory.xml).

  Vous pouvez définir des classifications de données qui gèrent des attributs sensibles comme suit :

  - Dans les fenêtres de tâche CA Identity Manager, affichez la valeur d'un attribut sous forme d'une série d'astérisques.

    Par exemple, vous pouvez afficher des mots de passe sous forme d'astérisques au lieu de les afficher en texte clair.

  - Dans les fenêtres Afficher les tâches soumises, masquez la valeur d'attribut.

    Cette option permet de masquer des attributs pour les administrateurs. Par exemple, vous pouvez masquer les détails des salaires pour des administrateurs qui consultent le statut des tâches dans CA Identity Manager, mais n'ont pas besoin de connaître les détails des salaires.

  - Ignorez certains attributs lors de la création d'une copie d'un objet existant.
  - Chiffrez un attribut.

- Styles de champ dans les fenêtres de profil de tâche

  Si vous ne voulez pas modifier d'attributs dans le fichier directory.xml, définissez la propriété d'affichage de l'attribut dans les définitions de fenêtres dans lesquelles l'attribut sensible apparaît.

  Le style de champ permet d'afficher des attributs, tels que des mots de passe, sous forme de série d'astérisques au lieu du texte clair.

  Remarque : Pour plus d'informations sur le style de champ des attributs sensibles, recherchez les styles de champ dans l'aide de la console d'utilisateur.

Attributs de classification de données

L'élément de classification des données fournit une méthode permettant d'associer des propriétés supplémentaires à une description d'attribut. Les valeurs de cet élément déterminent la gestion par CA Identity Manager de l'attribut. Cet élément prend en charge les paramètres suivants :

- sensitive

  CA Identity Manager affichera l'attribut sous forme d'une série d'astérisques (*) dans les fenêtres Afficher les tâches soumises. Ce paramètre empêche les valeurs anciennes et nouvelles de l'attribut de s'afficher en texte clair dans les fenêtres Afficher les tâches soumises.

  En outre, si vous créez une copie d'un utilisateur existant dans la console d'utilisateur, ce paramètre empêchera l'attribut d'être copié vers le nouvel utilisateur.

- vst_hide

  Masque l'attribut dans la fenêtre Détails de l'événement de l'onglet Afficher les tâches soumises. Contrairement aux attributs sensibles, qui sont affichés sous forme d'astérisques, les attributs vst_hidden ne sont pas affichés.

  Vous pouvez utiliser ce paramètre pour éviter que les modifications apportées à un attribut, tel que le salaire, ne s'affichent dans Afficher les tâches soumises.

- ignore_on_copy

  CA Identity Manager ignore un attribut lorsqu'un administrateur crée une copie d'un objet dans la console d'utilisateur. Par exemple, supposons que vous avez spécifié ignore_on_copy pour l'attribut de mot de passe sur un objet d'utilisateur. Lors de la copie d'un profil d'utilisateur, CA Identity Manager n'appliquera pas le mot de passe de l'utilisateur actuel au nouveau profil d'utilisateur.

- AttributeLevelEncrypt

  Chiffre les valeurs d'attribut si elles sont stockées dans le référentiel d'utilisateurs. Si la norme FIPS 140-2 est activée pour CA Identity Manager, CA Identity Manager utilisera le chiffrement RC2 ou FIPS 140-2.

  Pour plus d'informations sur la prise en charge de FIPS 140-2 dans CA Identity Manager, consultez le *Manuel de configuration*.

  Les attributs s'affichent en texte clair pendant l'exécution.

  Remarque : Pour éviter que des attributs s'affichent en texte clair dans des fenêtres, vous pouvez également ajouter un élément de classification de données sensibles à des attributs chiffrés. Pour plus d'informations, consultez la section Ajout du chiffrement de niveau attribut (page 75).

- PreviouslyEncrypted

  CA Identity Manager détecte et déchiffre toute valeur chiffrée dans l'attribut lors de l'accès à l'objet dans le référentiel d'utilisateurs.

  Utilisez cette classification de données pour déchiffrer toute valeur préalablement chiffrée.

  La valeur du texte clair est enregistrée dans le référentiel lors de l'enregistrement de l'objet.

Configuration des attributs de classification de données

Procédez comme suit:

1. Recherchez l'attribut dans le fichier de configuration d'annuaire.
2. Après la description d'attribut, ajoutez l'attribut suivant :

   <DataClassification name="*parameter*">

   parameter

   Représente l'un des paramètres suivants :

   sensitive

   vst_hide

   ignore_on_copy

   AttributeLevelEncrypt

   PreviouslyEncrypted

   Par exemple, une description d'attribut qui inclut l'attribut de classification de données vst_hide est similaire au code suivant :

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false" multivalued="false"
maxlength="0">
    <DataClassification name="vst_hide"/>
```

Chiffrement de niveau attribut

Vous pouvez chiffrer un attribut dans le référentiel d'utilisateurs en spécifiant la classification de données AttributeLevelEncypt pour cet attribut dans le fichier de configuration d'annuaire (directory.xml). Lorsque le chiffrement de niveau attribut est activé, CA Identity Manager chiffre la valeur de cet attribut avant de la stocker dans le référentiel d'utilisateurs. L'attribut est affiché en texte clair dans la console d'utilisateur.

Remarque : Pour éviter que des attributs s'affichent en texte clair dans des fenêtres, vous pouvez également ajouter un élément de classification de données sensibles à des attributs chiffrés. Pour plus d'informations, consultez la section Ajout du chiffrement de niveau attribut (page 75).

Si la prise en charge de FIPS 140-2 est activée, l'attribut sera chiffré à l'aide du chiffrement RC2 ou FIPS 140-2.

Avant d'implémenter le chiffrement de niveau attribut, tenez compte des points suivants :

- CA Identity Manager ne peut pas détecter les attributs chiffrés dans une recherche.

  Supposons qu'un attribut chiffré est ajouté à une stratégie de membre, d'administration, de propriété, ou d'identités. CA Identity Manager ne peut pas résoudre correctement la stratégie, car il ne peut pas rechercher l'attribut.

  Prévoyez de définir l'attribut sur searchable="false" dans le fichier directory.xml. Par exemple :

  <ImsManagedObjectAttr physicalname="title" description="Title" displayname="Title" valuetype="String" maxlength="0" searchable="false">

  <DataClassification name="AttributeLevelEncrypt"/>

  </ImsManagedObjectAttr>

- Si CA Identity Manager utilise un référentiel d'utilisateurs partagé et un annuaire de provisionnement, ne chiffrez pas les attributs du serveur de provisionnement.
- N'activez pas AttributeLevelEncrypt pour les mots de passe d'utilisateur dans les environnements conformes aux critères suivants :
  - Intégration de CA SiteMinder
  - Stockage d'utilisateurs dans une base de données relationnelles

  Lorsque CA Identity Manager comprend CA SiteMinder, les mots de passe chiffrés entraînent des problèmes lorsque des utilisateurs nouveaux tentent de se connecter et saisissent leur mot de passe en texte clair.
- Si vous activez le chiffrement de niveau attribut pour un référentiel d'utilisateurs utilisé par d'autres applications que CA Identity Manager, elles ne pourront pas utiliser l'attribut chiffré.

Ajout du chiffrement de niveau attribut

Supposons que vous avez ajouté un chiffrement de niveau attribut à un annuaire CA Identity Manager. CA Identity Manager chiffre automatiquement les valeurs d'attributs en texte clair existants lors de l'enregistrement de l'objet associé à l'attribut. Par exemple, le chiffrement de l'attribut de mot de passe permet de chiffrer le mot de passe lors de l'enregistrement du profil de l'utilisateur.

Remarque : Pour chiffrer la valeur d'un attribut, la tâche utilisée pour enregistrer l'objet doit inclure cet attribut. Pour chiffrer l'attribut de mot de passe dans l'exemple précédent, veillez à ce que le champ de mot de passe soit ajouté à la tâche utilisée pour enregistrer l'objet, telle que la tâche Modifier un utilisateur.

Tous les nouveaux objets sont créés avec des valeurs chiffrées dans le référentiel d'utilisateurs.

Procédez comme suit:

1. Effectuez l'une des tâches suivantes :
   - Création d'un annuaire CA Identity Manager
   - Mise à jour d'un annuaire existant via l'exportation des paramètres d'annuaire
2. Ajout des attributs de classification de données suivants à l'attribut que vous voulez chiffrer dans le fichier directory.xml :

   AttributeLevelEncrypt

   Conserve la valeur de l'attribut sous forme chiffré dans le référentiel d'utilisateurs.

   sensitive (facultatif)

   Masque la valeur de l'attribut dans les fenêtres CA Identity Manager. Par exemple, un mot de passe s'affiche sous forme d'astérisques (*).

   Exemple :

```
<ImsManagedObjectAttr physicalname="salary"
displayname="Salary" description="salary" valuetype="String"
required="false" multivalued="false" maxlength="0"
searchable="false">
<DataClassification name="AttributeLevelEncrypt"/>
<DataClassification name="sensitive"/>
```

3. Si vous avez créé un annuaire CA Identity Manager, associez-le à un environnement.
4. Pour forcer CA Identity Manager à chiffrer toutes les valeurs immédiatement, modifiez tous les objets à l'aide du chargeur en bloc.

   Remarque : Pour plus d'informations sur le chargeur en bloc, consultez le *Manuel d'administration*.

Suppression du chiffrement de niveau attribut

Si vous avez un attribut chiffré dans l'annuaire CA Identity Manager, stocké avec la valeur en texte clair, vous pouvez supprimer la classification de données AttributeLevelEncrypt.

Une fois la classification de données supprimée, CA Identity Manager arrête de chiffrer les nouvelles valeurs d'attribut. Les valeurs existantes sont déchiffrées lors de l'enregistrement de l'objet à l'attribut.

Remarque : Pour déchiffrer la valeur d'un attribut, la tâche utilisée pour enregistrer l'objet doit inclure cet attribut. Par exemple, pour déchiffrer le mot de passe d'un utilisateur existant, enregistrez l'objet d'utilisateur avec une tâche qui inclut le champ de mot de passe, telles que la tâche Modifier un utilisateur.

Pour forcer CA Identity Manager à détecter et déchiffrer toute valeur de l'attribut chiffrée conservée dans le référentiel d'utilisateurs, vous pouvez spécifier une autre classification de données : PreviouslyEncrypted. La valeur du texte clair est enregistrée dans le référentiel d'utilisateurs lors de l'enregistrement de l'objet.

Remarque : L'ajout de la classification de données PreviouslyEncrypted ajoute un traitement supplémentaire sur chaque chargement d'objet. Pour éviter tout problème de performance, envisagez d'ajouter la classification de données PreviouslyEncrypted, en chargeant et en enregistrant chaque objet associé à cet attribut, puis en supprimant la classification de données. Cette méthode convertit automatiquement toutes les valeurs chiffrées stockées en texte clair stocké.

Procédez comme suit:

1. Exportez les paramètres de l'annuaire CA Identity Manager approprié.
2. Dans le fichier directory.xml, supprimez la classification de données AttributeLevelEncrypt des attributs que vous voulez déchiffrer.
3. Si vous voulez forcer CA Identity Manager à supprimer préalablement des valeurs chiffrées, ajoutez l'attribut de classification de données PreviouslyEncrypted.

   Exemple :

   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false" multivalued="false"
   maxlength="0" searchable="false">
   <DataClassification name="PreviouslyEncrypted"/>
   ```

4. Pour forcer CA Identity Manager à déchiffrer toutes les valeurs immédiatement, modifiez tous les objets à l'aide du chargeur en bloc.

   Remarque : Pour plus d'informations sur le chargeur en bloc, consultez le *Manuel d'administration*.

Opérations personnalisées

Vous pouvez définir des opérations personnalisées de sorte à ce que certains objets gérés exécutent les tâches suivantes :

- Utilisation des procédures stockées
- Optimisation des requêtes pour leur structure de base de données
- Récupération d'un identificateur unique généré par la base de données

Les opérations personnalisées s'appliquent uniquement aux attributs.

Lors de la spécification d'opérations personnalisées, tenez compte des points suivants :

- Les utilisateurs qui spécifient des opérations personnalisées doivent connaître SQL.
- CA Identity Manager ne valide pas les opérations personnalisées. Avant l'exécution, les erreurs de syntaxe et les requêtes non valides ne sont pas signalées.

- Si vous spécifiez une opération personnalisée pour un attribut, vous ne pouvez pas utiliser cet attribut dans les filtres de recherche dans les tâches CA Identity Manager.
- Les opérations personnalisées doivent respecter les normes XML. Représentez des caractères spéciaux à l'aide de la syntaxe XML. Par exemple, spécifiez une apostrophe (') sous la forme &apos ;.

Pour spécifier une opération personnalisée, utilisez l'élément Operation.

Elément Operation

L'élément Operation définit une instruction SQL qui peut exécuter une requête personnalisée ou requiert une procédure stockée pour la création, la récupération, la modification, ou la suppression d'un attribut. L'élément Operation est un sous-élément de l'élément IMSManagedObjectAttr, comme illustré dans l'exemple suivant :

```
<ImsManagedObjectAttr physicalname="tblUsers.id" displayname="User Internal ID"
description="User Internal ID" valuetype="Number" required="false"
multivalued="false" maxlength="0" hidden="false" permission="READONLY">
  <Operation name="GetDb" value="select @@identity" />
```

Les paramètres de l'élément Operation se présentent comme suit :

name

Spécifie un nom prédéfini pour une opération. Les opérations valides sont les suivantes.

- Créer
- Obtenir
- Définir
- Supprimer
- GetDB

  L'opération GetDB permet de récupérer un identificateur unique de la base de données lors d'une tâche Créer, lorsque l'identificateur unique est généré dans la base de données ou à partir d'une procédure stockée.

value

Définit l'instruction SQL ou une procédure stockés à exécuter. Les valeurs valides sont les suivantes.

- INSERT
- SELECT

- UPDATE
- DELETE
- CALL (pour des procédures stockées)

Remarque : Les paramètres sont facultatifs, sauf indication contraire.

L'élément Operation peut contenir un ou plusieurs éléments Parameter.

Elément Parameter

Un élément Parameter spécifie des valeurs transmises à la requête. Lorsque plusieurs éléments Parameter sont définis, les valeurs sont transmises à la requête dans l'ordre de la liste indiqué.

Un élément Parameter requiert le paramètre name. La valeur du paramètre name peut être un attribut physique ou un attribut connu (page 79).

Remarque : CA Identity Manager doit connaître les valeurs transmises à une requête dans l'élément Parameter. Par exemple, la valeur peut être un nom physique ou un attribut connu défini dans les attributs ImsManagedObjectAttr.

Lorsque vous spécifiez un attribut physique, tenez compte des points suivants :

- Pour spécifier un attribut physique, utilisez la syntaxe suivante :

  nom_table.nom_colonne

  - *nom_table*

    Indique le nom de la table dans lequel l'attribut se trouve. Il doit s'agir de la table principale.

  - *nom_colonne*

    Définit le nom de la colonne qui stocke l'attribut.

- L'attribut spécifié doit exister dans la base de données et être défini dans le fichier de configuration d'annuaire, tel que décrit à la section Modification des descriptions d'attributs (page 122).

Exemple d'opérations personnalisées pour l'attribut Business Number (Numéro d'entreprise)

Dans l'exemple suivant, l'attribut Business Number est généré par l'appel d'une procédure stockée ; il ne s'agit pas d'un attribut physique dans la base de données.

```
<ImsManagedObjectAttr wellknown="%BUSINESS_NUMBER%"     displayname="Business
Number" description="Business Number"     valuetype="String" required="false"
multivalued="false"     maxlength="0">
<Operation name="Get" value="call sp_getbusinessnumber(?)">
    <Parameter name="%USER_ID%"/>
</Operation>
```

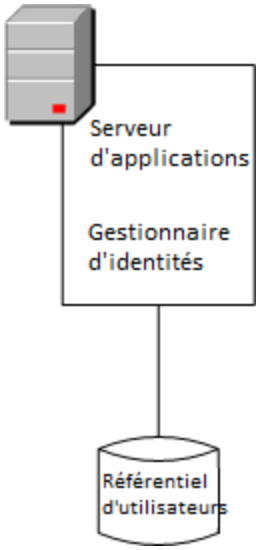
```
<Operation name="Set" value="call sp_setbusinessnumber(?,?)">
    <Parameter name="%USER_ID%"/>
    <Parameter name="%BUSINESS_NUMBER%"/>
</Operation>
<Operation name="Delete" value="call sp_deletebusinessnumber(?)">
    <Parameter name="%USER_ID%"/>
</Operation>
```

Notez les points suivants :

- sp_getbusinessnumber, sp_setbusinessnumbe, et sp_deletebusinessnumber sont des procédures stockées définies par l'utilisateur.
- La valeur renvoyée par l'opération Obtenir est mappée vers l'attribut %BUSINESS_NUMBER%.
- Le point d'interrogation (?) indique des remplacements effectuées lors de l'exécution avant l'exécution de la requête. Par exemple, dans l'opération Obtenir, l'attribut connu %USER_ID% est transmise à la procédure stockée sp_getbusinessnumber.

Connexion à l'annuaire d'utilisateurs

CA Identity Manager se connecte à un annuaire d'utilisateurs pour stocker des informations par exemple sur les utilisateurs, les groupes et les organisations comme illustré dans le schéma suivant :



Un nouvel annuaire ou une nouvelle base de données n'est pas nécessaire. Toutefois, l'annuaire ou la base de données qui existe doit être placé dans un système avec un nom de domaine complet.

Pour obtenir une liste de types d'annuaire et de base de données pris en charge, consultez le tableau de prise en charge CA Identity Manager sur le site du support de CA.

Configurez une connexion au référentiel d'utilisateurs lors de la création d'un annuaire CA Identity Manager dans la console de gestion.

Si vous exportez la configuration d'annuaire après la création d'un annuaire CA Identity Manager, les informations de connexion à l'annuaire d'utilisateurs apparaissent dans l'élément fournisseur du fichier de configuration d'annuaire.

Description d'une connexion à la base de données

Pour décrire une connexion à la base de données, utilisez l'élément Provider et ses sous-éléments dans le fichier directory.xml.

Remarque : Si vous créez un annuaire CA Identity Manager, il n'est pas nécessaire de fournir des informations de connexion à l'annuaire dans le fichier directory.xml. Indiquez les informations de connexion dans l'assistant de création d'annuaires CA Identity Manager dans la console de gestion.

Modifiez l'élément fournisseur aux fins de mise à jour uniquement.

Elément fournisseur

L'élément fournisseur inclut les sous-éléments suivants :

JDBC (requis)

Identifie la source de données JDBC à utiliser lors de la connexion au référentiel d'utilisateurs. Spécifiez le nom JNDI fourni lors de la création de la source de données JDBC (page 107).

Informations d'identification (requises)

Fournit le nom d'utilisateur et le mot de passe permettant d'accéder à la base de données.

DSN

Identifie la source de données ODBC à utiliser lors de la connexion au référentiel d'utilisateurs.

Remarque : Ce sous-élément s'applique uniquement lorsque CA Identity Manager comprend SiteMinder. Dans les environnements CA Identity Manager qui n'incluent pas SiteMinder, ce sous-élément est ignoré.

SiteMinderQuery

Spécifie des schémas de requête personnalisés pour rechercher des informations d'utilisateur dans une base de données relationnelles.

Remarque : Ce sous-élément s'applique uniquement lorsque CA Identity Manager comprend SiteMinder. Dans les environnements CA Identity Manager qui n'incluent pas SiteMinder, ce sous-élément est ignoré.

Une connexion à la base de données terminée est comparable à l'exemple suivant :

```
<Provider type="RDB" userdirectory="@SMDirName">
        <JDBC datasource="@SMDirJDBCDataSource"/>
        <Credentials user="@SMDirUser"
                cleartext="true">@SMDirPassword</Credentials>
        <DSN name="@SMDirDSN" />
        <SiteMinderQuery name="AuthenticateUser" query="SELECT TBLUSERS.LOGINID
FROM    TBLUSERS WHERE TBLUSERS.LOGINID='%s' AND TBLUSERS.PASSWORD='%s'" />
</provider>
```

Les attributs de l'élément Provider se présentent comme suit :

type

Spécifie le type de base de données. Pour les bases de données Microsoft SQL Server et Oracle, spécifiez RDB (valeur par défaut).

userdirectory

Spécifie le nom de la connexion à l'annuaire d'utilisateurs. Ce paramètre correspond au nom de l'objet de connexion fourni lors de la création de l'annuaire.

Si CA Identity Manager comprend SiteMinder pour l'authentification, il crée une connexion à l'annuaire d'utilisateurs dans SiteMinder avec le nom spécifié pour l'objet de connexion lors de l'installation. Si vous voulez vous connecter à un annuaire d'utilisateurs SiteMinder existant, saisissez le nom de cet annuaire d'utilisateurs lorsque l'objet de connexion est demandé. CA Identity Manager remplit le paramètre userdirectory avec le nom que vous spécifiez.

Si CA Identity Manager ne comprend pas SiteMinder, la valeur du paramètre userdirectory est un nom que vous donnez à la connexion JDBC au référentiel d'utilisateurs.

Remarque : Ne spécifiez pas de nom pour la connexion à l'annuaire d'utilisateurs dans le fichier directory.xml. CA Identity Manager vous invite à fournir le nom lors de la création de l'annuaire.

Informations d'identification de la base de données

Pour se connecter à la base de données, CA Identity Manager doit fournir des informations d'identification valides à la source de données. Ces informations d'identification sont définies dans le sous-élément Credentials, similaire au code suivant :

```
<Credentials user="@SMDirUser" cleartext="true">
  "MyPassword"
</Credentials>
```

Si vous ne spécifiez pas de mot de passe dans l'élément Credentials et que vous tentez de créer l'annuaire CA Identity Manager dans la console de gestion, vous serez invité à fournir le mot de passe.

Remarque : Il est recommandé de spécifier le mot de passe dans la console de gestion.

Ainsi, CA Identity Manager chiffre le mot de passe pour vous. Dans le cas contraire, si vous ne voulez pas que le mot de passe s'affiche en texte clair, chiffrez le mot de passe à l'aide de l'outil de modification de mots de passe fourni avec CA Identity Manager. Les mots de passe de CA SiteMinder contiennent des instructions pour l'utilisation de l'outil de modification de mots de passe.

Remarque : Vous pouvez spécifier un seul ensemble d'informations d'identification. Lorsque vous définissez plusieurs sources de données, les informations d'identification spécifiées doivent s'appliquer à toutes ces sources de données.

Les paramètres d'informations d'identification se présentent comme suit.

utilisateur

Spécifie l'ID de connexion d'un compte pouvant accéder à la source de données.

Ne spécifiez aucune valeur pour le paramètre utilisateur dans le fichier directory.xml. CA Identity Manager vous invite à fournir l'ID de connexion lors de la création de l'annuaire CA Identity Manager dans la console de gestion.

cleartext

Détermine si le mot de passe est affiché en texte clair dans le fichier directory.xml :

- True : le mot de passe est affiché en texte clair.
- False : le mot de passe est chiffré (valeur par défaut).

Remarque : Ces paramètres sont facultatifs.

Nom de la source de données (DSN)

L'élément DSN dans le fichier directory.xml contient un paramètre, le nom de la source de données ODBC utilisée par CA Identity Manager pour se connecter à la base de données. La valeur du paramètre name doit correspondre au nom d'une source de données existante.

Remarque : Cet élément s'applique uniquement lorsque CA Identity Manager comprend SiteMinder. Sinon, cet élément sera ignoré.

Si la valeur du paramètre name est @SmDirDSN, vous ne devez pas spécifier un nom DSN dans le fichier directory.xml. CA Identity Manager vous invite à fournir le nom DSN lors de l'importation du fichier directory.xml.

Pour configurer un basculement, définissez plusieurs éléments DSN. Si la source de données principale ne répond pas à une demande, la source de données suivante définie y répondra.

Par exemple, supposons que vous avez configuré le basculement de la façon suivante :

```
<nom DSN="DSN1">
<nom DSN="DSN2">
```

CA Identity Manager utilise la source de données DSN1 pour se connecter à la base de données. En cas de problème avec DSN1, CA Identity Manager tentera de se connecter à la base de données à l'aide de DSN2.

Remarque : Les informations d'identification spécifiées dans l'élément Credentials (page 139) doivent s'appliquer à tous les DSN définis.

Schémas de requête SQL

CA Identity Manager utilise des schémas de requête pour rechercher des informations d'utilisateur et de groupe dans une base de données relationnelles.

Remarque : Cet élément s'applique uniquement lorsque CA Identity Manager comprend SiteMinder. Dans les environnements qui n'incluent pas SiteMinder, ce paramètre est ignoré.

Lorsque vous créez un annuaire CA Identity Manager dans la console de gestion, CA Identity Manager génère un ensemble de schémas de requête basés sur les schémas de requête requis dans SiteMinder. Pour obtenir des informations complètes sur les schémas de requête SiteMinder, consultez le manuel *SiteMinder Web Access Manager Policy Server Configuration Guide*. Les noms de tables et colonnes dans les schémas de requête SiteMinder sont remplacés par des données spécifiées dans le fichier de configuration d'annuaire.

Définir des schémas de requête personnalisés

Les schémas de requête sont définis dans des éléments SiteMinderQuery dans le fichier de configuration d'annuaire. Un élément SiteMinderQuery est comparable à l'élément suivant :

```
<SiteMinderQuery name="SetUserProperty" query="update tblUsers set %s =
&apos;%s&apos; where loginid = &apos;%s&apos;" />
```

Remarque : Dans la requête d'exemple, &apos ; est la syntaxe XML correspondant à l'apostrophe simple (').

L'élément SiteMinderQuery s'applique uniquement lorsque CA Identity Manager comprend SiteMinder.

Les paramètres de schéma de requête se présentent comme suit :

name

Spécifie le nom redéfini d'un schéma de requête SiteMinder.

Ne modifiez pas cette valeur.

requête

Définit l'instruction SQL ou une procédure stockée à exécuter. Les valeurs valides sont les suivantes.

- INSERT
- SELECT
- UPDATE
- DELETE
- CALL (pour des procédures stockées)

Remarque : Ces paramètres sont requis pour l'élément SiteMinderQuery.

Avant de personnaliser des schémas de requête, procédez comme suit :

- Familiarisez-vous avec les schémas de requête par défaut.

  Remarque : Pour plus d'informations sur les schémas de requête SQL, consultez le manuel *SiteMinder Web Access Manager Policy Server Configuration Guide*.
- Obtenez des informations étendues sur le développement de requêtes SQL.

Modification des schémas de requête par défaut

Pour modifier les schémas de requête par défaut, procédez comme suit.

Procédez comme suit:

1. Exportez le fichier de configuration d'annuaire.

   CA Identity Manager génère un fichier de configuration d'annuaire qui contient tous les paramètres actuels de l'annuaire CA Identity Manager, y compris les schémas de requête générés.

2. Enregistrez le fichier de configuration d'annuaire.

   Remarque : Si vous voulez créer une sauvegarde du fichier de configuration d'annuaire d'origine, enregistrez-le sous un nom différent ou à un emplacement différent avant d'enregistrer le fichier exporté.

3. Recherchez le schéma de requête généré par CA Identity Manager que vous voulez modifier.

4. Saisissez le schéma de requête ou la procédure stockée à exécuter dans le paramètre query.

   Remarque : Ne modifiez pas le nom de la requête.

5. Après avoir apporté les modifications nécessaires, enregistrez le fichier de configuration d'annuaire.

   Importez le fichier pour mettre à jour l'annuaire CA Ide (page 186)ntity Manager.

Attributs connus d'une base de données relationnelles

Les attributs connus ont une signification spécifique dans CA Identity Manager. Ils sont identifiés par la syntaxe suivante :

%ATTRIBUTENAME%

Dans cette syntaxe, *ATTRIBUTENAME* doit être en majuscule.

Un attribut connu est mappé vers un attribut physique, à l'aide d'une description d'attribut (page 122).

Dans la description d'attribut suivante, l'attribut tblUsers.password est mappé vers l'attribut connu %PASSWORD% de sorte que CA Identity Manager traite la valeur dans tblUsers.password comme mot de passe, de la manière suivante :

```
<ImsManagedObjectAttr
        physicalname="tblUsers.password"
        displayname="Password"
        description="Password"
        valuetype="String"
        required="false"
        multivalued="false"
        wellknown="%PASSWORD%"
        maxlength="0" />
```

Certains attributs connus sont requis ; d'autres sont facultatifs.

Attributs connus d'utilisateur

Voici une liste d'attributs connus utilisateur :

%ADMIN_ROLE_CONSTRAINT%

Contient la liste des rôles d'administration (page 146) affectés à l'administrateur (page 146).

L'attribut physique mappé vers %ADMIN_ROLE_CONSTRAINT% doit posséder plusieurs valeurs pour prendre en charge plusieurs rôles.

Il est recommandé d'indexer l'attribut mappé vers %ADMIN_ROLE_CONSTRAINT%.

%CERTIFICATION_STATUS%

(Requis pour l'utilisation de la fonctionnalité de certification d'utilisateur)

Contient le statut de certification d'un utilisateur.

Remarque : Pour plus d'informations sur la certification d'utilisateur, consultez le *Manuel d'administration*.

%DELEGATORS%

Mappe vers une liste d'utilisateurs ayant délégué des tâches à l'utilisateur actuel.

Cet attribut est requis pour utiliser la délégation. L'attribut physique de mappage vers %DELEGATORS% doit être de valeurs multiples et en mesure de stocker des chaînes.

Important : La modification de ce champ directement à l'aide de tâches CA Identity Manager ou d'un outil externe peut affecter la sécurité de manière significative.

%EMAIL%

(Requis pour activer la fonctionnalité de notification par courriel)

Stocke l'adresse électronique d'un utilisateur.

%ENABLED_STATE%

(requis)

Effectue un suivi du statut d'un utilisateur.

Remarque : Les données de l'attribut physique mappé vers %ENABLED_STATE% doivent être de type chaîne.

%FIRST_NAME%

Contient le prénom d'un utilisateur.

%FULL_NAME%

(requis)

Contient le prénom et le nom d'un utilisateur.

%IDENTITY_POLICY%

Contient la liste des stratégies d'identité appliquées à un compte d'utilisateur.

CA Identity Manager utilise cet attribut pour déterminer si une stratégie d'identité doit être appliquée à un utilisateur. Si le paramètre Apply Once (Appliquer une fois) de la stratégie est activé et que la stratégie est répertoriée dans l'attribut %IDENTITY_POLICY%, CA Identity Manager n'appliquera pas les modifications dans la stratégie à l'utilisateur.

Remarque : Pour plus d'informations sur les stratégies d'identité, consultez le *Manuel d'administration*.

%LAST_CERTIFIED_DATE%

(Requis pour l'utilisation de la fonctionnalité de certification d'utilisateur)

Contient la date de certification du rôle d'un utilisateur.

Remarque : Pour plus d'informations sur la certification d'utilisateur, consultez le *Manuel d'administration*.

%LAST_NAME%

Contient le nom d'un utilisateur.

%ORG_MEMBERSHIP%

(Requis si les organisations sont prises en charge)

Contient l'identificateur unique de l'organisation à laquelle l'utilisateur appartient.

%ORG_MEMBERSHIP_NAME%

(Requis si les organisations sont prises en charge)

Contient le nom convivial de l'organisation à laquelle l'utilisateur appartient.

%PASSWORD%

Contient le mot de passe d'un utilisateur.

Remarque : La valeur de l'attribut %PASSWORD% apparaît toujours sous forme de série d'astérisque (*) dans les fenêtres CA Identity Manager, même lorsque l'attribut ou le champ n'est pas défini pour masquer les mots de passe.

%PASSWORD_DATA%

(requis pour la prise en charge de la stratégie de mot de passe)

Spécifie l'attribut de suivi des informations de stratégie de mot de passe.

Remarque : La valeur de l'attribut %PASSWORD_DATA% apparaît toujours sous forme de série d'astérisque (*) dans les fenêtres CA Identity Manager, même lorsque l'attribut ou le champ n'est pas défini pour masquer les mots de passe.

%PASSWORD_HINT%

(requis)

Contient des paires de question/réponse spécifiées par l'utilisateur. Les paires de question/réponse sont utilisées en cas d'oubli de mots de passe.

Remarque : La valeur de l'attribut %PASSWORD_HINT% apparaît toujours sous forme de série d'astérisque (*) dans les fenêtres CA Identity Manager, même lorsque l'attribut ou le champ n'est pas défini pour masquer les mots de passe.

%USER_ID%

(Requis)

Stocke un ID de connexion d'utilisateur.

Attributs connus de groupe

La liste suivante répertorie les attributs de groupe connus :

%GROUP_ADMIN%

Contient les administrateurs d'un groupe.

Remarque : L'attribut %GROUP_ADMIN% doit être à valeurs multiples.

%GROUP_DESC%

Contient la description d'un groupe.

%GROUP_ID%

Contient l'identificateur unique d'un groupe.

%GROUP_MEMBERSHIP%

(Requis)

Contient une liste des membres d'un groupe.

Remarque : L'attribut %GROUP_MEMBERSHIP% doit être à valeurs multiples.

%GROUP_NAME%

(Requis)

Stocke le nom d'un groupe.

%ORG_MEMBERSHIP%

Requis si les organisations sont prises en charge.

Contient l'identificateur unique de l'organisation à laquelle le groupe appartient.

%ORG_MEMBERSHIP_NAME%

Requis si les organisations sont prises en charge.

Contient le nom convivial de l'organisation à laquelle le groupe appartient.

%SELF_SUBSCRIBING%

Détermine si les utilisateurs peuvent s'abonner à un groupe.

Attribut %Admin_Role_Constraint%

Lorsque vous créez un rôle d'administration, vous spécifiez une ou plusieurs règles d'appartenance au rôle. Les utilisateurs qui répondent aux critères stipulés par ces règles d'appartenance ont le rôle. Par exemple, si la règle d'appartenance pour le rôle Gestionnaire d'utilisateurs est title=User Manager, les utilisateurs qui disposent du titre User Manager ont le rôle Gestionnaire d'utilisateurs.

Remarque : Pour plus d'informations sur les règles, reportez-vous au *Manuel d'administration*.

%ADMIN_ROLE_CONSTRAINT% vous permet de désigner un attribut de profil pour stocker tous les rôles d'administration d'un administrateur.

Utilisation de l'attribut %ADMIN_ROLE_CONSTRAINT%

Pour utiliser l'attribut %ADMIN_ROLE_CONSTRAINT% comme contrainte pour tous les rôles d'administration, procédez comme suit :

- Associez l'attribut connu %ADMIN_ROLE_CONSTRAINT% avec un attribut de profil à valeurs multiples pour prendre en charge plusieurs rôles.

- Lorsque vous configurez un rôle d'administration dans l'interface utilisateur de CA Identity Manager, le scénario suivant peut être une contrainte :

  Rôles d'administration égal à *nom_rôle*

  nom_rôle

  Définit le nom du rôle pour lequel vous spécifiez la contrainte.

  Par exemple, Rôles d'administration égal à Gestionnaire d'utilisateurs.

Remarque : Rôles d'administration est le nom d'affichage par défaut pour l'attribut %ADMIN_ROLE_CONSTRAINT%.

Configuration des attributs connus

Effectuez la procédure suivante pour configurer des attributs connus.

Procédez comme suit:

1. Dans le fichier de configuration d'annuaire, recherchez le signe suivant :

   ##

   Les valeurs requises sont identifiées par deux dièses (##).

2. Remplacez la valeur qui commence par ## par le nom physique de l'attribut approprié, tel qu'il existe dans la base de données. Spécifiez le nom de l'attribut au format suivant :

   nom_table.nom_colonne

   Par exemple, si l'attribut de mot de passe est stocké dans la colonne password de la table tblUsers, spécifiez-le de la façon suivante :

   `tblUsers.password`

3. Répétez les étapes 1 et 2 jusqu'à ce que vous ayez remplacé toutes les valeurs requises et les valeurs facultatives incluses que vous voulez.
4. Mappez les attributs connus facultatifs vers des attributs physiques, selon vos besoins.
5. Enregistrez le fichier de configuration d'annuaire.

Procédure de configuration de groupes avec auto-abonnement

Vous pouvez permettre aux utilisateurs de l'auto-administration de rejoindre des groupes en configurant la prise en charge des groupes d'auto-abonnement dans le fichier de configuration d'annuaire.

Procédez comme suit:

1. Dans la section des groupes d'auto-abonnement, ajoutez un élément SelfSubscribingGroups comme suit :

   ```
   <SelfSubscribingGroups type=type_recherche org=nom_unique_organisation>
   ```

2. Saisissez des valeurs pour les paramètres suivants :

   type

   Indique l'emplacement dans lequel CA Identity Manager recherche les groupes d'auto-abonnement. Les valeurs valides sont les suivantes.

   - NONE : CA Identity Manager ne recherche aucun groupe. Spécifiez NONE pour empêcher les utilisateurs de s'abonner à des groupes.
   - ALL : CA Identity Manager recherche tous les groupes du référentiel d'utilisateurs. Spécifiez ALL lorsque les utilisateurs peuvent s'abonner à tous les groupes.
   - INDICATEDORG (*uniquement pour les environnements qui prennent en charge les organisations*) : CA Identity Manager recherche les groupes d'auto-abonnement dans l'organisation d'un utilisateur et dans ses sous-organisations. Par exemple, lorsque le profil d'un utilisateur se trouve dans l'organisation Marketing, CA Identity Manager recherche les groupes d'auto-abonnement dans l'organisation Marketing et dans toutes ses sous-organisations.
   - SPECIFICORG (*uniquement pour les environnements qui prennent en charge les organisations*) : CA Identity Manager effectue les recherches dans une organisation spécifique. Spécifiez l'identificateur unique de l'organisation dans le paramètre org.

   org

   Définit l'identificateur unique de l'organisation dans laquelle CA Identity Manager recherche les groupes d'auto-abonnement.

   Remarque : Assurez-vous de spécifier le paramètre org si type=SPECIFICORG.

3. Redémarrez le serveur de stratégies SiteMinder si vous avez modifié :
   - le paramètre type sur SPECIFICORG ou si vous avez remplacé SPECIFICORG.
   - la valeur du paramètre org.

Une fois que la prise en charge des groupes d'auto-abonnement est configurée dans l'annuaire CA Identity Manager, les administrateurs CA Identity Manager peuvent spécifier ces groupes dans la console d'utilisateur.

Lorsqu'un utilisateur s'auto-inscrit, CA Identity Manager recherche les groupes des organisations spécifiées et affiche les groupes d'auto-abonnement.

Règles de validation

Une règle de validation applique des conditions aux données qu'un utilisateur saisit dans un champ de fenêtre de tâche. Les conditions permettent d'appliquer un type de données ou un format, ou de s'assurer de la validité des données dans le contexte d'autres données dans la fenêtre de tâche.

Les règles de validation sont associées à des attributs de profil. Avant le traitement d'une tâche, CA Identity Manager vérifie que les données entrées pour un attribut de profil soient conformes aux règles de validation associées.

Vous pouvez définir des règles de validation et les associer à des attributs de profil dans le fichier de configuration d'annuaire.

Gestion des organisations

CA Identity Manager vous permet de gérer les organisations pour les bases de données relationnelles. Si votre base de données prend en charge les organisations, les points suivants sont vrais :

- Les organisations ont une structure hiérarchique.
- Tous les objets gérés, tels que les utilisateurs, les groupes et d'autres organisations appartiennent à une organisation.
- Lorsque vous supprimez une organisation, les objets qu'elle comprend sont également supprimés.

Vous configurez l'objet d'organisation de la même façon que vous configurez les objets d'utilisateur et de groupe, avec quelques étapes supplémentaires.

Configuration de la prise en charge des organisations

Effectuez la procédure suivante pour configurer la prise en charge des organisations :

1. Configurez la prise en charge des organisations dans la base de données (page 150).
2. Décrivez l'objet d'organisation dans ImsManagedObject (page 118).

   Configurez les sous-éléments Table et UniqueIdentifier.

3. Configurez l'organisation de niveau supérieure (page 150).
4. Décrivez les attributs (page 122) qui constituent une organisation.
5. Définissez les attributs connus pour l'objet d'organisation (page 151).

Configuration de la prise en charge des organisations dans la base de données

Procédez comme suit:

1. Ouvrez l'un des scripts SQL suivants dans un éditeur :
   - Bases de données Microsoft SQL Server

     ims_mssql_rdb.sql
   - Bases de données Oracle :

     ims_oracle_rdb.sql

     Ces fichiers sont enregistrés dans l'emplacement suivant :

     outils_admin\directoryTemplates\RelationalDatabase

     outils_admin fait référence à l'emplacement d'installation des outils d'administration, qui se trouvent dans l'un des emplacements suivants :

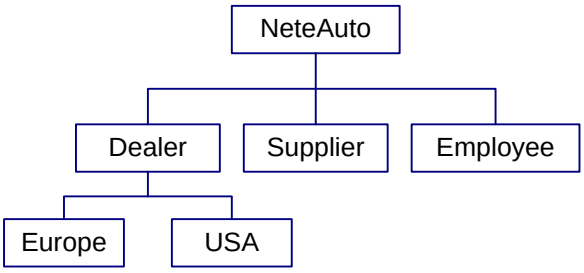
     Windows : <chemin_installation>\tools

     UNIX : <chemin_installation2>/tools
2. Dans le script SQL, recherchez et remplacez <@primary organization table@> par le nom de la table principale pour l'objet d'organisation. Enregistrez le script SQL.
3. Exécutez-le sur la base de données.

Spécification de l'organisation racine

L'organisation racine correspond à l'organisation de niveau supérieure ou à l'organisation parente dans l'annuaire. Toutes les organisations sont associées à l'organisation racine.

Dans l'illustration suivante, NeteAuto est l'organisation racine. Les autres organisations sont des sous-organisations de NeteAuto :



La définition de l'organisation racine complète ressemble à l'exemple suivant :

```
<ImsManagedObject name="Organization" description="My  Organizations"
objecttype="ORG">
   <RootOrg value="select orgid from tblOrganizations where parentorg is null">
      <Result name="%ORG_ID%" />
   </RootOrg>
```

Après avoir défini les informations de base pour l'objet d'organisation, y compris les tables qui constituent le profil d'organisation et l'identificateur unique de l'objet d'organisation, spécifiez l'organisation racine dans le fichier directory.xml :

- Dans le paramètre de valeur de l'élément RootOrg, définissez la requête utilisée par CA Identity Manager pour récupérer l'organisation racine, comme dans l'exemple suivant :

  ```
  <RootOrg value="select orgid from tblOrganizations where parentorg  is null">
  ```

- Dans le paramètre de nom de l'élément Result, saisissez l'identificateur unique de l'organisation, comme dans l'exemple suivant :

  ```
  <Result name="%ORG_ID%" />
  ```

  Remarque : La valeur du paramètre de nom doit être l'identificateur unique pour l'objet d'organisation.

Attributs connus pour les organisations

Définissez des attributs connus pour les attributs d'un profil d'organisation, comme décrit dans la section Attributs connus (page 79).

Les attributs connus requis et facultatifs pour les organisations sont les suivants :

%ORG_DESCR%

Description d'une organisation.

%ORG_MEMBERSHIP%

(Requis)

Contient l'organisation parente d'une organisation.

Remarque : Pour plus d'informations sur l'attribut %ORG_MEMBERSHIP%, consultez la rubrique Définition de la hiérarchie organisationnelle.

%ORG_MEMBERSHIP_NAME%

(Requis)

Contient le nom convivial de l'organisation parente (page 152) d'une organisation.

%ORG_NAME%

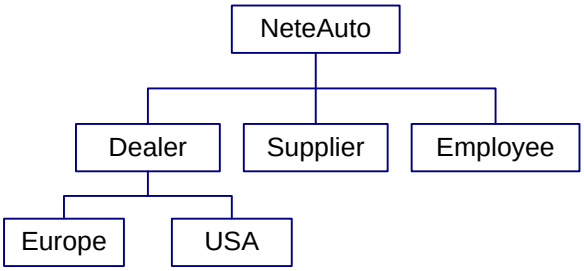
(Requis)

Contient le nom de l'organisation.

Définition de la hiérarchie organisationnelle

Dans CA Identity Manager, les organisations ont une structure hiérarchique qui inclut une organisation racine et des sous-organisations. Les sous-organisations peuvent également comprendre des sous-organisations.

Chaque organisation a une organisation parente, sauf l'organisation racine. Par exemple, dans l'illustration suivante, Dealer est l'organisation parente pour les organisations USA et Europe :



L'identificateur unique de l'organisation parente est stocké dans un attribut de profil d'une organisation. A l'aide des informations de cet attribut, CA Identity Manager peut générer la hiérarchie des organisations.

Pour spécifier l'attribut qui stocke l'organisation parente, utilisez les attributs connus %ORG_MEMBERSHIP% et %ORG_MEMBERSHIP_NAME% avec l'attribut physique stockant le nom de l'organisation parente dans une description d'attribut, comme suit :

```
<ImsManagedObjectAttr physicalname="tblOrganizations.parentorg"
displayname="Organization" description="Parent Organization" valuetype="Number"
required="false" multivalued="false" wellknown="%ORG_MEMBERSHIP%" maxlength="0"
/>
```

Amélioration des performances de recherche dans les annuaires

Pour améliorer les performances de recherches d'utilisateurs, d'organisations et de groupes dans les annuaires, effectuez les tâches suivantes :

- Indexez les attributs que les administrateurs peuvent spécifier dans des requêtes de recherche.
- Remplacez le délai d'expiration de l'annuaire par défaut en spécifiant des valeurs pour le délai d'expiration des recherches dans un fichier de configuration d'annuaire (directory.xml).
- Ajustez l'annuaire d'utilisateurs. Consultez la documentation de la base de données que vous utilisez.

Configurez les options spécifiques à votre base de données dans la source de données ODBC. Pour plus d'informations, consultez la documentation sur la source de données.

Amélioration des performances des recherches étendues

Lorsque CA Identity Manager gère un référentiel d'utilisateurs volumineux, les recherches qui renvoient un grand nombre de résultats peuvent monopoliser toutes les ressources mémoire du système.

Les deux paramètres suivants déterminent la modalité de gestion des recherches étendues :

- Nombre maximum de lignes

  Spécifie le nombre maximum de résultats renvoyés lors d'une recherche dans un annuaire d'utilisateurs. Lorsque le nombre de résultats dépasse la limite, une erreur s'affiche.

- Taille de la page

  Spécifie le nombre d'objets renvoyés pour une recherche unique. Si le nombre d'objets dépasse la taille de la page, plusieurs recherches sont effectuées.

  Remarque : Si le référentiel d'utilisateurs ne prend pas en charge la pagination et qu'une valeur pour maxrows est spécifiée, seule la valeur de maxrows est utilisée par CA Identity Manager pour contrôler la taille de la recherche.

Vous pouvez configurer le nombre maximum de lignes et la taille de la page dans les emplacements suivants :

- Référentiel d'utilisateurs

  Dans la plupart des référentiels d'utilisateurs et des bases de données, vous pouvez configurer des limites de recherche.

  Remarque : Pour plus d'informations, consultez la documentation du référentiel d'utilisateurs ou de la base de données que vous utilisez.

- Annuaire CA Identity Manager

  Vous pouvez configurer l'élément DirectorySearch (page 59) dans le fichier de configuration d'annuaire (directory.xml) que vous utilisez pour créer l'annuaire CA Identity Manager.

  Par défaut, la valeur maximale pour le nombre de lignes et la taille des pages est illimitée pour les répertoires existants. Pour les nouveaux répertoires, la valeur du nombre maximum de lignes est illimitée et la valeur maximale pour la taille de page est 2000.

- Définition d'un objet géré

  Pour définir le nombre maximum de lignes et la taille de page maximale qui s'appliquent à un seul type d'objet et non à un répertoire entier, configurez la *définition d'objet géré* (page 61) dans le fichier directory.xml que vous utilisez pour créer l'annuaire CA Identity Manager.

  La définition de limites pour un type d'objet géré vous permet de procéder à des ajustements en fonction des besoins métier. Par exemple, la plupart des sociétés ont plus d'utilisateurs que de groupes. Ces sociétés peuvent définir des limites pour les recherches d'objet d'utilisateur uniquement.

- Fenêtres de recherche de tâche

  Vous pouvez contrôler le nombre de résultats de recherche que les utilisateurs affichent dans les fenêtres de recherche et de liste dans la console d'utilisateur. Si le nombre de résultats dépasse le nombre de résultats par page défini pour la tâche, des liens vers les pages de résultats supplémentaires sont affichés.

  Cette configuration n'affecte pas le nombre de résultats renvoyés pour une recherche.

  Remarque : Pour plus d'informations sur la définition de la taille de page dans les fenêtres de recherche et de liste, consultez le *Manuel d'administration*.

Si les limites de nombre de lignes et les tailles de page maximales sont définies dans plusieurs endroits, le paramètre le plus spécifique s'applique. Par exemple, les paramètres d'objet géré ont priorité sur les paramètres de niveau annuaire.

Chapitre 5: Annuaires CA Identity Manager

Un annuaire CA Identity Manager fournit des informations sur l'annuaire d'utilisateurs géré par CA Identity Manager. Ces informations décrivent la méthode de stockage des objets, tels que les utilisateurs, les groupes et les organisations dans le référentiel d'utilisateurs et la modalité d'affichage dans CA Identity Manager.

Vous créez, affichez, exportez, mettez à jour et supprimez des annuaires CA Identity Manager dans la section CA Identity Manager directory (Annuaire) de la console de gestion.

Remarque : Si CA Identity Manager utilise un cluster de serveurs de stratégies SiteMinder, arrêtez-les tous sauf un avant de créer ou de mettre à jour les annuaires CA Identity Manager.

Ce chapitre traite des sujets suivants :

Conditions préalables à la création d'annuaire CA Identity Manager

Avant de créer un annuaire CA Identity Manager, effectuez les opérations suivantes.

- Arrêtez tous les noeuds CA Identity Manager sauf un avant de créer ou de modifier un annuaire CA Identity Manager.

  Remarque : Lorsque vous avez un cluster de noeuds CA Identity Manager, vous pouvez activer uniquement un noeud CA Identity Manager lorsque vous apportez des modifications dans la console de gestion.

- Arrêtez tous les serveurs de stratégie sauf un avant de créer ou de mettre à jour les annuaires CA Identity Manager.

  Remarque : Lorsque vous avez un cluster de serveurs de stratégies SiteMinder, vous pouvez activer uniquement un serveur de stratégies SiteMinder lorsque vous apportez des modifications dans la console de gestion.

Création d'un annuaire

Dans la console de gestion, vous créez un annuaire CA Identity Manager, qui décrit la structure et le contenu du référentiel d'utilisateurs, et l'annuaire de provisionnement, qui stocke les informations requises pour le serveur de provisionnement. Ces annuaires sont associés à l'environnement CA Identity Manager.

Pour créer des annuaires, utilisez l'une des deux méthodes suivantes :

- Utilisation de l'assistant de configuration d'annuaire

  Guide les administrateurs tout au long du processus de création d'un annuaire pour le référentiel d'utilisateurs. Cette méthode permet de minimiser les erreurs de configuration.

  Remarque : Utilisez l'Assistant de configuration d'annuaire pour créer des annuaires pour les référentiels d'utilisateurs LDAP uniquement. Pour créer un annuaire pour une base de données relationnelles ou pour mettre à jour un annuaire existant, importez un fichier directory.xml directement.

- Utilisation d'un fichier de configuration XML

  Permet aux administrateurs de sélectionner un fichier XML entièrement configuré afin de créer ou de modifier le référentiel d'utilisateurs ou le serveur de provisionnement.

  Sélectionnez cette méthode si vous créez un annuaire pour une base de données relationnelles ou si vous mettez à jour un annuaire existant.

Création d'un annuaire à l'aide de l'assistant de configuration d'annuaire

L'assistant de configuration d'annuaire oriente les administrateurs dans le processus de création d'un annuaire pour leur référentiel d'utilisateurs et les aide à limiter les erreurs de configuration. Avant de lancer l'assistant, chargez d'abord le modèle de configuration d'annuaire LDAP CA Identity Manager. Ces modèles sont préconfigurés et contiennent tous les attributs connus et nécessaires. Entrez les informations de connexion de votre référentiel d'utilisateurs LDAP ou de votre serveur de provisionnement. Vous pouvez ensuite sélectionner les attributs LDAP, mapper les attributs connus et saisir des métadonnées pour les attributs. Une fois le mappage des attributs effectué, cliquez sur Terminer pour créer l'annuaire.

Lancement de l'assistant de configuration d'annuaire

L'assistant de configuration d'annuaire permet à un administrateur de sélectionner un modèle CA Identity Manager et de le modifier pour l'utiliser dans votre environnement.

Procédez comme suit:

1. A partir de la console de gestion, cliquez sur Répertoires et sélectionnez Create from Wizard (Créer à partir de l'assistant).

   Vous êtes invité à sélectionner un fichier de configuration d'annuaire pour configurer le référentiel d'utilisateurs.

2. Cliquez sur Parcourir pour sélectionner le fichier de configuration pour configurer le référentiel d'utilisateurs ou le serveur de provisionnement à partir de l'emplacement par défaut suivant et cliquez sur Suivant.

   ```
   admin_tools\directoryTemplates\directory\
   ```

   Remarque : admin_tools spécifie le répertoire dans lequel les outils d'administration sont installés et directory spécifie le nom du fournisseur LDAP.

   Les outils d'administration sont situés aux emplacements par défaut ci-après.

   - Windows : <chemin_d'installation>\tools
   - UNIX : <chemin_installation2>/tools

3. Dans la fenêtre Détails de la connexion, spécifiez les informations de connexion pour l'annuaire LDAP ou le serveur de provisionnement, les paramètres de recherche d'annuaire et des informations de connexions de basculement, puis cliquez sur Suivant.

4. Dans la fenêtre Configure Managed Object (Configurer des objets gérés), spécifiez les objets à configurer et cliquez sur Suivant. Vous pouvez sélectionner les objets suivants :
   - Configure User Managed Object (Configuration d'objet utilisateur géré)
   - Configure Group Managed Object (Configuration d'objet groupe géré)
   - Configure Organization Object (Configuration d'objet organisation)
   - Show summary and deploy directory (Affichage de récapitulatif et déploiement d'annuaire)

     Remarque : Sélectionnez le récapitulatif et le déploiement d'annuaire uniquement si vous avez terminé la configuration de l'annuaire.

   a. Dans la fenêtre Sélectionner un attribut, affichez et modifiez les classes structurales et auxiliaires si nécessaire et cliquez sur Suivant.

   b. Dans la fenêtre Select Attributes: Mapping Well-Knowns (Sélectionner des attributs : mappage d'attributs connus), mappez les alias connus CA Identity Manager vers des attributs LDAP sélectionnés et cliquez sur Suivant.

   c. (Facultatif) Dans la fenêtre Describe User Attributes (Décrire des attributs utilisateur), affichez et modifiez les définitions d'attribut et cliquez sur Suivant. Vous pouvez modifier le nom d'affichage et la description.

   d. (Facultatif) Dans la fenêtre User Attribute Details (Détails des attributs utilisateur), définissez les métadonnées pour chaque attribut sélectionné à gérer et cliquez sur Suivant.

      La fenêtre Managed Object Selection (Sélection d'objets gérés) s'affiche.

      Pour configurer des groupes ou des organisations, sélectionnez l'objet géré et cliquez sur Suivant pour accéder aux fenêtres Attributs pour ces objets.

5. Dans la liste, sélectionnez Show summary and deploy directory (Affichage de récapitulatif et déploiement d'annuaire) et cliquez sur Suivant.

   La fenêtre Confirmation s'affiche.

6. Affichez les détails de l'annuaire.

   En cas d'erreurs, cliquez sur le bouton Précédent pour effectuer les modifications dans les fenêtres appropriées. Cliquez sur Terminer pour appliquer les modifications.

   CA Identity Manager valide la configuration et crée l'annuaire. Vous êtes ensuite redirigé dans la fenêtre de liste d'annuaires, dans laquelle vous pouvez afficher le nouvel annuaire.

Fenêtre Select Directory Template (Sélectionner un modèle d'annuaire)

Utilisez cette fenêtre pour sélectionner un fichier XML d'annuaire de sorte que LDAP configure un référentiel d'utilisateurs ou un serveur de provisionnement.

Cliquez sur Parcourir pour sélectionner le fichier de configuration pour configurer le référentiel d'utilisateurs ou le serveur de provisionnement à partir de l'emplacement par défaut suivant :

```
admin_tools\directoryTemplates\directory\
```

Remarque : admin_tools spécifie le répertoire dans lequel les outils d'administration sont installés et directory spécifie le nom du fournisseur LDAP.

Les outils d'administration sont situés aux emplacements par défaut ci-après.

- Windows : <chemin_d'installation>\tools
- UNIX : <chemin_installation2>/tools

Une fois le fichier XML d'annuaire sélectionné, cliquez sur Suivant pour passer à la fenêtre Détails de la connexion.

Fenêtre Détails de la connexion

Utilisez cette fenêtre pour saisir les informations d'identification de configuration de votre référentiel d'utilisateurs. Vous pouvez également entrer les paramètres de recherche d'annuaire et ajouter des connexions de basculement. Après avoir entré les informations de connexion, cliquez sur Suivant pour sélectionner les objets à gérer.

Remarque : Les champs qui s'affichent dans cette fenêtre dépendent du type de référentiel d'utilisateurs, ainsi que de l'utilisation de l'assistant de configuration d'annuaire ou de l'importation directe d'un fichier XML pour la création de la connexion.

Les champs suivants apparaissent dans cette fenêtre :

Nom

Spécifie le nom de l'annuaire d'utilisateurs auquel vous vous connectez.

Description

Spécifie une description de l'annuaire d'utilisateurs.

Hôte

Spécifie le nom d'hôte de l'ordinateur sur lequel le référentiel d'utilisateurs est installé.

Port

Spécifie le port de l'ordinateur sur lequel le référentiel d'utilisateurs est installé.

Nom relatif de l'utilisateur

Spécifie le nom de domaine de l'utilisateur pour l'accès au référentiel d'utilisateurs LDAP.

JDBC Data Source JNDI Name (Nom JNDI de la source de données JDBC)

Spécifie le nom d'une source de données JDBC existante utilisée par CA Identity Manager pour la connexion à la base de données.

Nom d'utilisateur

Spécifie le nom d'utilisateur pour l'accès au serveur de provisionnement.

Remarque : S'applique uniquement aux serveurs de provisionnement.

Domaine

Spécifie le nom du domaine pour l'accès au serveur de provisionnement.

Remarque : S'applique uniquement aux serveurs de provisionnement.

Mot de passe

Spécifie le mot de passe pour l'accès au référentiel d'utilisateurs LDAP/serveur de provisionnement.

Confirmer le mot de passe

Confirme le mot de passe pour l'accès au référentiel d'utilisateurs LDAP/serveur de provisionnement.

Connexion sécurisée

Si cette option est sélectionnée, elle force la connexion SSL (Secure Sockets Layer) à l'annuaire d'utilisateurs LDAP.

Rechercher la racine

Spécifie l'emplacement qui sert de point de départ pour l'annuaire LDAP ; en général, une organisation (o) ou une unité organisationnelle (ou).

Remarque : S'applique aux référentiels d'utilisateurs LDAP uniquement.

Search Maximum Rows (Nombre maximum de lignes de la recherche)

Spécifie le nombre maximum de résultats que CA Identity Manager peut renvoyer lors de la recherche d'un annuaire d'utilisateurs. Lorsque le nombre de résultats dépasse la limite, une erreur s'affiche.

Si vous définissez un nombre maximum de lignes, ce paramètre peut remplacer les paramètres de l'annuaire LDAP qui limitent les résultats de la recherche. Lorsque des paramètres contradictoires sont appliqués, le serveur LDAP utilise le paramètre dont la valeur est la plus faible.

Search Page Size (Taille de la page de recherche)

Spécifie le nombre d'objets renvoyés pour une recherche unique. Si le nombre d'objets dépasse la taille de la page, CA Identity Manager effectue plusieurs recherches.

Lors de la spécification de la taille de la page de recherche, tenez compte des points suivants :

- Pour utiliser l'option Search Page Size (Taille de la page de recherche), le référentiel d'utilisateurs géré par CA Identity Manager doit prendre en charge la pagination. Certains types de référentiel d'utilisateurs requièrent une configuration supplémentaire pour prendre en charge la pagination. Pour plus d'informations, consultez le *Manuel de configuration*.
- Si le référentiel d'utilisateurs ne prend pas en charge la pagination et qu'une valeur pour le nombre maximum de lignes de recherche est spécifiée, CA Identity Manager utilisera uniquement cette valeur pour contrôler la taille de la recherche.

Search Timeout (Délai d'expiration de la recherche)

Spécifie la durée maximum en secondes de la recherche d'un annuaire effectuée par CA Identity Manager avant de prendre fin.

Failover Host (Hôte de basculement)

Spécifie le nom d'hôte du système dans lequel un référentiel d'utilisateurs redondant ou un autre serveur de provisionnement existe, dans le cas où le système principal serait indisponible. Si plusieurs serveurs sont répertoriés, CA Identity Manager tentera de se connecter aux systèmes dans l'ordre indiqué.

Failover Port (Port de basculement)

Spécifie le port du système dans lequel un référentiel d'utilisateurs redondant ou un autre serveur de provisionnement existe, dans le cas où le système principal serait indisponible. Si plusieurs serveurs sont répertoriés, CA Identity Manager tentera de se connecter aux systèmes dans l'ordre indiqué.

Bouton Ajouter

Pour ajouter un nom d'hôte de basculement et des numéros de port supplémentaires, cliquez sur ce bouton.

Fenêtre Configure Managed Objects (Configurer les objets gérés)

Utilisez cette fenêtre pour sélectionner un objet à configurer.

La liste suivante décrit les champs de cette fenêtre :

Configure User Managed Object (Configuration d'objet utilisateur géré)

Décrit la méthode de stockage des utilisateurs dans le référentiel d'utilisateurs et leur représentation dans CA Identity Manager.

Configure Group Managed Object (Configuration d'objet groupe géré)

Décrit la méthode de stockage des groupes dans le référentiel d'utilisateurs et leur représentation dans CA Identity Manager.

Configure Organization Managed Object (Configuration d'objet organisation géré)

Si le référentiel d'utilisateurs inclut des organisations, ce champ décrit la méthode de stockage de ces organisations et leur représentation dans CA Identity Manager.

Show summary and deploy directory (Affichage de récapitulatif et déploiement d'annuaire)

Spécifie que tous les objets gérés ont été définis et indique si vous voulez déployer l'annuaire. Après avoir sélectionné Show summary and deploy directory (Affichage de récapitulatif et déploiement d'annuaire), cliquez sur Suivant et vous serez dirigé vers une page récapitulative.

Bouton Enregistrer

Pour enregistrer votre fichier XML, cliquez sur ce bouton.

Bouton Précédent

Pour revenir à la fenêtre Détails de la connexion et apporter des modifications, cliquez sur ce bouton.

Bouton Suivant

Pour passer à la fenêtre Select Attributes (Sélectionner des attributs) et y sélectionner les attributs utilisateur, groupe, ou organisation à configurer, cliquez sur ce bouton.

Fenêtre Select Attributes (Sélectionner des attributs)

Utilisez cette fenêtre pour modifier ou ajouter des classes structurales et auxiliaires pour vos objets utilisateur, groupe, ou organisation. Cette fenêtre est préconfigurée à l'aide de valeurs basées sur des schémas d'annuaire communs et des meilleures pratiques pour le type d'annuaire que vous utilisez. Un administrateur peut changer la classe structurale en sélectionnant une nouvelle classe dans le menu déroulant. Cette sélection met à jour la table avec des attributs appartenant à la nouvelle classe structurale.

Vous pouvez ajouter une classe auxiliaire en la sélectionnant dans le menu déroulant. Cette sélection met à jour la table avec des attributs appartenant à la nouvelle classe auxiliaire.

La liste suivante décrit les champs de cette fenêtre :

Structural Class Name (Nom de la classe structurale)

Spécifie la classe structurale de l'attribut à configurer.

Bouton Modifier

Pour modifier la classe structurale, cliquez sur ce bouton.

Auxiliary Class Name (Nom de la classe auxiliaire)

Spécifie la classe auxiliaire de l'attribut à configurer.

Bouton Ajouter

Pour ajouter une classe auxiliaire à configurer, cliquez sur ce bouton.

Classe d'objet

Spécifie la classe d'objet de conteneur.

ID

Spécifie l'ID du conteneur.

Nom

Spécifie le nom du conteneur.

Attributes Table (Table d'attributs)

Indique le nom physique, la classe d'objets, s'il s'agit d'attributs à valeurs multiples et le type de données des attributs sélectionnés. Vous pouvez trier les attributs dans cette table par les colonnes Sélectionné, Classe d'objets, Valeurs multiples et Type de données.

Bouton Précédent

Pour revenir à la fenêtre Configure Managed Objects (Configurer les objets gérés), cliquez sur ce bouton.

Suivant

Pour passer à la fenêtre Well-Known Mapping (Mappage d'attributs connus) et mapper les alias connus requis et facultatifs, cliquez sur ce bouton.

Fenêtre Well-Known Mapping (Mappage d'attributs connus)

Utilisez cette fenêtre pour mapper des attributs connus CA Identity Manager vers des attributs LDAP sélectionnés. Un administrateur peut ajouter des attributs à la liste d'attributs connus (s'ils sont requis pour le code personnalisé) en les introduisant dans le champ de texte et en cliquant sur le bouton Ajouter. La fenêtre s'actualise de sorte à ce que vous puissiez continuer d'ajouter autant d'attributs connus que nécessaire.

La liste suivante décrit les champs de cette fenêtre :

Required Well-Knowns (Attributs connus requis)

Spécifie les attributs connus pour les utilisateurs, groupes, ou organisations (le cas échéant) et requis pour le mappage vers des attributs LDAP.

Optional Well-Knowns (Attributs connus facultatifs)

Spécifie les attributs connus pour les utilisateurs, groupes, ou organisations (le cas échéant) que vous pouvez également mapper.

Nouvelle Well-Known

Spécifie un attribut connu tel que référencé par le code personnalisé.

Bouton Ajouter

Pour ajouter un nouvel attribut connu à la table d'attributs connus facultatifs, cliquez sur ce bouton.

Bouton Précédent

Pour revenir à la fenêtre Sélectionner un attribut et y sélectionner d'autres attributs, cliquez sur ce bouton. Les mappages déjà réalisés sont enregistrés et disponibles lorsque vous revenez à cette fenêtre.

Bouton Suivant

Pour passer à la fenêtre Basic Object Attribute Definition (Définition de l'attribut d'objet de base) et spécifier des définitions d'attribut de base, cliquez sur ce bouton.

Fenêtre Basic Object Attribute Definition (Définition de l'attribut d'objet de base)

Pour afficher et modifier les définitions communément définies : nom d'affichage et description, utilisez cette fenêtre.

La liste suivante décrit les champs de cette fenêtre :

Managed Object Table (Table de l'objet géré)

Spécifie le nom d'affichage, le nom physique, le nom connu et la description de l'objet géré. Pour changer la description, utilisez le menu déroulant. Après avoir apporté vos modifications, cliquez sur Suivant pour continuer.

Bouton Précédent

Pour revenir à la fenêtre Well-Known Mapping (Mappage d'attributs connus) et modifier les détails des mappages, cliquez sur ce bouton.

Bouton Suivant

Pour passer à la fenêtre Detailed Object Attribute Definition (Définition de l'attribut d'objet détaillée) dans laquelle vous pouvez spécifier des définitions d'attribut supplémentaires, cliquez sur ce bouton.

Fenêtre Detailed Object Attribute Definition (Définition de l'attribut d'objet détaillée)

Utilisez cette fenêtre pour spécifier d'autres définitions d'attribut. Pour définir les métadonnées de chaque attribut sélectionné, un administrateur peut modifier le nom d'affichage, gérer l'attribut dans les fenêtres de la console d'utilisateur, le type de données de la valeur, la longueur maximum et l'ensemble de règles de validation. Une fois les définitions d'attribut spécifiées, cliquez sur Suivant pour continuer.

Les champs qu'elle contient sont répertoriés ci-dessous.

Display Name (Nom d'affichage)

Spécifie le nom unique de l'attribut d'objet géré. Il s'agit du nom affiché dans la console d'utilisateur.

Tags (Balises)

Spécifie les balises de la classification des données pour la valeur de l'attribut d'objet géré. Toutes les balises sont facultatives et définies par défaut sur False, excepté Searchable (Peut être recherché). Vous pouvez sélectionner les balises suivantes :

Required (Requis)

Indique que l'attribut est obligatoire lors de la création d'objets.

Multiple Values (Valeurs multiples)

Indique que l'attribut apparaît comme attribut à valeurs multiples.

Masqué

Indique que l'attribut est masqué.

Système

Indique qu'il s'agit d'un attribut système et qu'il n'est pas ajouté aux fenêtres de tâche.

Searchable (Peut être recherché)

Indique que l'attribut est ajouté à des filtres de recherche. Par défaut, cette balise est définie sur True.

Sensitive Encrypt (Sensible et chiffré)

Indique que l'attribut est sensible et affiché sous forme d'une série d'astérisques (*).

Hide in VST (Masquer dans la fenêtre Afficher les tâches soumises)

Indique que l'attribut est masqué dans la fenêtre Détails de l'événement pour l'affichage des tâches soumises.

Do not copy (Ne pas copier)

Indique que l'attribut doit être ignoré lorsqu'un administrateur crée une copie d'objet.

Previously encrypted (Préalablement chiffré)

Indique que l'attribut faisant l'objet de l'accès dans le référentiel d'utilisateurs a préalablement été chiffré et requiert un déchiffrement. La valeur du texte clair est enregistrée dans le référentiel d'utilisateurs lors de l'enregistrement de l'objet.

Untagged encrypted (Sans balise et chiffré)

Indique que l'attribut a préalablement été chiffré dans le référentiel d'utilisateurs et ne contient pas le nom de la balise d'algorithme de chiffrement au début du texte chiffré.

Type de données

Spécifie le type de données de la valeur de l'attribut d'objet géré dans la console d'utilisateur. Vous pouvez effectuer une sélection dans la liste suivante :

- READONLY (lecture seule)
- WRITEONCE (écriture unique)
- READWRITE (lecture et écriture)

Longueur maximale

Spécifie la longueur maximale de la valeur pour l'attribut d'objet géré.

Valeur par défaut : 0

Validation Rule Set (Ensemble de règles de validation)

Spécifie l'ensemble de règles de validation pour valider la valeur de l'attribut d'objet géré. Vous pouvez effectuer une sélection dans la liste suivante :

- User Validation (Validation d'utilisateur)
- Phone Format (Format de numéro de téléphone)
- International Phone Format (Format de numéro de téléphone international)

Bouton Précédent

Pour revenir à la fenêtre Basic Object Attribute Definition Définition de l'attribut d'objet de base) pour apporter des modifications, cliquez sur ce bouton.

Bouton Suivant

Pour passer à la fenêtre Configure Managed Objects (Configurer les objets gérés), cliquez sur ce bouton. Cette fenêtre permet de sélectionner l'objet géré suivant à configurer. Une fois vos objets gérés configurés, sélectionnez l'option Show summary and deploy directory (Afficher le récapitulatif et déployer l'annuaire) pour afficher les informations de l'annuaire et déployer celui-ci.

Informations complémentaires :

Gestion des attributs sensibles (page 71)

Fenêtre Confirmation

Cette fenêtre contient un récapitulatif des détails de l'annuaire.

La liste suivante décrit les champs de cette fenêtre :

Détails de la connexion

Spécifie les détails de la connexion pour l'annuaire d'utilisateurs.

User/Group/Organization Details (Détails des utilisateurs/groupes/organisations)

Spécifie les modifications apportées à directory.xml.

Bouton Précédent

Pour modifier des détails dans l'assistant, cliquez sur ce bouton.

Bouton Enregistrer

Pour enregistrer vos sélections, cliquez sur ce bouton.

Bouton Terminer

Si tous les détails de l'annuaire sont corrects, cliquez sur ce bouton pour fermer l'assistant.

La configuration est validée et l'annuaire est créé. Vous êtes alors redirigé vers la page de liste des annuaires, dans laquelle le nouvel annuaire apparaît. Pour modifier ou exporter le nouvel annuaire, sélectionnez-le dans la liste des annuaires.

Création d'un annuaire avec un fichier de configuration XML

Vous pouvez créer ou mettre à jour un annuaire CA Identity Manager en important un fichier directory.xml rempli dans la console de gestion.

Remarque : Si vous créez un annuaire à l'aide d'un fichier directory.xml au lieu d'utiliser l'assistant de configuration d'annuaire, vérifiez que vous avez modifié le modèle de configuration par défaut. Pour plus d'informations, consultez le *Manuel de configuration*.

Procédez comme suit:

1. Pour ouvrir la console de gestion, saisissez l'URL suivante dans un navigateur :

   http://*nom_hôte*:*port*/iam/immanage

   hostname

   Définit le nom de domaine complet du serveur sur lequel CA Identity Manager est installé.

   port

   Définit le numéro de port du serveur d'applications.

2. Cliquez sur Directories (Annuaires).

   La fenêtre Directories (Annuaires) de CA Identity Manager s'affiche.

3. Cliquez sur Create or Update from XML (Créer ou mettre à jour à partir du fichier XML).

4. Saisissez le chemin d'accès et le nom du fichier XML de configuration d'annuaire pour créer l'annuaire CA Identity Manager ou accédez au fichier. Cliquez sur Suivant.

5. Spécifiez des valeurs pour les champs de cette fenêtre, comme suit :

   Remarque : Les champs qui s'affichent dans cette fenêtre dépendent du type de référentiel d'utilisateurs et des informations que vous avez fournies dans le fichier de configuration d'annuaire à l'étape 4. Si vous avez spécifié des valeurs dans l'un de ces champs dans le fichier de configuration d'annuaire, CA Identity Manager ne vous invite pas à respécifier ces valeurs.

   Nom

   Nom de l'annuaire CA Identity Manager que vous créez.

   Description

   (Facultatif) Description de l'annuaire CA Identity Manager.

   Connection Object Name (Nom d'objet de connexion)

   Spécifie le nom de l'annuaire d'utilisateurs que l'annuaire CA Identity Manager décrit. Entrez l'*une* des valeurs suivantes :

   - Si CA Identity Manager n'est pas intégré à SiteMinder, spécifiez un nom significatif pour l'objet utilisé par CA Identity Manager pour la connexion au référentiel d'utilisateurs.
   - Si CA Identity Manager est intégré à SiteMinder et que vous voulez créer un objet de connexion d'annuaire d'utilisateurs dans SiteMinder, spécifiez un nom significatif. CA Identity Manager crée l'objet de connexion d'annuaire d'utilisateurs dans SiteMinder avec le nom que vous spécifiez.
   - Si CA Identity Manager est intégré à SiteMinder et que vous voulez vous connecter à un annuaire d'utilisateurs SiteMinder existant, spécifiez le nom de l'objet de connexion d'annuaire d'utilisateurs SiteMinder tel qu'il s'affiche dans l'interface utilisateur du serveur de stratégies.

JDBC Data Source JNDI Name (Nom JNDI de source de données JDBC - annuaires relationnels uniquement)

Spécifie le nom d'une source de données JDBC existante utilisée par CA Identity Manager pour la connexion à la base de données.

Hôte (annuaires LDAP uniquement)

Indique le nom d'hôte ou l'adresse IP du système sur lequel l'annuaire d'utilisateurs est installé.

Pour les référentiels d'utilisateurs CA Directory, utilisez le nom de domaine complet du système hôte. N'utilisez pas localhost.

Pour les référentiels d'utilisateurs Active Directory, spécifiez le nom de domaine, pas l'adresse IP.

Port (annuaires LDAP uniquement)

Indique le numéro de port de l'annuaire d'utilisateurs.

Provisioning Domain (Domaine de provisionnement)

Domaine de provisionnement géré par CA Identity Manager.

Remarque : Le nom du domaine doit respecter la casse.

Nom d'utilisateur/DN d'utilisateur

Spécifie le nom d'utilisateur pour un compte qui peut accéder au référentiel d'utilisateurs.

Pour les référentiels d'utilisateurs de provisionnement, le compte d'utilisateur que vous spécifiez doit avoir un profil d'administrateur de domaines ou un ensemble de droits équivalents sur le domaine de provisionnement.

Mot de passe

Spécifie le mot de passe pour le compte d'utilisateur que vous avez spécifié dans le champ Nom d'utilisateur (bases de données relationnelles) ou Nom unique de l'utilisateur (annuaires LDAP).

Confirmer le mot de passe

Confirmez le mot de passe saisi dans le champ Mot de passe.

Connexion sécurisée (annuaires LDAP uniquement)

Indique si CA Identity Manager utilise une connexion sécurisée.

Assurez-vous de sélectionner cette option pour les référentiels d'utilisateurs Active Directory.

Cliquez sur Suivant.

6. Vérifiez les paramètres de l'annuaire CA Identity Manager. Cliquez sur Terminer pour créer l'annuaire CA Identity Manager avec les paramètres actuels ou sur Précédent pour les modifier.

   Des informations sur le statut sont affichées dans la fenêtre Directory Configuration Output (Résultat de la configuration d'annuaire).

7. Cliquez sur Continuer pour sortir.

   CA Identity Manager crée l'annuaire.

Activation de l'accès au serveur de provisionnement

Vous activez l'accès au serveur de provisionnement à l'aide du lien Directories (Annuaires) dans la console de gestion.

Remarque : Une condition préalable à cette procédure est l'installation de l'annuaire de provisionnement sur CA Directory. Pour plus d'informations, reportez-vous au *Manuel d'installation*.

Procédez comme suit:

1. Pour ouvrir la console de gestion, saisissez l'URL suivante dans un navigateur :

   `http://nom_hôte:port/iam/immanage`

   hostname

   Définit le nom d'hôte complet du système sur lequel le serveur CA Identity Manager est installé.

   port

   Définit le numéro de port du serveur d'applications.

2. Cliquez sur Directories (Annuaires).

   La fenêtre Directories (Annuaires) de CA Identity Manager s'affiche.

3. Cliquez sur Create from Wizard (Créer à partir de l'assistant).

4. Saisissez le chemin d'accès et le nom du fichier XML de l'annuaire pour configurer l'annuaire de provisionnement. Il est stocké sous directoryTemplates\ProvisioningServer dans le dossier Outils d'administration. L'emplacement par défaut de ce dossier est :

   - Windows : <chemin_d'installation>\tools
   - UNIX : <chemin_installation2>/tools

   Remarque : Vous pouvez utiliser ce fichier de configuration d'annuaire tel quel, sans avoir à y apporter de modification.

5. Cliquez sur Suivant.

6. Spécifiez des valeurs pour les champs de cette fenêtre, comme suit :

Nom

Nom de l'annuaire de provisionnement associé au serveur de provisionnement que vous configurez.

- Si CA Identity Manager n'est pas intégré à SiteMinder, spécifiez un nom significatif pour l'objet utilisé par CA Identity Manager pour la connexion à l'annuaire d'utilisateurs.
- Si CA Identity Manager est intégré à SiteMinder, vous avez deux possibilités :

  Si vous voulez créer un objet de connexion d'annuaire d'utilisateurs dans SiteMinder, spécifiez un nom significatif. CA Identity Manager crée cet objet dans SiteMinder avec ce nom.

  Si vous voulez vous connecter à un annuaire d'utilisateurs SiteMinder existant, spécifiez le nom de l'objet de connexion d'annuaire d'utilisateurs SiteMinder tel qu'il s'affiche dans l'interface utilisateur du serveur de stratégies.

Description

(Facultatif) Description de l'annuaire CA Identity Manager.

Hôte

Indique le nom d'hôte ou l'adresse IP du système sur lequel l'annuaire d'utilisateurs est installé.

Port

Indique le numéro de port de l'annuaire d'utilisateurs.

Domaine

Nom du domaine de provisionnement géré par CA Identity Manager.

Important : Lors de la création d'un annuaire de provisionnement via la console de gestion, n'utilisez aucun caractère de langue étrangère pour le nom du domaine, car autrement, sa création échouera.

Le nom doit correspondre au nom du domaine de provisionnement que vous avez spécifié pendant l'installation.

Remarque : Le nom du domaine est sensible à la casse.

Nom d'utilisateur

Spécifie un utilisateur qui peut se connecter au gestionnaire de provisionnement.

L'utilisateur doit avoir un profil d'administrateur de domaines ou un ensemble équivalent de droits sur le domaine de provisionnement.

Mot de passe

Spécifie le mot de passe pour l'utilisateur global que vous avez saisi dans le champ Nom d'utilisateur.

Confirmer le mot de passe

Confirmez le mot de passe saisi dans le champ Mot de passe.

Connexion sécurisée

Indique si CA Identity Manager utilise une connexion sécurisée.

Assurez-vous de sélectionner cette option pour les référentiels d'utilisateurs Active Directory.

Directory Search Parameters (Paramètres de recherche d'annuaire)

maxrows spécifie le nombre maximum de résultats renvoyés lors d'une recherche dans un annuaire d'utilisateurs. Cette valeur remplace les limites définies dans l'annuaire LDAP. Lorsque des paramètres contradictoires sont appliqués, le serveur LDAP utilise le paramètre dont la valeur est la plus faible.

Remarque : Le paramètre maxrows ne limite pas le nombre de résultats qui sont affichés dans la fenêtre de tâche de CA Identity Manager. Pour configurer les paramètres d'affichage, modifiez la définition de la fenêtre de liste dans la console d'utilisateur CA Identity Manager. Pour obtenir des instructions, consultez le *Manuel de conception de la console d'utilisateur*.

timeout détermine le nombre maximum de secondes que tarde la recherche dans un annuaire avant de se terminer.

Failover Connections (Connexions de basculement)

Nom d'hôte et numéro de port d'un ou de plusieurs systèmes facultatifs qui sont des serveurs de provisionnement secondaires. Si vous spécifiez plusieurs serveurs, CA Identity Manager tente de se connecter aux systèmes répertoriés.

Les serveurs de provisionnement secondaires sont utilisés si un échec du serveur de provisionnement principal se produit. Lorsque le serveur de provisionnement principal redevient disponible, l'utilisation du serveur de provisionnement secondaire se poursuit. Si vous voulez utiliser le serveur de provisionnement principal à nouveau, redémarrez les serveurs de provisionnement secondaires.

7. Cliquez sur Suivant.
8. Sélectionnez les objets à gérer, comme les utilisateurs ou les groupes.
9. Après avoir configuré les objets de manière appropriée, affichez le récapitulatif, déployez l'annuaire de provisionnement et vérifiez ses paramètres.
10. Cliquez sur l'une de ces actions :
    a. Pour effectuer une modification, cliquez sur Précédent.
    b. Cliquez sur Enregistrer pour enregistrer les informations de l'annuaire si vous voulez revenir et effectuer le déploiement plus tard.
    c. Cliquez sur Terminer pour terminer la procédure et commencer la configuration d'un environnement à l'aide du provisionnement (page 197).

Affichage d'un annuaire CA Identity Manager

Effectuez la procédure suivante pour afficher un annuaire CA Identity Manager.

Procédez comme suit:

1. Dans la console de gestion CA Identity Manager, cliquez sur Directories (Annuaires).
2. Cliquez sur le nom de l'annuaire CA Identity Manager à afficher. La fenêtre Directory Properties (Propriétés de l'annuaire) s'affiche avec les propriétés de l'annuaire CA Identity Manager.

Propriétés de l'annuaire CA Identity Manager

Les propriétés de l'annuaire CA Identity Manager sont les suivantes :

Remarque : Les propriétés qui sont affichées dépendent du type de base de données ou d'annuaire associé à l'annuaire CA Identity Manager.

Nom

Définit le nom unique de l'annuaire CA Identity Manager.

Description

Affiche la description de l'annuaire CA Identity Manager.

Type

Définit le type de fournisseur d'annuaire.

Connection Object Name (Nom d'objet de connexion)

Affiche le nom de l'annuaire d'utilisateurs que l'annuaire CA Identity Manager décrit.

Si CA Identity Manager est intégré à SiteMinder, le nom d'objet de connexion correspond au nom de la connexion d'annuaire d'utilisateurs SiteMinder.

Root Organization (Organisation racine - référentiels d'utilisateurs incluant des organisations)

Spécifie le point d'entrée dans le référentiel d'utilisateurs.

Pour les annuaires LDAP, l'organisation racine est spécifiée en tant que nom unique. Pour les bases de données relationnelles, l'identificateur unique de l'organisation racine est affiché.

JDBC Data Source (Source de données JDBC)

Spécifie le nom de la source de données JDBC utilisée par CA Identity Manager pour la connexion à la base de données.

URL

URL ou adresse IP du référentiel d'utilisateurs.

Nom d'utilisateur

Spécifie le nom d'utilisateur pour un compte qui peut accéder au référentiel d'utilisateurs.

Search Maximum Rows (Nombre maximum de lignes)

Indique le nombre maximum de lignes renvoyées dans les résultats d'une recherche.

Search Page Size (Taille de la page de recherche)

Spécifie le nombre d'objets renvoyés pour une recherche unique. Si le nombre d'objets dépasse la taille de la page, plusieurs recherches sont effectuées.

Remarque : Le référentiel d'utilisateurs géré par CA Identity Manager doit prendre en charge la pagination. Certains types de référentiel d'utilisateurs requièrent une configuration supplémentaire pour prendre en charge la pagination. Pour plus d'informations, consultez le *Manuel de configuration*.

Supports Paging (Prise en charge de la pagination)

Indique que l'annuaire prend en charge la pagination.

Search Timeout (Délai d'expiration de la recherche - annuaires LDAP uniquement)

Spécifie le nombre maximum de secondes que tarde la recherche dans un référentiel d'utilisateurs avant de se terminer.

Provisioning Domain (Domaine de provisionnement - annuaires de serveur de provisionnement uniquement)

Domaine de provisionnement géré par CA Identity Manager.

Fenêtre Directory Properties (Propriétés de l'annuaire) de CA Identity Manager

Les informations générales d'un annuaire CA Identity Manager sont présentées dans la fenêtre de propriétés pour l'annuaire que vous sélectionnez. La fenêtre Directory Properties (Propriétés de l'annuaire) est divisée selon les sections suivantes :

Directory Properties (Propriétés de l'annuaire)

Affiche les propriétés de base sur l'annuaire CA Identity Manager, notamment le domaine de provisionnement associé, si le provisionnement est activé pour l'environnement.

Managed Objects (Objets gérés) (page 179)

Descriptions du type d'objets de référentiel d'utilisateurs géré par CA Identity Manager.

Validation Rule Sets (Ensembles de règles de validation) (page 184)

Répertorie les ensembles de règles de validation qui s'appliquent à l'annuaire CA Identity Manager.

Environments (Environnements)

Répertorie les environnements associés à l'annuaire CA Identity Manager. Vous pouvez associer un annuaire à plusieurs environnements CA Identity Manager.

Pour afficher plus d'informations sur un environnement CA Identity Manager, cliquez sur son nom.

Pour modifier les propriétés d'un annuaire CA Identity Manager, importez un fichier de configuration d'annuaire selon la procédure décrite dans la section Mise à jour d'un annuaire CA Identity Manager (page 186).

Outre l'affichage des propriétés, vous pouvez également effectuer les opérations suivantes :

Mise à jour de l'authentification

Permet aux administrateurs de modifier l'annuaire utilisé par CA Identity Manager pour authentifier les administrateurs de la console de gestion. Les administrateurs peuvent également ajouter des administrateurs de console de gestion supplémentaires dans l'annuaire d'authentification existant.

Remarque : Les options de mise à jour d'authentification s'appliquent uniquement lorsque la sécurité CA Identity Manager native protège la console de gestion. Pour plus d'informations sur l'activation de la sécurité native ou l'utilisation d'une méthode de sécurité différente, consultez le *Manuel de configuration*.

Exporter (page 186)

Exporte la définition d'annuaire dans un fichier XML. Après avoir exporté les paramètres d'annuaire, vous pouvez modifier le fichier XML, puis le réimporter pour mettre à jour l'annuaire. Vous pouvez également importer le fichier XML dans un autre annuaire pour définir les mêmes paramètres pour celui-ci.

Mise à jour (page 186)

Permet aux administrateurs d'ajouter ou de modifier les définitions d'objet gérés, tels que les attributs d'un objet, de définir les paramètres de recherche et de modifier les propriétés d'annuaire.

Affichage des attributs et des propriétés d'objet géré

Un objet géré décrit un type d'entrée dans le référentiel d'utilisateurs, comme un utilisateur, un groupe ou une organisation. Les propriétés et les attributs qui s'appliquent à un objet géré s'appliquent à toutes les entrées de ce type. Par exemple, un profil d'utilisateur est constitué de toutes les propriétés et de tous les attributs de l'objet géré Utilisateur.

Pour afficher les détails d'un objet géré, cliquez sur son nom pour ouvrir la fenêtre Managed Object Properties (Propriétés de l'objet géré).

Propriétés des objets gérés

La fenêtre Managed Object Properties (Propriétés d'objet géré) décrit les propriétés et les attributs pour un type d'objet géré.

Les informations concernant cette fenêtre dépendent du type de référentiel d'utilisateurs que vous gérez. Les propriétés d'un objet géré sont les suivantes :

Description

Description de l'objet géré.

Type

Indique le type d'entrée que l'objet géré représente. Il peut s'agir de l'un des types suivants :

- Utilisateur
- Groupe
- Organisation

Classe d'objets (annuaires LDAP uniquement)

Spécifie les classes d'objets pour l'objet géré. Un objet géré peut avoir plusieurs classes d'objets.

Sort Order (Ordre de tri - annuaires LDAP uniquement)

Spécifie l'attribut utilisé par CA Identity Manager pour trier les résultats de la recherche selon la logique métier personnalisée. L'ordre de tri n'affecte pas l'ordre de résultats de la recherche dans la console d'utilisateur.

Par exemple, lorsque vous spécifiez l'attribut cn pour l'objet d'utilisateur, CA Identity Manager trie les résultats d'une recherche d'utilisateurs alphabétiquement selon l'attribut cn.

Primary Table (Table principale - bases de données relationnelles uniquement)

Spécifie la table qui contient l'identificateur unique pour l'objet géré.

Nombre maximum de lignes

Spécifie le nombre maximum de résultats que CA Identity Manager peut renvoyer pour une recherche d'objet de ce type. Lorsque le nombre de résultats dépasse la limite, une erreur s'affiche.

Si vous définissez un nombre maximum de lignes, ce paramètre peut remplacer les paramètres de l'annuaire LDAP qui limitent les résultats de la recherche. Lorsque des paramètres contradictoires sont appliqués, le serveur LDAP utilise le paramètre dont la valeur est la plus faible.

Taille de la page

Spécifie le nombre d'objets renvoyés pour une recherche unique. Si le nombre d'objets dépasse la taille de la page, plusieurs recherches sont effectuées.

Remarque : Le référentiel d'utilisateurs géré par CA Identity Manager doit prendre en charge la pagination. Certains types de référentiel d'utilisateurs requièrent une configuration supplémentaire pour prendre en charge la pagination. Pour plus d'informations, consultez le *Manuel de configuration*.

Propriétés de conteneur (annuaires LDAP uniquement)

Dans un annuaire LDAP, les groupes de *conteneur* contiennent des objets d'un certain type. Lorsqu'un conteneur est spécifié, CA Identity Manager gère uniquement les entrées de ce conteneur. Par exemple, lorsque vous spécifiez le conteneur ou=People, CA Identity Manager gère les utilisateurs existant dans le conteneur People uniquement.

Remarque : Les utilisateurs et les groupes qui existent dans l'annuaire LDAP sans être inclus dans le conteneur défini peuvent s'afficher dans la console d'utilisateur. Des problèmes peuvent survenir lorsque vous gérez ces utilisateurs et ces groupes.

Les conteneurs regroupent des utilisateurs et des groupes uniquement. Vous ne pouvez pas spécifier un conteneur pour les organisations.

Les propriétés d'un conteneur sont les suivantes :

objectclass

Spécifie la classe d'objet LDAP du conteneur dans lequel les objets d'un certain type sont créés. Par exemple, la valeur par défaut pour le conteneur d'utilisateurs est top,organizationalUnit, ce qui indique que les utilisateurs sont créés dans des unités organisationnelles LDAP (ou).

ID

Spécifie l'attribut qui référence le nom de conteneur, par exemple, ou. L'attribut est associé avec la valeur de l'attribut Name pour former le nom unique relatif du conteneur, comme dans l'exemple suivant :

ou=People

Nom

Spécifie le nom du conteneur.

Propriétés de table secondaires (bases de données relationnelles uniquement)

Les tables secondaires contiennent des attributs supplémentaires pour un objet géré. Par exemple, une table secondaire nommée tblUserAddress peut contenir les attributs de rue, de ville, d'état et de code postal pour l'objet géré Utilisateur.

Les propriétés suivantes sont affichées pour les tables secondaires :

Table

Spécifie le nom de la table.

Référence

Décrit le mappage entre la table principale et la table secondaire.

La référence est affichée à l'aide du format suivant :

table_principale.attribut=table_secondaire.attribut

Par exemple, tblUsers.id = tblUserAddress.userid indique que l'attribut ID dans la table principale tblUsers mappe vers l'attribut userid de la table tblUserAddress.

Propriétés d'attribut dans la fenêtre Managed Object Properties

Les propriétés suivantes sont affichées pour les attributs dans la fenêtre Propriétés de l'objet géré :

Nom d'affichage

Nom convivial de l'attribut. Ce nom s'affiche dans la liste d'attributs disponibles lorsque vous concevez une fenêtre pour une tâche dans la console d'utilisateur.

Physical Name (Nom physique)

Nom de l'attribut dans le référentiel d'utilisateurs.

Nom Well-Known

Les noms connus indiquent des attributs ayant une signification spéciale dans CA Identity Manager, comme l'attribut utilisé pour stocker des mots de passe d'utilisateur.

Propriétés d'attribut dans la fenêtre Attribute Properties

Vous pouvez afficher des détails supplémentaires sur un attribut en cliquant sur son nom pour ouvrir la fenêtre Attribute Properties.

Les propriétés d'attribut suivantes sont affichées dans la fenêtre Attribute Properties :

Description

Description de l'attribut.

Physical Name (Nom physique)

Nom de l'attribut dans le référentiel d'utilisateurs.

Classe d'objets (pour les attributs d'utilisateur, de groupe et d'organisation dans les annuaires LDAP uniquement)

Classe auxiliaire LDAP pour un attribut d'utilisateur, lorsque l'attribut ne fait pas partie de la classe d'objet principal spécifié pour l'objet d'utilisateur.

Vous pouvez spécifier une classe d'objets auxiliaire pour les objets d'utilisateur et de groupe uniquement.

Nom Well-Known

Indiquent des attributs ayant une signification spéciale dans CA Identity Manager, comme l'attribut utilisé pour stocker des mots de passe d'utilisateur.

Requis

Indique si une valeur est requise pour l'attribut, comme suit :

- True indique que l'attribut doit avoir une valeur.
- False indique qu'une valeur est facultative.

Lecture seule

Indique le niveau d'autorisation pour un attribut, comme suit :

- True indique que vous ne pouvez pas modifier l'attribut.
- False indique que vous pouvez modifier l'attribut.

Masqué

Indique si vous pouvez afficher un attribut dans une fenêtre de tâche pour une certaine tâche.

Les attributs masqués sont souvent utilisés dans les schémas d'attribut logiques.

Remarque : Pour plus d'informations, reportez-vous au manuel *Programming Guide for Java*.

Supports Multiple Values (Prise en charge de valeurs multiples)

Indique si l'attribut peut avoir plusieurs valeurs ou non. Par exemple, l'attribut utilisé pour stocker les membres d'un groupe est à valeurs multiples.

- True indique que l'attribut peut prendre en charge plusieurs valeurs.
- False indique que l'attribut peut avoir une seule valeur.

Multiple Value Delimiter (Délimiteur de valeurs multiples - bases de données relationnelles uniquement)

Caractère qui sépare plusieurs valeurs stockées dans une colonne unique.

System Attribute (Attribut système)

Indique si l'attribut est utilisé uniquement par CA Identity Manager, comme suit :

- True indique que l'attribut est un attribut système. L'attribut ne peut pas être ajouté à la fenêtre de tâche.
- False indique que les utilisateurs peuvent utiliser cet attribut. L'attribut peut s'afficher dans la fenêtre de tâche.

Type de données

Spécifie le type de données de l'attribut. La valeur par défaut est Chaîne.

Longueur maximale

Spécifie la longueur maximum d'une valeur d'attribut. Si vous la définissez sur 0, il n'y a aucune limite à sa longueur.

Validation Rule Set (Ensemble de règles de validation)

Spécifie le nom de l'ensemble de règles de validation associé à l'attribut, le cas échéant.

Ensembles de règles de validation

Une règle de validation applique aux données les conditions qu'un utilisateur saisit dans un champ de fenêtre de tâche. Ces conditions permettent d'appliquer un type de données ou un format, ou de s'assurer de la validité des données dans le contexte d'autres données de la fenêtre de tâche.

Une ou plusieurs règles de validation sont regroupées dans un ensemble de règles de validation, qui est ensuite associé à un attribut de profil. Par exemple, vous pouvez créer un ensemble de règles de validation qui contient une règle de validation Format de date, qui applique un format de date mm-jj-aaaa. Vous pouvez associer l'ensemble de règles de validation à l'attribut qui stocke la date d'embauche d'un employé.

Remarque : Vous créez des règles et des ensembles de règles de validation à partir du fichier de configuration d'annuaire ou de la console d'utilisateur.

La fenêtre Managed Object Properties (Propriétés de l'objet géré) affiche une liste des ensembles de règles de validation qui s'appliquent à l'annuaire CA Identity Manager. Pour afficher les détails d'un ensemble de règles de validation, cliquez sur son nom pour ouvrir la fenêtre Validation Rule Set Properties (Propriétés de l'ensemble de règles de validation).

Propriétés de règle de validation

Les informations suivantes sont affichées dans la fenêtre Validation Rule Properties (Propriétés de la règle de validation) :

Nom

Nom de la règle de validation

Description

Description de la règle

Classe

Nom de la classe Java qui implémente la règle de validation.

Ce champ ne s'affiche pas, sauf si la règle de validation est définie dans une classe Java.

Nom de fichier

Nom du fichier qui contient l'implémentation JavaScript de la règle de validation.

Ce champ ne s'affiche pas, sauf si la règle de validation est définie dans un fichier.

Expression régulière

Spécifie l'expression régulière qui implémente la règle de validation.

Ce champ ne s'affiche pas, sauf si la règle de validation est définie en tant qu'expression régulière.

Propriétés d'ensemble de règles de validation

Les informations suivantes sont affichées dans la fenêtre Validation Rule Set Properties (Propriétés de l'ensemble de règles de validation) :

Nom

Nom de l'ensemble de règles de validation

Description

Description de l'ensemble de règles de validation

La page Validation Rule Set Properties (Propriétés de l'ensemble de règles de validation) inclut également une liste des règles de validation comprises dans l'ensemble. Vous pouvez cliquer sur le nom de la règle de validation pour ouvrir la fenêtre Validation Rule Set Properties (Propriétés de l'ensemble de règles de validation).

Mise à jour des paramètres d'un annuaire CA Identity Manager

Pour afficher les paramètres actuels d'un annuaire CA Identity Manager, exportez-les et enregistrez-les dans un fichier XML.

Après avoir exporté les paramètres de l'annuaire, vous pouvez modifier le fichier XML, puis le réimporter pour mettre à jour l'annuaire. Vous pouvez également importer le fichier XML dans un autre annuaire pour définir les mêmes paramètres pour celui-ci.

Exportation d'un annuaire CA Identity Manager

Effectuez la procédure suivante pour exporter un annuaire CA Identity Manager.

Procédez comme suit:

1. Cliquez sur Directories (Annuaires).

   La liste des annuaires CA Identity Manager s'affiche.

2. Cliquez sur le nom de l'annuaire à exporter.

   La fenêtre Propriétés de l'annuaire CA Identity Manager s'affiche.

3. Au bas de cette fenêtre, cliquez sur Exporter.

4. Lorsque vous y êtes invité, enregistrez le fichier XML.

Mise à jour d'un annuaire CA Identity Manager

La mise à jour d'un annuaire CA Identity Manager permet :

- D'ajouter des définitions d'objet géré, y compris les attributs d'un objet, ou de les modifier.
- De définir les paramètres de recherche
- De modifier les propriétés d'annuaire

Remarque : CA Identity Manager ne supprime pas les définitions d'objet ou d'attribut.

Le fichier de configuration d'annuaire peut contenir uniquement les modifications que vous voulez apporter. N'incluez aucune propriété ou attribut déjà définis.

Remarque : Lorsque vous avez un cluster de noeuds CA Identity Manager, vous pouvez activer uniquement un noeud CA Identity Manager lorsque vous apportez des modifications dans la console de gestion. Arrêtez tous les noeuds CA Identity Manager sauf un avant de créer ou de modifier un annuaire CA Identity Manager.

Procédez comme suit:

1. Exportez les paramètres actuels de l'annuaire CA Identity Manager dans un fichier XML.
2. Modifiez le fichier XML.
3. Cliquez sur Directories (Annuaires).

   La liste des annuaires CA Identity Manager s'affiche.
4. Cliquez sur le nom de l'annuaire à mettre à jour.

   Les propriétés de l'annuaire CA Identity Manager s'affichent.
5. Au bas de cette fenêtre, cliquez sur Mettre à jour.
6. Saisissez le chemin d'accès et le nom du fichier XML pour mettre à jour l'annuaire CA Identity Manager ou accédez au fichier. Cliquez sur Terminer.

   Des informations sur le statut sont affichées dans la fenêtre Directory Configuration Output (Résultat de la configuration d'annuaire).
7. Cliquez sur Continue (Continuer).

Suppression d'un annuaire CA Identity Manager

Avant de supprimer un annuaire CA Identity Manager, supprimez tous les environnements CA Identity Manager qui y sont associés.

Procédez comme suit:

1. Dans la console de gestion, cliquez sur Directories (Annuaires).

   La liste des annuaires CA Identity Manager s'affiche.
2. Cochez la case à gauche des annuaires à supprimer.
3. Cliquez sur Supprimer.

   Un message de confirmation apparaît.
4. Cliquez sur OK pour confirmer la suppression.

Chapitre 6: Environnements CA Identity Manager

Ce chapitre traite des sujets suivants :

Environnements CA Identity Manager

Un environnement CA Identity Manager est une vue d'un référentiel d'utilisateurs. Dans un environnement CA Identity Manager, vous pouvez gérer des utilisateurs, des groupes, des organisations, des tâches et des rôles. Vous pouvez également attribuer des comptes à des utilisateurs dans des terminaux gérés, tels que des comptes de messagerie ou d'autres applications.

La console de gestion permet d'effectuer les tâches suivantes :

- Création, modification, ou suppression d'un environnement CA Identity Manager
- Exportation et importation d'un environnement CA Identity Manager
- Configuration des paramètres avancés
- Importation de rôles et de tâches
- Réinitialisation du compte du responsable du système

Conditions préalables à la création d'un environnement CA Identity Manager

Avant de commencer, utilisez la feuille de calcul dans la table suivante pour collecter les informations nécessaires :

Feuille de calcul de configuration d'environnement CA Identity Manager	
Informations requises	**Valeur**
Nom d'environnement CA Identity Manager explicite de votre choix Par exemple : MyEnvironment	
URL de base utilisée par CA Identity Manager pour former l'URL de redirection pour la stratégie de mots de passe par défaut de l'environnement Exemple : http://server.yourcompany.org	
Alias ajouté à l'URL permettant d'accéder à des tâches protégées dans l'environnement Exemple : http://server.yourcompany.org/iam/im/alias	
Alias ajouté à l'URL permettant d'accéder à des tâches publiques, telles que l'auto-enregistrement et des tâches de mot de passe oublié Exemple : http://server.yourcompany.org/iam/im/public_alias/index.jsp?task.tag=SelfRegistration **Remarque :** Si l'environnement n'inclut pas de tâches publiques, ne spécifiez pas d'alias public.	
Si vous avez fourni un alias public, nom d'un utilisateur existant qui fait office d'utilisateur public CA Identity Manager utilise les informations d'identification de l'utilisateur public au lieu des informations d'identification fournies par l'utilisateur lors de l'accès aux tâches publiques.	
Nom d'un CA Identity Manager (page 103)	

Feuille de calcul de configuration d'environnement CA Identity Manager	
Informations requises	**Valeur**
Nom de l'annuaire de provisionnement, lorsque l'environnement CA Identity Manager prend en charge le provisionnement	
Identificateur unique d'un utilisateur existant qui administre l'environnement CA Identity Manager Par exemple : myadmin	
Nom de l'agent SiteMinder ou du groupe d'agents qui protège l'environnement CA Identity Manager, si CA Identity Manager comprend SiteMinder	

Création d'un environnement CA Identity Manager

Les environnements CA Identity Manager permettent de gérer des objets dans un annuaire à l'aide d'un ensemble de rôles et de tâches. Utilisez l'assistant de création d'environnements CA Identity Manager pour vous orienter dans les étapes de création d'un environnement CA Identity Manager.

Avant de créer un environnement CA Identity Manager, tenez compte des points suivants :

- Supposons que vous utilisez un référentiel d'utilisateurs LDAP et vous avez configuré un conteneur d'utilisateurs comme ou=People dans le fichier de configuration d'annuaire (directory.xml) pour votre annuaire CA Identity Manager. Vérifiez que les utilisateurs sélectionnés lors de la création de l'environnement CA Identity Manager existent dans ce conteneur. La sélection d'un compte d'utilisateur qui n'existe pas dans le conteneur d'utilisateurs peut entraîner des échecs.
- Lorsque vous configurez un environnement CA Identity Manager pour gérer un annuaire d'utilisateurs LDAP avec une structure d'utilisateur hiérarchique ou non hiérarchique, le profil de l'utilisateur sélectionné doit inclure son organisation. Pour assurer la correcte configuration du profil d'un utilisateur, ajoutez le nom de son organisation à l'attribut physique correspondant à l'attribut connu %ORG_MEMBERSHIP% dans le fichier directory.xml (page 86). Par exemple, lorsque la description de l'attribut physique est mappée vers l'attribut reconnu %ORG_MEMBERSHIP% dans le fichier directory.xml et que l'utilisateur appartient à l'organisation Employees, le profil de l'utilisateur doit contenir la paire attribut/valeur description=Employees.

Procédez comme suit:

1. Si CA Identity Manager utilise un cluster de serveurs de stratégies, démarrez un seul serveur de stratégies.
2. Si vous avez un cluster de noeuds CA Identity Manager, démarrez un seul noeud CA Identity Manager.
3. Dans la console de gestion, cliquez sur Environnements.
4. Cliquez sur Créer.

   L'assistant de création d'environnements CA Identity Manager s'ouvre.
5. Renseignez les informations suivantes :

   - **Environment name (Nom de l'environnement)**

     Spécifie un nom unique pour l'environnement.

   - **Description**

     Décrit l'environnement.

   - **Protected alias (Alias protégé)**

     Spécifie un nom unique, tel que Employees. Cet alias est ajouté à l'URL permettant d'accéder à des tâches protégées dans l'environnement CA Identity Manager. Par exemple, si l'alias est Employees, l'URL permettant d'accéder à l'environnement d'employés sera http://my*server.mycompany.com*/iam/im/employees.

     Remarque : L'alias respecte la casse et ne peut pas contenir d'espaces. Lors de la spécification de l'alias, il est recommandé d'utiliser des minuscules sans ponctuation ni espace.

   - **Adresse de base**

     Spécifie l'URL pour CA Identity Manager. Cette URL requiert un nom d'hôte et ne peut pas inclure d'hôte local. De même, n'incluez pas l'alias, par exemple : http://*myserver.mycompany.com*/iam/im.

     Si vous utilisez un agent Web, veillez à ce que l'adresse de base soit changée pour refléter l'URL de l'agent Web.

     Remarque : Si vous utilisez un agent Web pour protéger des ressources CA Identity Manager, ne spécifiez pas de numéro de port dans le champ Adresse de base. Si vous utilisez un agent Web et que l'adresse de base contient un numéro de port, les liens aux tâches CA Identity Manager ne fonctionneront pas correctement.

     Pour plus d'informations sur la protection des ressources CA Identity Manager, consultez le *Manuel d'installation* de votre serveur d'applications.

     Cliquez sur Suivant.
6. Sélectionnez un annuaire CA Identity Manager à associer à l'environnement que vous créez et cliquez sur Suivant.

7. Si l'environnement CA Identity Manager prend en charge le provisionnement, sélectionnez le serveur de provisionnement approprié à utiliser.

   Remarque : Si vous avez sélectionné un annuaire de provisionnement comme annuaire CA Identity Manager, vous ne serez pas invité à sélectionner un serveur de provisionnement.

8. Configurez la prise en charge des tâches publiques. En règle générale, les tâches publiques sont des tâches d'auto-administration, telles que les tâches d'auto-enregistrement ou de mot de passe oublié. Les utilisateurs n'ont pas besoin de se connecter pour accéder à des tâches publiques.

   Remarque : Pour permettre aux utilisateurs d'utiliser des tâches d'auto-administration, configurez la prise en charge de tâches publiques.

   a. Spécifiez un nom unique qui sera ajouté à l'URL pour l'accès aux tâches publiques.

      Exemple : Pour accéder à la tâche d'auto-enregistrement par défaut, vous utiliserez l'URL suivante :

      http://*myserver.mycompany.com*/iam/im/*alias*/index.jsp?task.tag=SelfRegistration

      Dans cette URL, *alias* est le nom unique que vous fournissez.

   b. Spécifiez l'un des comptes d'utilisateurs existants suivants qui sert de compte d'utilisateur public. CA Identity Manager utilise ce compte pour permettre aux utilisateurs inconnus d'accéder à des tâches publiques sans fournir d'informations d'identification.

      - Les utilisateurs LDAP saisissent l'identificateur unique ou le nom unique relatif au compte d'utilisateur public. Veillez à ce que cette valeur soit mappée vers %USER_ID% connu (page 79). Par exemple, si le nom unique de l'utilisateur est uid=Admin1, ou=People, ou=Employees, ou=NeteAuto, saisissez Admin1.
      - Les utilisateurs de la base de données relationnelles saisissent la valeur mappée vers l'attribut reconnu %USER_ID% dans le fichier de configuration de l'annuaire, ou l'identificateur unique de l'utilisateur.

   Pour afficher l'identificateur complet de l'utilisateur, cliquez sur Valider.

9. Sélectionnez les tâches et les rôles à créer pour cet environnement. Vous pouvez effectuer les tâches suivantes :

   - **Création de rôles par défaut**

     Crée un ensemble de tâches et de rôles par défaut qui sont initialement disponibles dans l'environnement. Les administrateurs peuvent utiliser ces tâches et ces rôles comme modèles pour créer d'autres tâches et rôles dans la console d'utilisateur.

- **Création uniquement du rôle de responsable du système**

  Crée uniquement le rôle de responsable du système et les tâches qui lui sont associées.

  Le rôle de responsable du système est requis pour accéder à l'environnement.

  Un responsable du système peut créer d'autres tâches et rôles dans la console d'utilisateur.

- **Importation de rôles du fichier**

  Importe un fichier de définitions de rôles que vous avez exporté à partir d'un autre environnement CA Identity Manager.

  Remarque : Pour utiliser l'environnement CA Identity Manager, le fichier de définitions de rôles doit au moins inclure le rôle de responsable du système ou un rôle qui inclut des tâches similaires.

  A partir du bouton d'option de fichier, Sélectionnez Import roles (Importer des rôles) et saisissez le chemin d'accès et le nom de fichier du fichier de définitions de rôles, ou recherchez le fichier à importer.

10. Sélectionnez Role Definitions files (Fichiers de définitions de rôles) pour créer des définitions de tâches par défaut pour votre environnement et cliquez sur Suivant.

    Les fichiers de définitions de rôles sont des fichiers XML qui définissent un ensemble de tâches et de rôles requis pour la prise en charge de fonctionnalités spécifiques. Par exemple, si vous voulez gérer des terminaux Active Directory et UNIX NIS, sélectionnez ces fichiers de définitions de rôles.

    Remarque : Cette étape est facultative. Si vous ne voulez pas créer de tâches par défaut supplémentaires pour la prise en charge de cette nouvelle fonctionnalité, ignorez cette fenêtre.

11. Définissez un utilisateur pour agir en tant que responsable du système pour cet environnement comme suit :

    a. Dans le champ System Manager (Responsable du système), saisissez la valeur mappée vers l'attribut reconnu %USER_ID% dans le fichier de configuration d'annuaire, ou spécifiez l'un des comptes d'utilisateur suivants :

       - Les utilisateurs LDAP saisissent l'identificateur unique ou le nom unique relatif de l'utilisateur. Par exemple, si le nom unique de l'utilisateur est uid=Admin1, ou=People, ou=Employees, ou=NeteAuto, saisissez Admin1.
       - Les utilisateurs de la base de données relationnelles saisissent l'identificateur unique de l'utilisateur.

b. Cliquez sur Ajouter.

   CA Identity Manager ajoute l'identificateur complet de l'utilisateur à la liste d'utilisateurs.

c. Cliquez sur Suivant.

Lors de la spécification du responsable du système, tenez compte des points suivants :

- Le responsable du système ne doit *pas* être le même utilisateur que l'administrateur du référentiel d'utilisateurs.
- Vous pouvez spécifier plusieurs responsables du système pour l'environnement. Toutefois, vous pouvez uniquement spécifier le responsable du système initial dans la console de gestion. Pour spécifier des responsables du système supplémentaires, affectez le rôle de responsable du système aux utilisateurs appropriés dans la console d'utilisateur.

12. Dans le champ Inbound Administrateur (Administrateur entrant), spécifiez un compte d'administrateur CA Identity Manager qui peut exécuter des tâches d'administrateur mappées vers des mappages entrants.

    L'utilisateur doit pouvoir exécuter toutes ces tâches sur un utilisateur. Le rôle Provisionnement du gestionnaire de synchronisations contient les tâches de provisionnement incluses dans les mappages entrants par défaut.

13. Saisissez un mot de passe pour le référentiel de clés, base de données de clés qui chiffrent et déchiffrent des données.

    La définition de ce mot de passe est une condition préalable à la définition de clés dynamiques. Vous pouvez modifier le mot de passe après la création de l'environnement à l'aide de Système, tâches Clés secrètes.

    Une page résumant les paramètres de l'environnement s'affiche.

14. Révisez ces paramètres. Pour les modifier, cliquez sur Précédent, ou pour créer l'environnement CA Identity Manager avec les paramètres actuels, cliquez sur Terminer.

    La fenêtre Environment Configuration Output (Résultat de la configuration de l'environnement) affiche la progression de la création de l'environnement.

15. Pour fermer l'assistant de création d'environnements CA Identity Manager, cliquez sur Continuer.

16. Démarrez l'environnement.

    Cliquez sur le nom de l'environnement, puis cliquez sur Lancer.

17. Si vous avez arrêté des serveurs de stratégies à l'étape 1, redémarrez-les maintenant.

Accès à un environnement CA Identity Manager

Après avoir créé un environnement CA Identity Manager, vous pouvez y accéder en saisissant une URL dans un navigateur.

Remarque : Pour accéder à la console de gestion, activez JavaScript dans le navigateur que vous utilisez.

Le format de l'URL dépend de la configuration de l'environnement et du type de tâche à laquelle vous voulez accéder.

- Pour accéder à des tâches protégées à partir de la console d'utilisateur, utilisez l'URL suivante :

  `http://nomhôte/iam/im/alias`

  hostname

  Définit le nom de domaine complet du serveur sur lequel CA Identity Manager est installé. Par exemple : myserver.mycompany.com

  alias

  Définit l'alias de l'environnement ; par exemple : employees.

  Connectez-vous à l'environnement CA Identity Manager avec un compte d'administrateur privilégié, tel que le compte du responsable du système créé pour l'environnement CA Identity Manager.

  Remarque : Toutes les tâches CA Identity Manager sont protégées, sauf si vous configurez des tâches publiques.

- Pour accéder à des tâches publiques, pour lesquelles les utilisateurs n'ont pas à fournir d'informations d'identification, utilisez une URL au format suivant :

  `http://nomhôte/iam/im/alias/index.jsp?task.tag=tasktag`

  hostname

  Définit le nom de domaine complet du serveur sur lequel CA Identity Manager est installé. Par exemple : myserver.mycompany.com

alias

Définit l'alias des tâches publiques. Par exemple : auto-administration.

task_tag

Définit la balise pour la tâche à appeler.

Spécifiez la balise lors de la configuration d'une tâche dans la console d'utilisateur.

Les balises de tâche pour les tâches d'auto-enregistrement par défaut et de réinitialisation de mot de passe oublié sont SelfRegistration et ForgottenPasswordReset.

Remarque : Pour plus d'informations, reportez-vous au *manuel d'administration*.

Procédure de configuration d'un environnement pour le provisionnement

Une fois l'accès au serveur de provisionnement activé (page 173), vous pouvez configurer un environnement pour le provisionnement.

Puis, vous pouvez créer un utilisateur CA Identity Manager spécial, appelé administrateur entrant, créer une connexion au serveur de provisionnement et configurer la synchronisation entrante dans le gestionnaire de provisionnement.

Remarque : Lors de la modification des propriétés de provisionnement d'un environnement, veillez à redémarrer le serveur d'applications afin que les modifications s'appliquent.

Configuration de l'administrateur entrant

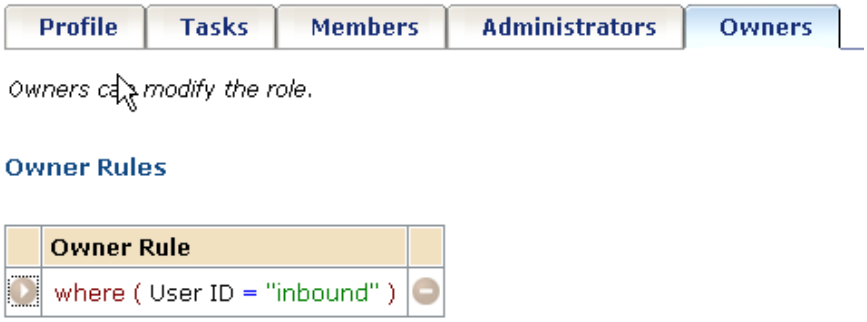
Pour le fonctionnement correct de la synchronisation entrante, créez un utilisateur CA Identity Manager spécial appelé *administrateur entrant*. Dans les versions précédentes de CA Identity Manager, l'administrateur entrant était appelé *utilisateur d'entreprise*. Aucun utilisateur ne se connecte à ce compte, mais CA Identity Manager l'utilise en interne. Toutefois, créez ce compte d'utilisateur et attribuez-lui les tâches appropriées.

Procédez comme suit:

1. Connectez-vous à l'environnement CA Identity Manager en tant qu'utilisateur disposant du rôle de responsable du système.
2. Créez un utilisateur. Vous pouvez nommer cet utilisateur **entrant** comme rappel de son objectif.

3. Sélectionnez Rôle d'administration, Modifier un rôle d'administration et sélectionnez un rôle qui contient les tâches que vous utilisez pour la synchronisation.
   - Provisionnement de la création d'utilisateur
   - Provisionnement de l'activation/désactivation d'utilisateur
   - Provisionnement de la modification d'utilisateur

   Remarque : Si vous n'avez pas modifié les tâches de synchronisation par défaut, utilisez le rôle Provisionnement du gestionnaire de synchronisations.
4. Dans l'onglet Membres, ajoutez une stratégie de membre qui inclut :
   - Une règle de membre à laquelle le nouvel utilisateur est conforme
   - Une règle de portée fournissant l'accès à tous les utilisateurs affectés par les modifications de l'annuaire de provisionnement déclenchant la synchronisation entrante

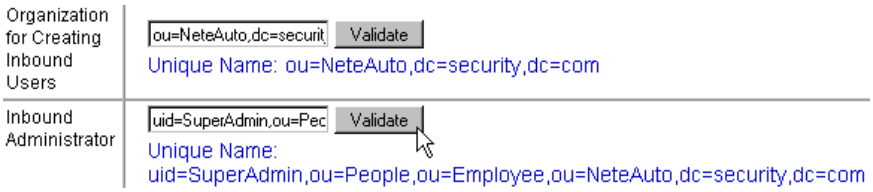


5. Dans la console de gestion :
   a. Sélectionnez l'environnement.
   b. Cliquez sur Paramètres avancés (Advanced Settings), Provisioning (Provisionnement).
   c. Remplissez le champ Organization for Creating Inbound Users (Organisation pour la création d'utilisateurs entrants) si l'annuaire CA Identity Manager inclut une organisation.

      Cette organisation contient les utilisateurs créés lors de la synchronisation entrante. Par exemple, lorsqu'un utilisateur est ajouté à l'annuaire de provisionnement, CA Identity Manager l'ajoute à cette organisation.

d. Remplissez le champ Inbound Administrator (Administrateur entrant) en indiquant l'ID de l'utilisateur créé à l'étape 2.

e. Cliquez sur Valider pour confirmer que l'ID d'utilisateur est accepté, comme illustré dans l'exemple suivant dans lequel l'ID d'utilisateur complet s'affiche sous l'ID d'utilisateur saisi.



f. Modifiez d'autres champs de cette fenêtre. Aucune modification n'est requise.

Si vous apportez des modifications, veillez à connaître le fonctionnement des champs. Pour obtenir des détails sur chaque champ, cliquez sur le lien Aide de la fenêtre.

Connection d'un environnement au serveur de provisionnement

Procédez comme suit:

1. Dans la console de gestion, cliquez sur Environnements.

   Une liste des environnements existants s'affiche.

2. Cliquez sur le nom de l'environnement que vous voulez associer au serveur de provisionnement.

3. Dans le champ Serveur de provisionnement, cliquez sur l'icône de flèche vers la droite.

   La fenêtre Provisioning Properties (Propriétés de provisionnement) s'ouvre.

4. Sélectionnez le serveur de provisionnement.

5. Au bas de la page, Cliquez sur Enregistrer.

6. Configurez la synchronisation dans le gestionnaire de provisionnement (page 199).

Configuration de la synchronisation dans le gestionnaire de provisionnement

La synchronisation entrante assure la mise à jour de CA Identity Manager et applique les modifications apportées à l'annuaire de provisionnement. Les modifications incluent les changements effectués à l'aide du gestionnaire de provisionnement et les changements effectués dans les terminaux pour lesquels le serveur de provisionnement dispose d'un connecteur. Chaque serveur de provisionnement prend en charge un environnement unique. Toutefois, si l'environnement actuel est indisponible, vous pouvez configurer des environnements de sauvegarde sur différents systèmes dans un cluster.

Procédez comme suit:

1. Sélectionnez Lancer, CA Identity Manager, Provisioning Manager (Gestionnaire de provisionnement).
2. Cliquez sur Système, CA Identity Manager Setup (Configuration de CA Identity Manager).
3. Renseignez le champ Nom d'hôte avec le nom du système dans lequel le serveur CA Identity Manager est installé.
4. Renseignez le champ Port avec le numéro de port du serveur d'applications.
5. Renseignez le champ Environment name (Nom de l'environnement) avec l'alias de l'environnement.
6. Sélectionnez Connexion sécurisée si vous voulez utiliser le protocole HTTPS pour communiquer avec le serveur CA Identity Manager au lieu d'utiliser HTTP et de chiffrer chaque notification.
7. Cliquez sur Ajouter.
8. Répétez les étapes 3 à 6 pour chaque version de sauvegarde de l'environnement.

   Si le serveur d'applications pour l'environnement actuel est indisponible, CA Identity Manager échouera à basculer vers un environnement de sauvegarde. Pour définir l'ordre de basculement, vous pouvez réorganiser les environnements en cours et de sauvegarde.
9. S'il s'agit du premier environnement, remplissez le champ Secret partagé à l'aide du mot de passe saisi lors de l'installation de CA Identity Manager pour l'utilisateur des composants intégrés.

   Remarque : Ces champs ne s'appliquent pas si la norme FIPS est activée dans cette installation.
10. Définissez le niveau de journalisation comme suit :
    - No log (Aucune journalisation) : aucune information n'est écrite dans le fichier journal.
    - Erreur : seuls les messages d'erreur sont journalisés.
    - Informations : les messages d'erreur et d'informations sont journalisés (valeur par défaut).
    - Avertissement : les messages d'erreur, d'avertissement et d'informations sont journalisés.
    - Débogage : toutes les informations sont journalisées.
11. Avant de vous connecter à l'environnement, redémarrez le serveur d'applications.

Remarque : Pour un journal d'opérations de synchronisation entrante et tout problème rencontré lors de la synchronisation, consultez le fichier suivant :

PSHOME\logs\etanotify<date>.log

Importation de rôles de provisionnement personnalisés

Lors de la création de l'environnement, vous pouvez choisir d'utiliser les rôles par défaut ou un fichier de définitions de rôles personnalisés que vous créez. Si vous importez des définitions de rôles personnalisés, importez *également* les définitions de rôle de provisionnement uniquement. Une fois l'environnement créé, importez les définitions de rôle à partir du fichier ProvisioningOnly-RoleDefinitions.xml, situé dans l'un des dossiers suivants :

admin_tools/ProvisioningOnlyRoleDefinitions/Organization
admin_tools/ProvisioningOnlyRoleDefinitions/NoOrganization

Emplacement par défaut d'*admin_tools* :

- **Windows :** <chemin_d'installation>\tools
- **UNIX :** <chemin_installation2>/tools

Synchronisation des comptes pour la tâche Réinitialiser le mot de passe de l'utilisateur

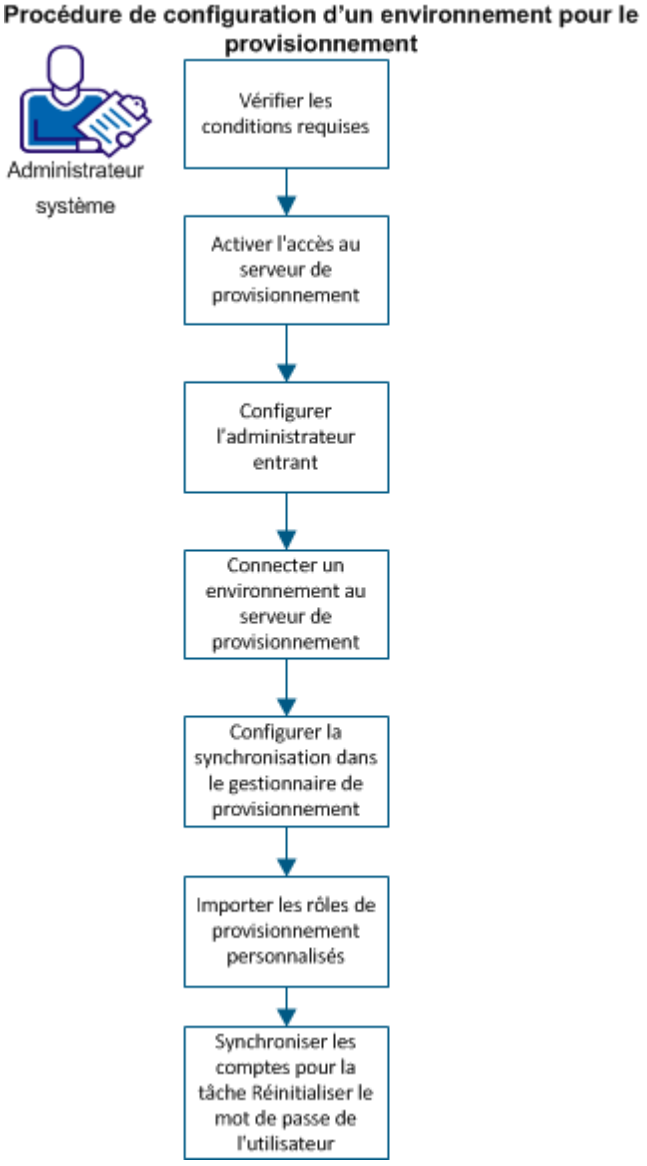
Pour activer le provisionnement pour un environnement CA Identity Manager, vous devez importer le fichier de configuration ProvisioningOnly-RoleDefinitions.xml, qui permet de créer les rôles et les tâches pour le provisionnement de l'utilisateur.

Dans ce fichier, le paramètre de synchronisation des comptes par défaut est défini sur Désactivé pour la tâche Réinitialiser le mot de passe de l'utilisateur. Avant d'activer le provisionnement, le paramètre de provisionnement est défini sur A la fin de la tâche.

Pour lancer la tâche Réinitialiser le mot de passe de l'utilisateur en vue de déclencher la synchronisation des comptes, définissez l'option de synchronisation après avoir importé le fichier ProvisioningOnly-RoleDefinitions.xml pour activer le provisionnement.

Procédure de création et de déploiement de connecteurs à l'aide de Connector Xpress

Vous pouvez configurer le provisionnement de sorte qu'un environnement fournisse des comptes dans d'autres systèmes à des utilisateurs gérés par CA Identity Manager. Les comptes permettent aux utilisateurs d'accéder à des ressources supplémentaires, comme un compte de messagerie. Vous fournissez ces comptes supplémentaires en affectant des rôles de provisionnement que vous créez dans CA Identity Manager.



Connectez-vous en tant qu'administrateur et effectuer les opérations suivantes :

1. Vérification des conditions préalables (page 203)

2. Activation de l'accès au serveur de provisionnement (page 173)
3. Configuration de l'administrateur entrant (page 197)
4. Connection d'un environnement au serveur de provisionnement (page 199)
5. Configuration de la synchronisation dans le gestionnaire de provisionnement (page 199)
6. Importation de rôles de provisionnement personnalisés (page 201)
7. Synchronisation de comptes pour la tâche Réinitialiser le mot de passe de l'utilisateur (page 201)

Vérification des conditions préalables

Avant de configurer l'environnement pour le provisionnement, vérifiez que l'annuaire de provisionnement est installé sur CA Directory. Pour plus d'informations, reportez-vous au *Manuel d'installation*.

Activation de l'accès au serveur de provisionnement

Vous activez l'accès au serveur de provisionnement à l'aide du lien Directories (Annuaires) dans la console de gestion.

Remarque : Une condition préalable à cette procédure est l'installation de l'annuaire de provisionnement sur CA Directory. Pour plus d'informations, reportez-vous au *Manuel d'installation*.

Procédez comme suit:

1. Pour ouvrir la console de gestion, saisissez l'URL suivante dans un navigateur :

   `http://nom_hôte:port/iam/immanage`

   hostname

   Définit le nom d'hôte complet du système sur lequel le serveur CA Identity Manager est installé.

   port

   Définit le numéro de port du serveur d'applications.

2. Cliquez sur Directories (Annuaires).

   La fenêtre Directories (Annuaires) de CA Identity Manager s'affiche.

3. Cliquez sur Create from Wizard (Créer à partir de l'assistant).

4. Saisissez le chemin d'accès et le nom du fichier XML de l'annuaire pour configurer l'annuaire de provisionnement. Il est stocké sous directoryTemplates\ProvisioningServer dans le dossier Outils d'administration. L'emplacement par défaut de ce dossier est :

   - Windows : <chemin_d'installation>\tools
   - UNIX : <chemin_installation2>/tools

   Remarque : Vous pouvez utiliser ce fichier de configuration d'annuaire tel quel, sans avoir à y apporter de modification.

5. Cliquez sur Suivant.

6. Spécifiez des valeurs pour les champs de cette fenêtre, comme suit :

   Nom

   Nom de l'annuaire de provisionnement associé au serveur de provisionnement que vous configurez.

   - Si CA Identity Manager n'est pas intégré à SiteMinder, spécifiez un nom significatif pour l'objet utilisé par CA Identity Manager pour la connexion à l'annuaire d'utilisateurs.
   - Si CA Identity Manager est intégré à SiteMinder, vous avez deux possibilités :

     Si vous voulez créer un objet de connexion d'annuaire d'utilisateurs dans SiteMinder, spécifiez un nom significatif. CA Identity Manager crée cet objet dans SiteMinder avec ce nom.

     Si vous voulez vous connecter à un annuaire d'utilisateurs SiteMinder existant, spécifiez le nom de l'objet de connexion d'annuaire d'utilisateurs SiteMinder tel qu'il s'affiche dans l'interface utilisateur du serveur de stratégies.

   Description

   (Facultatif) Description de l'annuaire CA Identity Manager.

   Hôte

   Indique le nom d'hôte ou l'adresse IP du système sur lequel l'annuaire d'utilisateurs est installé.

   Port

   Indique le numéro de port de l'annuaire d'utilisateurs.

Domaine

Nom du domaine de provisionnement géré par CA Identity Manager.

Important : Lors de la création d'un annuaire de provisionnement via la console de gestion, n'utilisez aucun caractère de langue étrangère pour le nom du domaine, car autrement, sa création échouera.

Le nom doit correspondre au nom du domaine de provisionnement que vous avez spécifié pendant l'installation.

Remarque : Le nom du domaine est sensible à la casse.

Nom d'utilisateur

Spécifie un utilisateur qui peut se connecter au gestionnaire de provisionnement.

L'utilisateur doit avoir un profil d'administrateur de domaines ou un ensemble équivalent de droits sur le domaine de provisionnement.

Mot de passe

Spécifie le mot de passe pour l'utilisateur global que vous avez saisi dans le champ Nom d'utilisateur.

Confirmer le mot de passe

Confirmez le mot de passe saisi dans le champ Mot de passe.

Connexion sécurisée

Indique si CA Identity Manager utilise une connexion sécurisée.

Assurez-vous de sélectionner cette option pour les référentiels d'utilisateurs Active Directory.

Directory Search Parameters (Paramètres de recherche d'annuaire)

maxrows spécifie le nombre maximum de résultats renvoyés lors d'une recherche dans un annuaire d'utilisateurs. Cette valeur remplace les limites définies dans l'annuaire LDAP. Lorsque des paramètres contradictoires sont appliqués, le serveur LDAP utilise le paramètre dont la valeur est la plus faible.

Remarque : Le paramètre maxrows ne limite pas le nombre de résultats qui sont affichés dans la fenêtre de tâche de CA Identity Manager. Pour configurer les paramètres d'affichage, modifiez la définition de la fenêtre de liste dans la console d'utilisateur CA Identity Manager. Pour obtenir des instructions, consultez le *Manuel de conception de la console d'utilisateur*.

timeout détermine le nombre maximum de secondes que tarde la recherche dans un annuaire avant de se terminer.

Failover Connections (Connexions de basculement)

Nom d'hôte et numéro de port d'un ou de plusieurs systèmes facultatifs qui sont des serveurs de provisionnement secondaires. Si vous spécifiez plusieurs serveurs, CA Identity Manager tente de se connecter aux systèmes répertoriés.

Les serveurs de provisionnement secondaires sont utilisés si un échec du serveur de provisionnement principal se produit. Lorsque le serveur de provisionnement principal redevient disponible, l'utilisation du serveur de provisionnement secondaire se poursuit. Si vous voulez utiliser le serveur de provisionnement principal à nouveau, redémarrez les serveurs de provisionnement secondaires.

7. Cliquez sur Suivant.
8. Sélectionnez les objets à gérer, comme les utilisateurs ou les groupes.
9. Après avoir configuré les objets de manière appropriée, affichez le récapitulatif, déployez l'annuaire de provisionnement et vérifiez ses paramètres.
10. Cliquez sur l'une de ces actions :
    a. Pour effectuer une modification, cliquez sur Précédent.
    b. Cliquez sur Enregistrer pour enregistrer les informations de l'annuaire si vous voulez revenir et effectuer le déploiement plus tard.
    c. Cliquez sur Terminer pour terminer la procédure et commencer la configuration d'un environnement à l'aide du provisionnement (page 197).

Configuration de l'administrateur entrant

Pour le fonctionnement correct de la synchronisation entrante, créez un utilisateur CA Identity Manager spécial appelé *administrateur entrant*. Dans les versions précédentes de CA Identity Manager, l'administrateur entrant était appelé *utilisateur d'entreprise*. Aucun utilisateur ne se connecte à ce compte, mais CA Identity Manager l'utilise en interne. Toutefois, créez ce compte d'utilisateur et attribuez-lui les tâches appropriées.

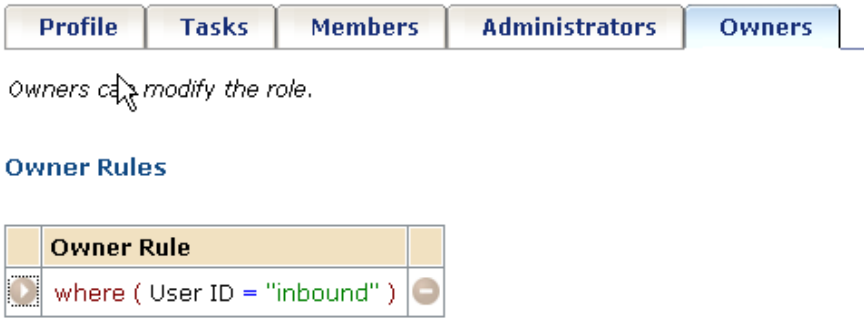
Procédez comme suit:

1. Connectez-vous à l'environnement CA Identity Manager en tant qu'utilisateur disposant du rôle de responsable du système.
2. Créez un utilisateur. Vous pouvez nommer cet utilisateur **entrant** comme rappel de son objectif.

3. Sélectionnez Rôle d'administration, Modifier un rôle d'administration et sélectionnez un rôle qui contient les tâches que vous utilisez pour la synchronisation.
   - Provisionnement de la création d'utilisateur
   - Provisionnement de l'activation/désactivation d'utilisateur
   - Provisionnement de la modification d'utilisateur

   Remarque : Si vous n'avez pas modifié les tâches de synchronisation par défaut, utilisez le rôle Provisionnement du gestionnaire de synchronisations.

4. Dans l'onglet Membres, ajoutez une stratégie de membre qui inclut :
   - Une règle de membre à laquelle le nouvel utilisateur est conforme
   - Une règle de portée fournissant l'accès à tous les utilisateurs affectés par les modifications de l'annuaire de provisionnement déclenchant la synchronisation entrante

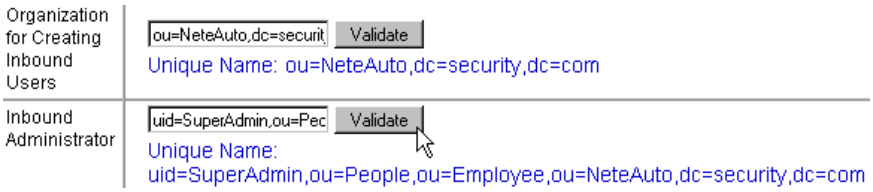


5. Dans la console de gestion :
   a. Sélectionnez l'environnement.
   b. Cliquez sur Paramètres avancés (Advanced Settings), Provisioning (Provisionnement).
   c. Remplissez le champ Organization for Creating Inbound Users (Organisation pour la création d'utilisateurs entrants) si l'annuaire CA Identity Manager inclut une organisation.

      Cette organisation contient les utilisateurs créés lors de la synchronisation entrante. Par exemple, lorsqu'un utilisateur est ajouté à l'annuaire de provisionnement, CA Identity Manager l'ajoute à cette organisation.

d. Remplissez le champ Inbound Administrator (Administrateur entrant) en indiquant l'ID de l'utilisateur créé à l'étape 2.

e. Cliquez sur Valider pour confirmer que l'ID d'utilisateur est accepté, comme illustré dans l'exemple suivant dans lequel l'ID d'utilisateur complet s'affiche sous l'ID d'utilisateur saisi.



f. Modifiez d'autres champs de cette fenêtre. Aucune modification n'est requise.

Si vous apportez des modifications, veillez à connaître le fonctionnement des champs. Pour obtenir des détails sur chaque champ, cliquez sur le lien Aide de la fenêtre.

Connection d'un environnement au serveur de provisionnement

Procédez comme suit:

1. Dans la console de gestion, cliquez sur Environnements.

   Une liste des environnements existants s'affiche.

2. Cliquez sur le nom de l'environnement que vous voulez associer au serveur de provisionnement.

3. Dans le champ Serveur de provisionnement, cliquez sur l'icône de flèche vers la droite.

   La fenêtre Provisioning Properties (Propriétés de provisionnement) s'ouvre.

4. Sélectionnez le serveur de provisionnement.

5. Au bas de la page, Cliquez sur Enregistrer.

6. Configurez la synchronisation dans le gestionnaire de provisionnement (page 199).

Configuration de la synchronisation dans le gestionnaire de provisionnement

La synchronisation entrante assure la mise à jour de CA Identity Manager et applique les modifications apportées à l'annuaire de provisionnement. Les modifications incluent les changements effectués à l'aide du gestionnaire de provisionnement et les changements effectués dans les terminaux pour lesquels le serveur de provisionnement dispose d'un connecteur. Chaque serveur de provisionnement prend en charge un environnement unique. Toutefois, si l'environnement actuel est indisponible, vous pouvez configurer des environnements de sauvegarde sur différents systèmes dans un cluster.

Procédez comme suit:

1. Sélectionnez Lancer, CA Identity Manager, Provisioning Manager (Gestionnaire de provisionnement).
2. Cliquez sur Système, CA Identity Manager Setup (Configuration de CA Identity Manager).
3. Renseignez le champ Nom d'hôte avec le nom du système dans lequel le serveur CA Identity Manager est installé.
4. Renseignez le champ Port avec le numéro de port du serveur d'applications.
5. Renseignez le champ Environment name (Nom de l'environnement) avec l'alias de l'environnement.
6. Sélectionnez Connexion sécurisée si vous voulez utiliser le protocole HTTPS pour communiquer avec le serveur CA Identity Manager au lieu d'utiliser HTTP et de chiffrer chaque notification.
7. Cliquez sur Ajouter.
8. Répétez les étapes 3 à 6 pour chaque version de sauvegarde de l'environnement.

   Si le serveur d'applications pour l'environnement actuel est indisponible, CA Identity Manager échouera à basculer vers un environnement de sauvegarde. Pour définir l'ordre de basculement, vous pouvez réorganiser les environnements en cours et de sauvegarde.
9. S'il s'agit du premier environnement, remplissez le champ Secret partagé à l'aide du mot de passe saisi lors de l'installation de CA Identity Manager pour l'utilisateur des composants intégrés.

   Remarque : Ces champs ne s'appliquent pas si la norme FIPS est activée dans cette installation.
10. Définissez le niveau de journalisation comme suit :
    - No log (Aucune journalisation) : aucune information n'est écrite dans le fichier journal.
    - Erreur : seuls les messages d'erreur sont journalisés.
    - Informations : les messages d'erreur et d'informations sont journalisés (valeur par défaut).
    - Avertissement : les messages d'erreur, d'avertissement et d'informations sont journalisés.
    - Débogage : toutes les informations sont journalisées.
11. Avant de vous connecter à l'environnement, redémarrez le serveur d'applications.

Remarque : Pour un journal d'opérations de synchronisation entrante et tout problème rencontré lors de la synchronisation, consultez le fichier suivant :

PSHOME\logs\etanotify<date>.log

Importation de rôles de provisionnement personnalisés

Lors de la création de l'environnement, vous pouvez choisir d'utiliser les rôles par défaut ou un fichier de définitions de rôles personnalisés que vous créez. Si vous importez des définitions de rôles personnalisés, importez *également* les définitions de rôle de provisionnement uniquement. Une fois l'environnement créé, importez les définitions de rôle à partir du fichier ProvisioningOnly-RoleDefinitions.xml, situé dans l'un des dossiers suivants :
admin_tools/ProvisioningOnlyRoleDefinitions/Organization
admin_tools/ProvisioningOnlyRoleDefinitions/NoOrganization

Emplacement par défaut d'*admin_tools* :

- **Windows :** <chemin_d'installation>\tools
- **UNIX :** <chemin_installation2>/tools

Synchronisation des comptes pour la tâche Réinitialiser le mot de passe de l'utilisateur

Pour activer le provisionnement pour un environnement CA Identity Manager, vous devez importer le fichier de configuration ProvisioningOnly-RoleDefinitions.xml, qui permet de créer les rôles et les tâches pour le provisionnement de l'utilisateur.

Dans ce fichier, le paramètre de synchronisation des comptes par défaut est défini sur Désactivé pour la tâche Réinitialiser le mot de passe de l'utilisateur. Avant d'activer le provisionnement, le paramètre de provisionnement est défini sur A la fin de la tâche.

Pour lancer la tâche Réinitialiser le mot de passe de l'utilisateur en vue de déclencher la synchronisation des comptes, définissez l'option de synchronisation après avoir importé le fichier ProvisioningOnly-RoleDefinitions.xml pour activer le provisionnement.

Gestion des environnements

Cette section décrit la gestion d'un environnement.

Modification des propriétés d'environnement CA Identity Manager

La fenêtre Environment Properties CA Identity Manager (Propriétés de l'environnement CA Identity Manager) de la console de gestion permet d'effectuer les tâches suivantes :

- Affichage des paramètres actuels de l'environnement
- Modification de la description, de l'adresse de base et des alias protégés et publics

- Importation d'un environnement CA Identity Manager existant suite à une mise à niveau

  Remarque : Pour plus d'informations sur l'importation d'environnements CA Identity Manager existants, consultez la section sur la mise à niveau du *Manuel d'installation*.

- Démarrage et arrêt de l'environnement
- Pour la configuration des tâches suivantes, accédez aux pages correspondantes :
  - **Paramètres avancés**

    Permet de configurer des fonctionnalités avancées, notamment des fonctionnalités créées à l'aide des API CA Identity Manager.
  - **Paramètres de rôles et de tâches**

    Permet d'importer un fichier de définitions de rôles exporté à partir d'un autre environnement CA Identity Manager.
  - **Responsable du système**

    Affecte des rôles de responsable du système.

Procédez comme suit:

1. Si CA Identity Manager utilise un cluster de serveurs de stratégies CA SiteMinder, démarrez un seul serveur de stratégies.
2. Si vous avez un cluster de noeuds CA Identity Manager, démarrez un seul noeud CA Identity Manager.
3. Cliquez sur Environnements.

   La fenêtre d'environnements CA Identity Manager s'affiche et contient une liste d'environnements CA Identity Manager.
4. Cliquez sur le nom de l'environnement CA Identity Manager à modifier.

   La fenêtre Propriétés CA Identity Manager s'affiche et contient les propriétés suivantes :

   ID d'objet

   Définit un identificateur unique pour l'environnement. CA Identity Manager génère cet identificateur lors de la création d'un environnement CA Identity Manager.

   Utilisez l'ID d'objet lors de la configuration de la suppression de tâches d'une base de données de persistance des tâches. Reportez-vous au *Manuel d'installation*.

   Nom

   Spécifie le nom unique de l'environnement CA Identity Manager.

Description

Fournit une description de l'environnement CA Identity Manager.

Annuaire CA Identity Manager

Spécifie l'annuaire CA Identity Manager auquel l'environnement est associé.

Enable Verbose Log Output (Activer la sortie de journal détaillé)

Contrôle la quantité d'informations enregistrées et affichées par CA Identity Manager dans le journal d'environnement lors de l'importation d'un environnement. Le journal de l'environnement est affiché dans la fenêtre de statut de la console de gestion lors de l'importation d'un environnement ou d'autres définitions d'objet d'un fichier.

Remarque : L'activation de cette case à cocher peut affecter de manière significative les performances.

Le journal détaillé inclut des messages de validation et de déploiement pour chaque objet (tâche, fenêtre, rôle et stratégie) et ses attributs dans l'environnement.

Pour consulter le journal détaillé, sélectionnez cette case à cocher et enregistrez les propriétés de l'environnement. Lors de l'importation de rôles ou d'autres paramètres à partir d'un fichier, les informations supplémentaires s'affichent dans le journal.

Serveur de provisionnement

Spécifie l'annuaire de provisionnement utilisé comme référentiel d'utilisateurs de provisionnement.

Pour configurer l'annuaire de provisionnement dans la page des propriétés de provisionnement, cliquez sur la flèche vers la droite.

Version

Permet de définir le numéro de la version de CA Identity Manager.

Adresse de base

Spécifie la partie de l'adresse de CA Identity Manager qui n'inclut pas l'alias protégé ou public de l'environnement.

CA Identity Manager utilise l'adresse de base pour former l'URL de redirection qui pointera vers la tâche de services de mots de passe dans la stratégie de mots de passe par défaut pour l'environnement.

Protected alias (Alias protégé)

Définit le nom de l'adresse de base permettant d'accéder à des tâches protégées dans la console d'utilisateur d'un environnement CA Identity Manager.

Alias public

Définit le nom de l'adresse de base permettant d'accéder à des tâches publiques, telles que des tâches d'auto-enregistrement et de mot de passe oublié.

Public User (Utilisateur public)

Définit le compte d'utilisateur utilisé par CA Identity Manager au lieu des informations d'identification fournies par l'utilisateur pour accéder à des tâches publiques.

Job Timeout (Délai d'expiration de job)

Détermine la durée de l'attente par CA Identity Manager avant l'affichage d'un message de statut après la soumission d'une tâche.

Cette valeur est définie dans la page de console d'utilisateur dans les paramètres avancés.

Statut

Arrête ou redémarre l'environnement CA Identity Manager.

Migrate Task Persistence Data from CA Identity Manager 8.1 (Migration des données de persistance des tâche à partir de CA Identity Manager 8.1)

Migre des données à partir d'une base de données de persistance des tâches CA Identity Manager 8.1 vers la base de données de persistance des tâches CA Identity Manager 12.6.4.

Pour plus d'informations, reportez-vous au *Manuel d'installation*.

Remarque : Le bouton Migrate Task Persistence Data from CA Identity Manager 8.1 (Migration des données de persistance des tâche à partir de CA Identity Manager 8.1) est uniquement visible dans les environnements créés dans des versions précédentes de CA Identity Manager et migrés vers CA Identity Manager 12.6.4.

5. Modifiez la description, l'adresse de base, ou l'alias protégé ou public, si nécessaire.
6. Si vous avez modifié des propriétés de l'environnement, redémarrez l'environnement CA Identity Manager.
7. Si vous avez arrêté des serveurs de stratégies à l'étape 1, redémarrez-les maintenant.

Paramètres d'environnement

Les informations spécifiques de l'environnement sont stockées dans trois fichiers de paramètres d'environnement :

- *alias*_environment_roles.xml
- *alias*_environment_settings.xml
- *alias*_environment.xml

Remarque : *alias* se réfère à l'alias de l'environnement. Spécifiez l'alias lors de la création de l'environnement.

Lors de l'exportation des paramètres d'environnement, générez un fichier .zip contenant ces fichiers, qui reflètent la configuration actuelle.

Une fois les paramètres d'environnement exportés, importez-les pour réaliser l'une des tâches suivantes :

- Gestion de plusieurs environnements avec des paramètres similaires. Dans ce cas, créez un environnement avec les paramètres nécessaires, importez ces paramètres vers d'autres environnements, puis personnalisez-les dans chaque environnement, le cas échéant.
- Migration d'un environnement à partir d'un système de développement vers un système de production
- Mise à jour d'un environnement existant suite à la mise à niveau vers une nouvelle version de CA Identity Manager

Exportation d'un environnement CA Identity Manager

Pour déployer un environnement CA Identity Manager sur un système de production, exportez cet environnement à partir d'un système de développement ou de stockage intermédiaire et importez-le vers le système de production.

Remarque : Lors de l'importation d'un environnement préalablement exporté, CA Identity Manager affiche un journal dans une fenêtre de statut de la console de gestion. Pour consulter des informations de validation et de déploiement pour chaque objet géré et ses attributs dans ce journal, *avant d'exporter* l'environnement, sélectionnez le champ Enable Verbose Log Output (Activer la sortie de journal détaillé) dans la page des propriétés d'environnement. Veillez à ce que ce champ n'entraîne aucun problème de performance significatif lors de l'importation.

Procédez comme suit:

1. Dans la console de gestion, cliquez sur Environnements.

   La fenêtre d'environnements CA Identity Manager s'affiche et contient une liste d'environnements CA Identity Manager.

2. Sélectionnez l'environnement à exporter.
3. Cliquez sur le bouton Exporter.

   Une fenêtre File Download (Téléchargement de fichier) s'affiche.

4. Enregistrez le fichier .zip à un emplacement accessible au système de production.
5. Cliquez sur Terminer.

Les informations de l'environnement sont exportées vers un fichier .zip que vous pouvez importer dans un autre environnement.

Importation d'un environnement CA Identity Manager

Vous pouvez importer des paramètres d'environnement CA Identity Manager pour réaliser l'une des tâches suivantes :

- Gestion de plusieurs environnements avec des paramètres similaires. Dans ce cas, créez un environnement avec les paramètres nécessaires, importez ces paramètres vers d'autres environnements, puis personnalisez-les dans chaque environnement, le cas échéant.
- Migration d'un environnement à partir d'un système de développement vers un système de production
- Mise à jour d'un environnement existant suite à la mise à niveau vers une nouvelle version de CA Identity Manager

Procédez comme suit:

1. Dans la console de gestion, cliquez sur Environnements.

   La fenêtre d'environnements CA Identity Manager s'affiche et contient une liste d'environnements CA Identity Manager.

2. Cliquez sur Importer.

   La fenêtre Import Environment (Importer un environnement) s'affiche.

3. Pour importer un environnement, accédez au fichier .zip requis.

4. Cliquez sur Terminer.

L'environnement est importé dans CA Identity Manager.

Redémarrage d'un environnement CA Identity Manager

Procédez comme suit:

1. Dans la console de gestion, cliquez sur Environnements.

   La fenêtre d'environnements CA Identity Manager s'affiche et contient une liste d'environnements CA Identity Manager.

2. Cliquez sur le nom de l'environnement CA Identity Manager à démarrer.

   La fenêtre Environment Properties (Propriétés d'environnement) CA Identity Manager s'affiche.

3. Sélectionnez l'une des options suivantes.

   Restart Environment (Redémarrer l'environnement)

   Permet d'arrêter et de démarrer un environnement.

   Arrêter

   Permet d'arrêter un environnement en cours d'exécution.

   Démarrer

   Permet de démarrer un environnement non exécuté.

Suppression d'un environnement CA Identity Manager

Utilisez cette procédure pour supprimer un environnement CA Identity Manager.

Remarque : Si CA Identity Manager comprend CA SiteMinder pour l'authentification avancée, il supprimera également le domaine de stratégie CA SiteMinder protégeant l'environnement et les schémas d'authentification par défaut créés pour l'environnement.

Procédez comme suit:

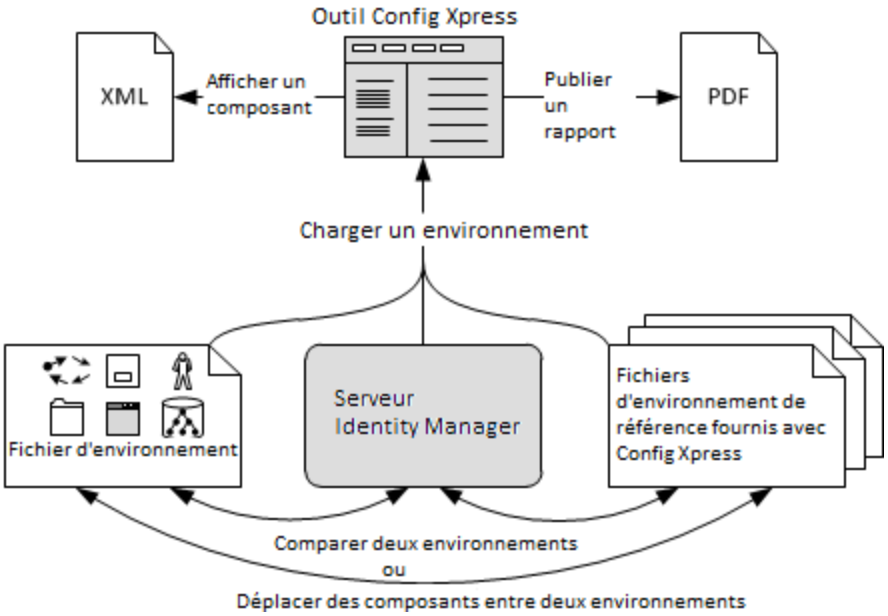
1. Dans la fenêtre Environnements, sélectionnez la case à cocher des environnements CA Identity Manager à supprimer.
2. Cliquez sur Supprimer.

   CA Identity Manager affiche un message de confirmation.
3. Cliquez sur OK pour confirmer la suppression.

Gestion de la configuration

Config Xpress est un outil fourni avec CA Identity Manager. Vous pouvez l'utiliser pour analyser et utiliser les configurations de vos environnements CA Identity Manager.

L'outil permet notamment de déplacer des composants entre des environnements. Config Xpress détecte automatiquement tout autre composant requis et vous invite à les déplacer également. Cette aide peut permettre de gagner du temps et de réduire le risque de problèmes.



Procédez comme suit:

1. Configuration de Config Xpress (page 218)
2. Avant d'utiliser cet outil, chargez un environnement CA Identity Manager (page 219) dans Config Xpress aux fins d'analyse.
3. Utilisez Config Xpress pour effectuer les tâches suivantes avec l'environnement chargé :
   - Déplacement de composants entre des environnements (page 221)
   - Publication d'un rapport PDF des composants système (page 222)
   - Affichage de la configuration XML d'un composant particulier (page 223)

Configuration de Config Xpress

Les fichiers d'installation de Config Xpress sont fournis dans le lecteur d'installation, mais l'outil n'est pas installé.

Voici les configurations logicielles requises de Config Xpress :

- CA Identity Manager r12.0 et versions ultérieures
- Système d'exploitation Windows
- Adobe Air Runtime
- PDF Reader pour l'affichage des rapports

Procédez comme suit:

1. Téléchargez Adobe Air Runtime à partir de l'adresse suivante http://get.adobe.com/air, puis installez-le.
2. Vérifiez que les outils d'administration sont installés.
3. Recherchez le fichier d'installation de Config Xpress à l'emplacement suivant :

   ```
   C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\ConfigXpress
   ```

4. Pour installer Config Xpress, exécutez Config Xpress.air.
5. A l'issue de l'installation, Config Xpress démarre.

Chargement d'un environnement dans Config Xpress

Pour utiliser Config Xpress, chargez un ou plusieurs environnements dans l'outil. Cette tâche permet de travailler avec l'environnement dans Config Xpress.

Vous pouvez charger un environnement dans Config Xpress directement à partir d'un serveur CA Identity Manager actif, ou à partir d'un fichier d'environnement. Si vous utilisez l'un des fichiers d'environnement de référence installés avec Config Xpress, vous pouvez comparer votre environnement à la configuration prête à l'emploi.

Le processus de chargement d'un environnement peut prendre quelques minutes.

Procédez comme suit:

1. Ouvrez Config Xpress.
2. Pour charger un environnement **actif** directement à partir d'un serveur CA Identity Manager :
   a. Cliquez sur l'onglet Serveur (Réseau).
   b. Saisissez le nom et le port du serveur CA Identity Manager. Exemple :

      ```
      servername.ca.com:8080
      ```

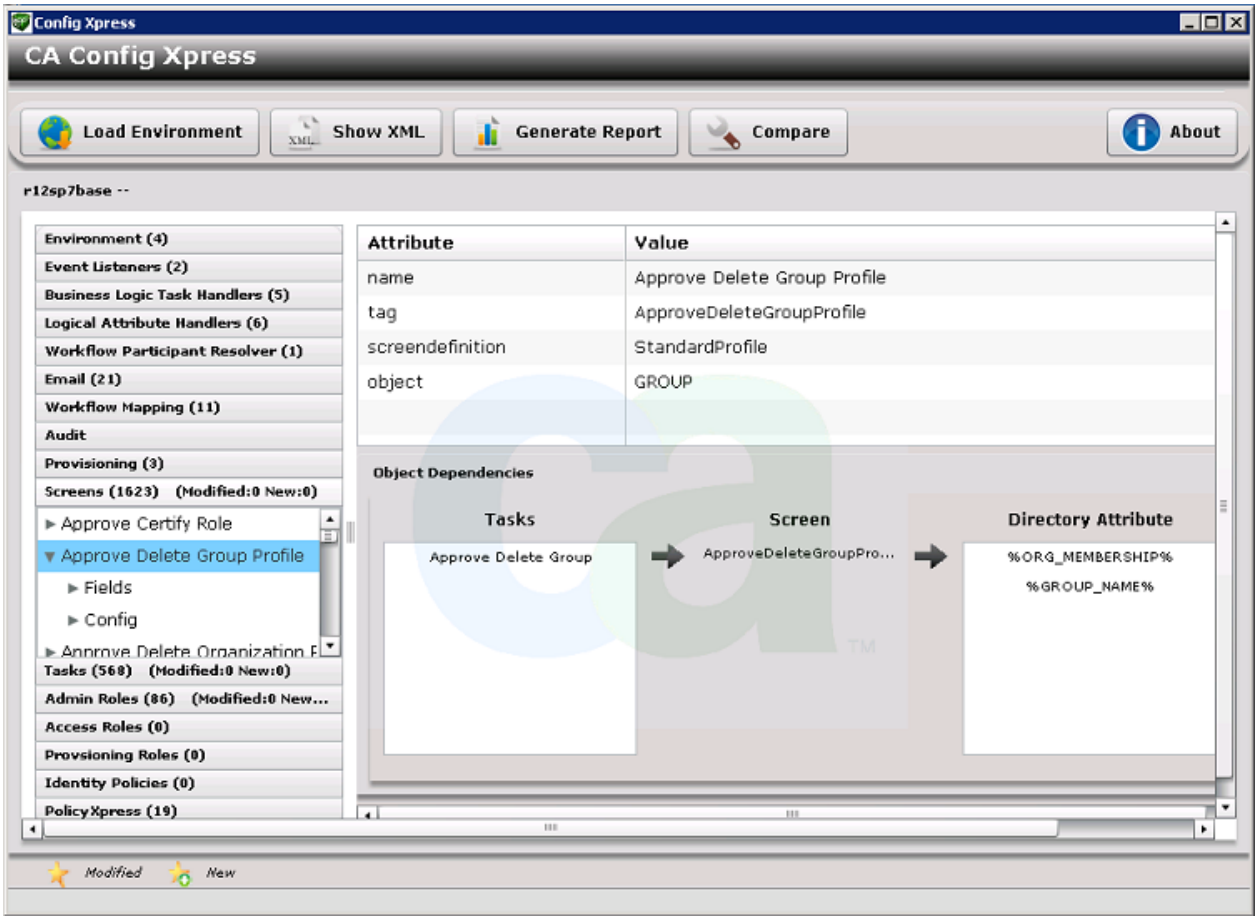
   c. Si votre serveur est configuré pour autoriser HTTPS uniquement, sélectionnez Utiliser le protocole HTTPS.
   d. Si la version du serveur est antérieure à r12.5 SP6, sélectionnez 12.5 SP7.
   e. Cliquez sur Se connecter.
   f. Sélectionnez un environnement dans la liste *Choose Environment to load (Sélectionner un environnement à charger)*, puis cliquez sur Charger.
3. Pour charger un **fichier d'environnement** exporté à partir de votre environnement CA Identity Manager :
   a. Exportez un environnement CA Identity Manager.
   b. Dans Config Xpress, cliquez sur l'onglet File System (Système de fichiers).
   c. Sélectionnez la version, puis recherchez le fichier de l'environnement et cliquez sur Charger.
4. Pour charger un **fichier d'environnement de référence** installé avec Config Xpress :
   a. Cliquez sur l'onglet Base Versions (Versions de base).
   b. Sélectionnez la version nécessaire, puis cliquez sur Sélectionner.

Config Xpress analyse l'environnement, puis affiche ses détails.

Vous pouvez ensuite publier certains ou tous les détails de l'environnement au format PDF (page 222) ou XML (page 223). Si vous chargez un deuxième environnement, vous pouvez les comparer et déplacer des composants (page 221) entre eux.

Exemple : Config Xpress suite au chargement d'un fichier de configuration de référence

Cette capture d'écran illustre l'affichage d'objets dépendants par Config Xpress :



Déplacement d'un composant d'un environnement à un autre

Sans Config Xpress, la tâche de déplacement de composants entre différentes zones de stockage intermédiaires est complexe et est susceptible d'échouer.

Lorsque vous utilisez Config Xpress pour déplacer des composants, l'outil déplace également tous les objets requis. Par exemple, si vous déplacez une tâche qui requiert une fenêtre, Config Xpress vous demande si vous voulez sélectionner les composants requis également. Config Xpress comprend que la tâche utilise cette fenêtre et qu'elle doit également être déplacée vers l'environnement cible.

Si vous voulez déplacer un composant vers un environnement actif, Config Xpress le charge immédiatement. Si vous voulez déplacer le composant vers un fichier d'environnement, enregistrez-le en tant que fichier XML, puis importez ce fichier dans l'environnement.

Procédez comme suit:

1. Chargez l'environnement qui contient le composant que vous voulez déplacer.
2. Comparez cet environnement avec un deuxième :
   a. Cliquez sur Compare (Comparer).
   b. Chargez l'environnement cible.

      Config Xpress affiche une liste des différences entre les deux environnements.
3. Dans cette liste de différences, recherchez un composant que vous voulez déplacer. Vous pouvez cliquer sur la colonne Nom pour trier la liste.
4. Pour chaque composant, suivez la procédure suivante :
   a. Sélectionnez l'élément dans la colonne Action.

      Config Xpress analyse le composant, ce qui peut prendre quelques minutes.
   b. Si le composant a des composants dépendants, la zone Add Modified Dependant Screens (Ajouter des fenêtres dépendantes modifiées) s'affiche. Pour continuer, cliquez sur Oui ou Non.

   Lorsque vous avez sélectionné tous les composants que vous voulez déplacer, vous pouvez déplacer les composants mis à jour.
5. Si vous déplacez les composants vers un serveur actif, cliquez sur Upload To (Charger vers).

   Les composants sont immédiatement déplacés.
6. Si vous déplacez les composants vers un fichier d'environnement :
   a. Cliquez sur Enregistrer.
   b. Saisissez un nom de fichier, puis cliquez sur Enregistrer à nouveau.

Config Xpress enregistre tous les composants sélectionnés dans un fichier XML. Vous pouvez maintenant importer ce fichier XML dans l'environnement cible en cours.

Publication d'un rapport PDF

Config Xpress peut générer un rapport qui indique l'état actuel d'un environnement CA Identity Manager. Vous pouvez utiliser ce rapport pour prendre un cliché d'un environnement de production. Lorsque vous générez ce rapport, décidez d'inclure la configuration complète, ou les modifications apportées depuis l'installation uniquement.

Ce rapport est utile à titre de référence ultérieure ou dans le cadre d'un plan de récupération de système.

Procédez comme suit:

1. Chargez un environnement dans Config Xpress.
2. Cliquez sur Generate Report (Générer le rapport).

   Dans la boîte de dialogue Generate PDF Report (Générer le rapport PDF), vous pouvez changer la taille de police et saisir le texte des pages de titre ou de garde. Décidez également d'inclure tous les éléments de configuration, ou les éléments nouveaux ou modifiés uniquement.

   Important : Si vous ne cliquez pas dans la zone *Only include details of new or modified tasks, screens, roles (Inclure uniquement les détails des tâches, fenêtres et rôles nouveaux ou modifiés)* le rapport contiendra l'environnement complet. Le fichier PDF contiendra environ 2 000 pages et plus de 40 Mo.
3. Cliquez sur OK.
4. Saisissez un nom de fichier, puis enregistrez le rapport. L'enregistrement peut prendre quelques minutes ou plus longtemps si vous avez choisi de publier l'environnement complet.

   Le rapport s'ouvre dans PDF Reader.

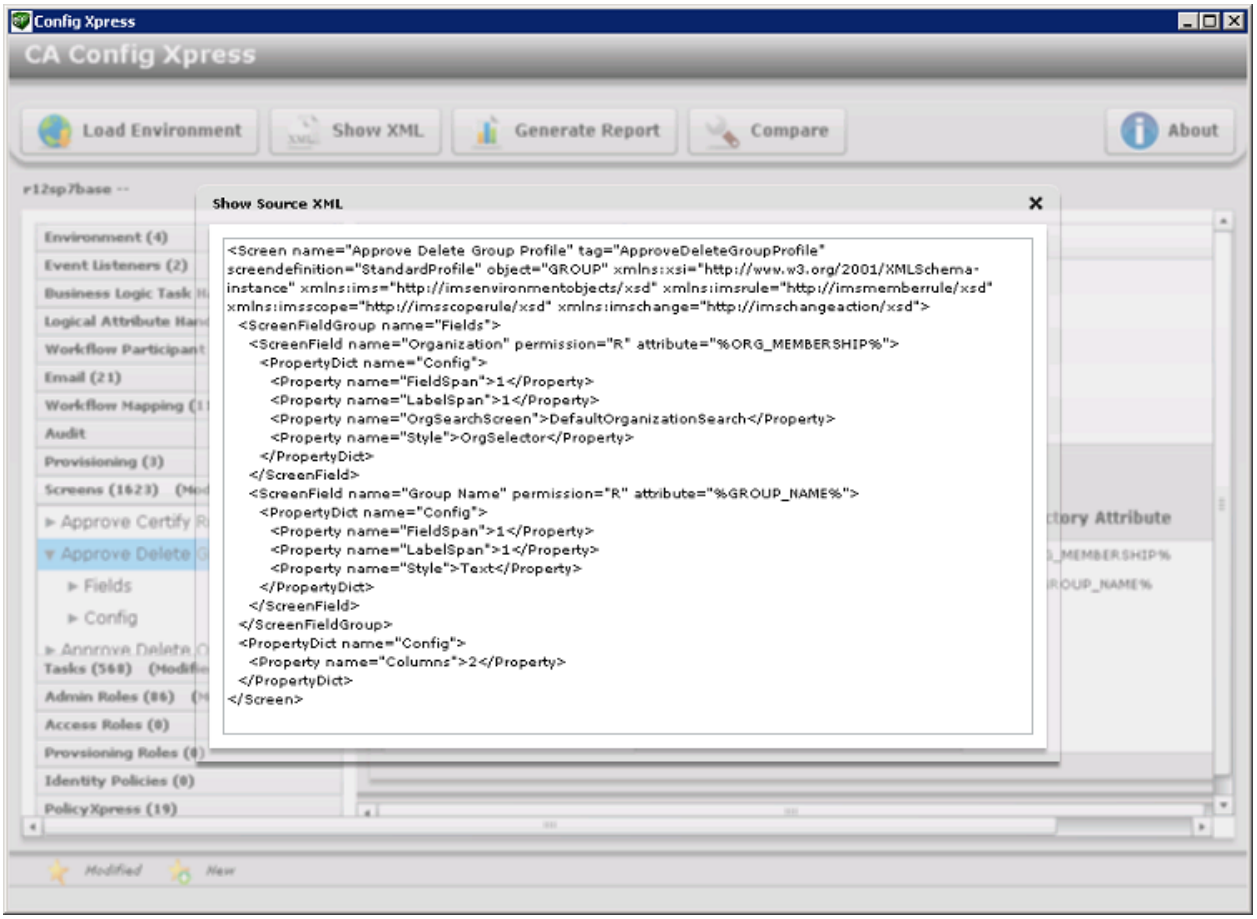
Affichage de la configuration XML

Config Xpress peut afficher la configuration XML d'un composant particulier. Vous pouvez étudier ce fichier XML pour comprendre un système.

Procédez comme suit:

1. Chargez un environnement dans Config Xpress.
2. Dans la fenêtre Config Xpress, cliquez sur un composant.
3. Cliquez sur le bouton "Show XML" (afficher le format des objets de gestion).

   La page de configuration XML apparaît :



Optimisation de l'évaluation de règle de stratégie

Les règles de stratégie, qui identifient de façon dynamique un ensemble d'utilisateurs, sont utilisées dans l'évaluation des stratégies de membre avec rôle, d'administration, de propriété et d'identité. L'évaluation de ces règles peut prendre un temps considérable dans le cas d'implémentations CA Identity Manager étendues.

Remarque : Pour plus d'informations sur les stratégies de membre, d'administration, de propriété et d'identité, consultez le *Manuel d'administration*.

Pour réduire le temps d'évaluation des règles comprenant des attributs d'utilisateur, vous pouvez activer l'option d'évaluation en mémoire. Lorsque l'option d'évaluation de mémoire est activée, CA Identity Manager récupère des informations sur un utilisateur à évaluer à partir du référentiel d'utilisateurs et enregistre une représentation de celui-ci dans la mémoire. CA Identity Manager utilise la représentation de mémoire pour comparer les valeurs d'attribut par rapport aux règles de stratégie. Cela limite le nombre d'appels effectués directement par CA Identity Manager au référentiel d'utilisateurs.

Activez l'option d'évaluation de mémoire pour un environnement dans la console de gestion.

Procédez comme suit:

1. Ouvrez la console de gestion.
2. Sélectionnez Environnements, *Environment Name (Nom de l'environnement)*, Paramètres avancés (Advanced Settings), Divers.

   La page User Defined Properties (Propriétés définies par l'utilisateur) s'ouvre.
3. Dans le champ Propriété, saisissez le texte suivant :

   UseInMemoryEvaluation
4. Dans le champ Valeur, saisissez l'*un* des nombres suivants :

   0

   In-memory evaluation is disabled (L'évaluation de mémoire est désactivée.).

   1

   In-memory evaluation is enabled (L'évaluation de mémoire est activée.). Si cette option est spécifiée, la comparaison d'attribut respecte la casse.

   3

   In-memory evaluation is enabled (L'évaluation de mémoire est activée.). Si cette option est spécifiée, la comparaison d'attribut ne respecte pas la casse.
5. Cliquez sur Ajouter.

   CA Identity Manager ajoute la nouvelle propriété à la liste des propriétés existantes de l'environnement.
6. Cliquez sur Enregistrer.

Paramètres de rôles et de tâches

Dans la fenêtre Role and Task Settings (Paramètres de rôles et de tâches) de la console de gestion, vous pouvez importer ou exporter des paramètres de fenêtre, d'onglet, de rôle et de tâche dans un fichier XML, appelé fichier de définitions de rôles. CA Identity Manager fournit des fichiers de définitions de rôles prédéfinis qui créent des fenêtres, des onglets, des rôles et des tâches pour un ensemble de fonctionnalités. Par exemple, un fichier de définitions de rôles prend en charge le provisionnement intelligent et d'autres fichiers prennent en charge des fenêtres de gestion des terminaux.

De plus, vous pouvez utiliser un fichier de définitions de rôles pour appliquer les paramètres d'un environnement à plusieurs autres environnements. Effectuez les étapes suivantes :

- Configurez des paramètres de fenêtre, d'onglet, de tâche et de rôle dans un environnement.
- Exportez ces paramètres dans un fichier XML.
- Importez le fichier XML vers l'environnement requis.

Exportation des paramètres de rôles et de tâches

Pour exporter des paramètres de rôles et tâches, suivez la procédure suivante.

Procédez comme suit:

1. Dans la console de gestion, cliquez sur Environnements.

   Une liste d'environnements CA Identity Manager s'affiche.

2. Cliquez sur le nom de l'environnement CA Identity Manager approprié.

   La fenêtre Propriétés pour cet environnement s'affiche.

3. Cliquez sur Role and Task Settings (Paramètres de rôles et de tâches), puis sur Exporter.

4. Cliquez sur Ouvrir pour afficher le fichier dans une fenêtre de navigateur ou sur Enregistrer pour enregistrer les paramètres dans un fichier XML.

Importation des paramètres de rôles et de tâches

Les paramètres de rôles et de tâches sont définis dans des fichiers XML, appelés fichiers de définitions de rôles. Vous pouvez importer des fichiers de définitions de rôles prédéfinis pour prendre en charge des définitions spécifiques de fonctionnalité CA Identity Manager (par exemple, provisionnement intelligent) ou des fichiers de définitions de rôles d'un environnement à un autre.

Remarque : Vous pouvez également importer des définitions de rôles pour des connecteurs personnalisés créés avec Connector Xpress. Créez ces fichiers de définitions de rôles à l'aide du générateur de définitions des rôles. Pour plus d'informations, reportez-vous au *Manuel de Connector Xpress*.

Pour importer des paramètres de rôles et tâches, suivez la procédure suivante.

Procédez comme suit:

1. Dans la console de gestion, cliquez sur Environnements.

   Une liste d'environnements CA Identity Manager s'affiche.

2. Cliquez sur le nom de l'environnement CA Identity Manager dans lequel vous voulez importer les paramètres de rôles et tâches.

   La fenêtre Propriétés pour cet environnement s'affiche.

3. Cliquez sur Role and Task Settings (Paramètres de rôles et de tâches), puis sur Importer.

4. Effectuez l'une des actions suivantes :

   - Sélectionnez un ou plusieurs fichiers de définitions de rôles pour créer des rôles et des tâches par défaut pour l'environnement.

     Pour sélectionner tous les fichiers de définitions de rôles disponibles, cliquez sur Select/Deselect All (Tout sélectionner/désélectionner).

   - Saisissez le chemin d'accès et le nom du fichier de définitions de rôles à importer ou recherchez le fichier. Puis, cliquez sur Terminer.

5. Cliquez sur Terminer.

   Le statut est affiché dans la fenêtre Role Configuration Output (Résultat de la configuration de rôle).

6. Cliquez sur Continuer pour sortir.

Création de rôles et de tâches pour des terminaux dynamiques

A l'aide de Connector Xpress, vous pouvez configurer des connecteurs dynamiques pour permettre le provisionnement et la gestion des bases de données SQL et des annuaires LDAP. Pour chaque connecteur dynamique, vous pouvez utiliser le générateur de définitions des rôles pour créer des définitions de tâches et de fenêtres pour des fenêtres de gestion de comptes qui s'affichent dans la console d'utilisateur.

Après avoir exécuté le générateur de définitions des rôles, importez le fichier de définitions de rôles résultant (page 226) dans la console de gestion.

Remarque : Pour plus d'informations sur le générateur de définitions des rôles, consultez le *Manuel de Connector Xpress*.

Modification du compte du responsable du système

Un responsable du système doit configurer et maintenir un environnement CA Identity Manager. Généralement, les tâches d'un responsable du système sont les suivantes :

- Création et gestion de l'environnement initial
- Création et modification des rôles d'administration
- Création et modification d'autres comptes d'administrateur

Créez un compte de responsable du système lors de la création d'un environnement CA Identity Manager. Si ce compte est verrouillé, par exemple, si le responsable du système oublie le mot de passe, vous pouvez le recréer à l'aide de l'assistant du responsable du système.

L'assistant responsable du système vous oriente dans les étapes pour affecter un rôle de gestion de système à un utilisateur.

Avant de modifier le compte du responsable du système, tenez compte des points suivants :

- Veillez à utiliser un référentiel d'utilisateurs LDAP et à configurer un conteneur d'utilisateurs comme ou=People dans le fichier de configuration d'annuaire (directory.xml) pour votre annuaire CA Identity Manager. Les utilisateurs sélectionnés doivent exister dans le même conteneur dans lequel vous configurez le responsable du système. La sélection d'un compte d'utilisateur qui n'existe pas dans le conteneur d'utilisateurs peut entraîner des échecs.
- Lorsque l'environnement CA Identity Manager gère un annuaire d'utilisateurs avec une structure d'utilisateur hiérarchique ou non hiérarchique, le profil de l'utilisateur sélectionné doit également inclure l'organisation. Pour assurer la correcte configuration du profil d'un utilisateur, ajoutez le nom de son organisation à l'attribut physique correspondant à l'attribut connu %ORG_MEMBERSHIP% dans le fichier directory (page 86).xml. Par exemple, lorsque la description de l'attribut physique est mappée vers l'attribut connu %ORG_MEMBERSHIP% dans le fichier directory.xml et que l'utilisateur appartient à l'organisation Employés, le profil de l'utilisateur doit contenir la paire attribut/valeur description=Employees.

Procédez comme suit:

1. Dans la fenêtre d'environnements CA Identity Manager, cliquez sur le nom de l'environnement CA Identity Manager approprié.

   Les propriétés de cet environnement s'affichent.

2. Cliquez sur System Manager (Responsable du système).

   L'assistant de responsable du système s'affiche.

3. Saisissez le nom unique de l'utilisateur disposant du rôle de responsable du système comme suit :

   - Pour des utilisateurs de base de données relationnelles, saisissez l'identificateur unique ou la valeur mappée vers l'attribut connu %USER_ID% dans le fichier de configuration d'annuaire.
   - Pour des utilisateurs LDAP, saisissez le nom unique relatif de l'utilisateur. Par exemple, si le nom unique de l'utilisateur est uid=Admin1, ou=People, ou=Employees, ou=NeteAuto, saisissez Admin1.

   Remarque : Veillez à ce que le responsable du système soit *différent* de l'administrateur du référentiel d'utilisateurs.

4. Pour afficher l'identificateur complet de l'utilisateur, cliquez sur Valider.

5. Cliquez sur Suivant.

6. Dans la deuxième page de l'assistant, sélectionnez un rôle à affecter à l'utilisateur comme suit :
   - Si vous voulez affecter le rôle de responsable du système, effectuez les tâches suivantes :
     a. Sélectionnez le bouton radio près du rôle de responsable du système.
     b. Cliquez sur Terminer.
   - Si vous voulez affecter un rôle différent du responsable du système, effectuez les tâches suivantes :
     a. Sélectionnez une condition dans la première liste.
     b. Saisissez un nom de rôle partiel ou complet ou un astérisque (*) dans la deuxième zone de liste. Cliquez sur Rechercher.
     c. Dans la liste des résultats de la recherche, sélectionnez le rôle à affecter.
     d. Cliquez sur Terminer.

   La fenêtre System Manager Configuration Output (Résultat de la configuration du responsable du système) affiche les informations sur le statut.
7. Pour fermer l'assistant de responsable du système, cliquez sur Continuer.

Accès au statut d'un environnement CA Identity Manager

CA Identity Manager inclut une page de statut que vous pouvez utiliser pour vérifier le statut suivant :

- L'annuaire CA Identity Manager est chargé correctement.
- CA Identity Manager peut se connecter au référentiel d'utilisateurs.
- L'environnement CA Identity Manager se charge correctement.

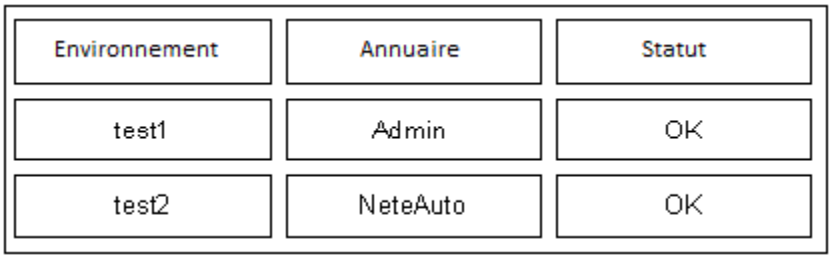
Pour accéder à la page de statut, saisissez l'URL suivante dans un navigateur :

`http://nomhôte/iam/im/status.jsp`

hostname

Définit le nom de domaine complet du serveur sur lequel CA Identity Manager est installé. Par exemple : myserver.mycompany.com

Si l'environnement CA Identity Manager démarre correctement et que toutes les connexions s'exécutent correctement, la page de statut sera similaire à l'illustration suivante :



La page de statut indique également si l'environnement est conforme à la norme FIPS 140-2.

Dépannage d'environnements CA Identity Manager

Le tableau suivant décrit des messages d'erreur possibles et le processus de dépannage :

Message	Description	Dépannage
Non chargé	L'annuaire CA Identity Manager associé à l'environnement n'a pas été chargé lors du démarrage de CA Identity Manager.	1. Vérifiez que le référentiel d'utilisateurs est en cours d'exécution. Si CA Identity Manager comprend CA SiteMinder, vérifier que CA SiteMinder peut se connecter au référentiel d'utilisateurs.
Not OK (Echec)	CA Identity Manager ne peut pas se connecter à l'annuaire CA Identity Manager.	Dans l'interface utilisateur du serveur de stratégies, pour vérifier la connexion, ouvrez la page des propriétés pour la connexion au référentiel d'utilisateurs CA SiteMinder associé au référentiel d'utilisateurs et cliquez sur le bouton Afficher le contenu. Si vous pouvez afficher le contenu du référentiel d'utilisateurs, CA SiteMinder peut se connecter correctement. Pour plus d'informations sur le serveur de stratégies, consultez le *Manuel de configuration du serveur de stratégies gestionnaire d'accès au Web de CA SiteMinder*. 2. Redémarrez CA Identity Manager et le serveur de stratégies.

Message	Description	Dépannage
SM connection is not OK (La connexion SM n'est pas établie).	CA Identity Manager ne peut pas se connecter au serveur de stratégies CA SiteMinder (dans le cas d'implémentations qui incluent CA SiteMinder).	1. Vérifiez les conditions suivantes : ■ Le serveur de stratégies est en cours d'exécution. ■ L'agent Web protège des ressources. Vous pouvez vérifier que l'agent Web est correctement exécuté en accédant à l'interface utilisateur du serveur de stratégies. Si vous êtes invité à fournir des informations d'identification, l'agent Web fonctionne correctement. 2. Redémarrez CA Identity Manager et le serveur de stratégies.
IMS is not available now (IMS est indisponible.)	Une erreur s'est produite dans CA Identity Manager.	Pour obtenir des détails de l'erreur, consultez le journal du serveur d'applications.
Message d'erreur Windows 500	La page de statut ne s'affiche pas si vous tentez d'y accéder lors de la suppression de la connectivité avec l'annuaire d'utilisateurs LDAP.	Pour afficher la page de statut, désactivez l'option du navigateur Internet Show friendly error message (Afficher le message d'erreur simplifié).

Chapitre 7: Paramètres avancés

La fenêtre Advanced Settings (Paramètres avancés) dans la console de gestion vous permet d'effectuer les configurations suivantes :

- Accéder aux fenêtres pour configurer les paramètres avancés
- Importer et exporter les paramètres avancés, tel que décrit dans la rubrique Importation/exportation de paramètres avancés (page 248).

Ce chapitre traite des sujets suivants :

Audit

Les journaux d'audit conservent les enregistrements des opérations effectuées dans un environnement CA Identity Manager. Vous pouvez utiliser les données de ces journaux pour surveiller l'activité du système.

CA Identity Manager audite les *événements*. Un événement est une opération générée par une tâche CA Identity Manager. Une tâche peut générer plusieurs événements. Par exemple, la tâche CreateUser peut générer les événements CreateUserEvent et AddToGroupEvent.

Par défaut, CA Identity Manager exporte toutes les informations d'événement dans la base de données d'audit. Pour contrôler le type et la quantité d'informations d'événement enregistrées par CA Identity Manager, effectuez les tâches suivantes :

- Activez l'audit pour les tâches d'administration de CA Identity Manager.
- Activez l'audit pour les événements CA Identity Manager générés par les tâches d'administration.
- Enregistrez les informations d'événement correspondant à un état, par exemple, lorsqu'un événement se termine ou est annulé.
- Journalisez les informations sur les attributs impliqués dans un événement. Par exemple, vous pouvez journaliser les attributs modifiés au cours d'un événement ModifyUserEvent.
- Définissez le niveau d'audit pour les événements et les attributs.

Gestionnaires de tâches métier (GTM)

Un gestionnaire de tâches métier exécute une logique métier personnalisée avant la soumission d'une tâche CA Identity Manager pour traitement. En général, la logique métier personnalisée valide les données. Par exemple, un gestionnaire de tâches métier peut vérifier la limite d'appartenance d'un groupe avant que CA Identity Manager y ajoute un membre. Lorsque la limite d'appartenance au groupe est atteinte, le gestionnaire de tâches métier affiche un message informant l'administrateur de groupe que l'ajout d'un nouveau membre est impossible.

Vous pouvez utiliser les gestionnaires de tâches métier prédéfinis ou vous pouvez créer des gestionnaires personnalisés à l'aide de l'API de gestionnaire de tâches métier.

Remarque : Pour plus d'informations sur la création de logique métier personnalisée, consultez le manuel *Programming Guide for Java*.

La fenêtre Gestionnaires de tâches métier (GTM) contient une liste des gestionnaires de tâches métier globaux existants. Cette liste comprend les gestionnaires prédéfinis fournis avec CA Identity Manager, ainsi que les gestionnaires personnalisés définis sur votre site. CA Identity Manager exécute les gestionnaires selon l'ordre spécifié dans la liste.

Vous pouvez implémenter des gestionnaires de tâches métier globaux uniquement dans Java.

Effacement automatique des champs de mot de passe via la tâche de réinitialisation de mot de passe d'utilisateur

Vous pouvez configurer CA Identity Manager pour effacer automatiquement les champs de mot de passe lorsqu'une valeur préalablement entrée enfreint une stratégie de mot de passe ou lorsque les valeurs des champs Mot de passe et Confirmer le mot de passe ne correspondent pas.

Procédez comme suit:

1. Démarrez la console de gestion.
2. Sélectionnez l'environnement à gérer, puis cliquez sur Advanced Settings (Paramètres avancés).

   La page des paramètres avancés s'affiche.
3. Cliquez sur Business Logic Task Handlers (Gestionnaires de tâches métier), BlthPasswordServices.

   La page Business Logic Handler Properties (Propriétés du gestionnaire de tâches métier) s'affiche.
4. Créez les propriétés suivantes :

   ClearPwdIfInvalid=true

   PwdConfirmAttrName=|passwordConfirm|
5. Vérifiez que les paramètres de ConfirmPasswordHandler sont les suivants :
   - Object type – User
   - Class – ConfirmPasswordHandler
   - ConfirmationAttributeName = |passwordConfirm|
   - OldPasswordAttributeName = |oldPassword|
   - passwordAttributeName = %PASSWORD%

   Les utilisateurs peuvent désormais effacer les champs de mot de passe dans la tâche de réinitialisation de mot de passe d'utilisateur.

Liste des événements

Les tâches d'administration incluent des *événements*, actions qu'CA Identity Manager effectue pour réaliser la tâche. Une tâche peut inclure plusieurs événements. Par exemple, la tâche Créer un utilisateur peut inclure des événements qui créent le profil de l'utilisateur, ajoutent l'utilisateur à un groupe et affectent des rôles.

CA Identity Manager audite les événements, applique les règles métier spécifiques au client associées aux événements et requiert l'approbation des événements lorsque ces derniers sont mappés aux processus de flux de travaux.

Utilisez cette page pour afficher la liste des événements disponibles dans CA Identity Manager.

Notifications par courriel

CA Identity Manager peut envoyer des notifications par courriel lorsqu'une tâche ou un événement se termine, ou lorsqu'un événement placé sous le contrôle du flux de travaux atteint un état spécifique. Par exemple, un courriel peut informer un approbateur qu'un événement requiert son approbation.

Pour spécifier le contenu des notifications par courriel, vous pouvez utiliser des modèles de courriel prédéfinis ou personnaliser des modèles en fonction de vos besoins.

La console de gestion vous permet d'effectuer les tâches suivantes :

- Activer les notifications par courriel pour un environnement CA Identity Manager.
- Spécifier les ensembles de modèles pour créer des courriels.
- Indiquer les événements et les tâches pour lesquelles les notifications par courriel sont envoyées.

Ecouteurs d'événements

Une tâche CA Identity Manager est constituée d'une ou de plusieurs actions, également nommées événements, que CA Identity Manager effectue au cours de l'exécution de la tâche. Par exemple, la tâche Créer un utilisateur peut inclure les événements suivants :

- CreateUserEvent : crée un profil d'utilisateur dans une organisation.
- AddToGroupEvent (facultatif) : ajoute l'utilisateur en tant que membre d'un groupe.
- AssignAccessRole (facultatif) : affecte un rôle d'accès à l'utilisateur.

Un *écouteur d'événements* recherche un certain type d'événement, puis exécute la logique métier personnalisée à un point du cycle de vie de l'événement. Par exemple, après la création d'un utilisateur dans CA Identity Manager, un écouteur d'événements peut ajouter ses informations à une base de données d'une autre application.

Remarque : Pour en savoir plus sur les écouteurs d'événements, consultez le manuel *Programming Guide for Java*.

Stratégies d'identité

Une stratégie d'identité applique un ensemble de modifications métier aux utilisateurs qui remplissent certaines règles ou conditions. Vous pouvez utiliser des stratégies d'identité pour effectuer les tâches suivantes :

- Automatiser certaines tâches de gestion d'identité, telles que l'affectation de rôles, d'appartenances à un groupe ou de ressources, ou encore la modification d'attributs de profils d'utilisateurs).
- Appliquer la séparation des fonctions. Par exemple, vous pouvez créer une stratégie d'identité qui interdit aux membres du rôle Signataire de chèque de disposer du rôle Approbateur de chèque.
- Appliquer la conformité. Par exemple, vous pouvez effectuer un audit sur les utilisateurs disposant d'un certain titre et générant plus de 100 000 euros.

Vous créez et gérez les ensembles de stratégies d'identité à partir de la console d'utilisateur. Pour plus d'informations sur les stratégies d'identité, reportez-vous au *Manuel d'administration*.

Avant d'utiliser des stratégies d'identité, effectuez les tâches suivantes à partir de la console de gestion :

- Activez les stratégies d'identité pour un environnement CA Identity Manager.
- Définissez le niveau de traitement récursif (facultatif).

Gestionnaires d'attributs logiques

Les attributs logiques de CA Identity Manager permettent d'afficher les attributs de référentiel d'utilisateurs appelés *attributs physiques* dans un format convivial, dans des fenêtres de tâche. Les administrateurs de CA Identity Manager utilisent les fenêtres de tâches pour exécuter des fonctions dans CA Identity Manager.

Les attributs logiques n'existent pas dans un référentiel d'utilisateurs. En général, ils représentent un ou plusieurs attributs physiques pour simplifier la présentation. Par exemple, l'attribut logique *date* peut représenter les attributs physiques *month*, *day* et *year*.

Les attributs logiques sont traités par des attributs logiques constitués d'objets Java écrits à l'aide de l'API d'attribut logique. Par exemple, lorsqu'une fenêtre de tâche s'affiche, un gestionnaire d'attributs logiques peut convertir des données d'attributs physiques provenant du référentiel d'utilisateurs en données d'attributs logiques.

Vous pouvez utiliser des attributs logiques prédéfinis et les gestionnaires d'attributs logiques inclus dans CA Identity Manager, ou en créer de nouveaux à l'aide de l'API d'attribut logique.

Remarque : Pour plus d'informations, reportez-vous au manuel *Programming Guide for Java*.

Divers

Les propriétés définies par l'utilisateur dans cette fenêtre s'appliquent à l'environnement CA Identity Manager entier. Ils sont transférés sous la forme de paires nom/valeur à la méthode init() de tous les objets Java personnalisés que vous créez avec les API CA Identity Manager. Un objet personnalisé peut utiliser ces données selon les modalités requises par la logique métier de l'objet.

Ces propriétés sont également définies pour un objet personnalisé particulier. Par exemple, supposez que les propriétés définies par l'utilisateur sont définies dans la fenêtre Propriétés pour l'écouteur d'événements MyListener. Les propriétés définies par l'utilisateur pour un objet et les propriétés d'environnement définies dans les fenêtres Divers sont transférées à MyListener.init() dans un appel unique.

Pour ajouter une propriété définie par l'utilisateur, spécifiez une valeur et un nom de propriété, puis cliquez sur Ajouter.

Pour supprimer une ou plusieurs propriétés définies par l'utilisateur, cochez la case à côté de chaque paire nom/valeur à supprimer, puis cliquez sur Supprimer.

Une fois que vous avez apporté les modifications appropriées, cliquez sur Enregistrer. Redémarrez le serveur d'applications pour appliquer les modifications.

Remarque : Toutes les propriétés diverses doivent respecter la casse. Par conséquent, si vous définissez une propriété SelfRegistrationLogoutUrl et une propriété selfregistrationlogouturl, les deux propriétés sont ajoutées.

Règles de notification

Les règles de notification déterminent les destinataires des notifications par courriel. Lorsqu'une tâche se termine ou qu'un événement dans une tâche atteint un certain état (En attente d'approbation, Approuvé ou Rejeté), les utilisateurs reçoivent une notification par courriel en fonction de la règle de notification.

Remarque : Pour plus d'informations sur les fonctionnalités de notification par courriel, consultez le *Manuel d'administration*.

CA Identity Manager inclut les règles de notification prédéfinies suivantes :

ADMIN_ADAPTER

Envoie un courriel à l'administrateur qui initialise la tâche.

USER_ADAPTER

Envoie un courriel à l'utilisateur affecté par la tâche.

USER_MANAGER

Envoie un courriel au responsable de l'utilisateur dans le contexte actuel.

Pour créer des règles de notification personnalisées, utilisez l'API de création de règles de notification.

Remarque : Pour en savoir plus sur les règles de notification, reportez-vous au manuel *Programming Guide for Java*.

Sélecteurs d'organisation

Un sélecteur d'organisation est un gestionnaire d'attributs logiques personnalisés qui détermine l'emplacement dans lequel CA Identity Manager crée le profil d'un utilisateur auto-enregistré, selon les informations fournies pendant cet enregistrement. Par exemple, le profil pour les utilisateurs qui fournissent un code promotionnel lorsqu'ils s'inscrivent peut être ajouté à une organisation Utilisateurs de promotion.

Provisionnement

Utilisez cette fenêtre lorsque vous utilisez CA Identity Manager pour le provisionnement.

Remarque : Pour obtenir une procédure plus détaillée, consultez la section traitant de la Procédure de configuration d'un environnement CA Identity Manager pour le provisionnement (page 197).

Les options de provisionnement sont les suivantes :

Activé

Spécifie l'utilisation de deux référentiels d'utilisateurs : un pour CA Identity Manager et un référentiel d'utilisateurs distinct appelé Annuaire de provisionnement pour provisionner les comptes. Si cette option est désactivée, seul le référentiel d'utilisateurs CA Identity Manager est utilisé.

Use Session Pool (Utiliser un pool de sessions)

Active l'utilisation d'un pool de sessions.

Session Pool Initial Sessions (Sessions initiales du pool de sessions)

Définit le nombre de sessions minimum qui sont disponibles dans le pool au démarrage.

Valeur par défaut : 8

Session Pool Maximum Sessions (Nombre maximum de sessions du pool de sessions)

Définit le nombre maximum de sessions dans le pool.

Valeur par défaut : 32

Enable Password Changes (Activer les modifications de mot de passe) sous Endpoint Accounts (Comptes de terminal)

Définit la configuration de Enable Password Synchronization Agent (Activer l'agent de synchronisation de mots de passe pour chaque utilisateur) dans le serveur de provisionnement. Cette option permet la synchronisation des mots de passe entre les utilisateurs CA Identity Manager et les comptes de terminal associés.

Enable Accumulation of Provisioning Role Membership Events (Activer l'accumulation des événements d'appartenance à un rôle de provisionnement)

Si vous cochez cette case, CA Identity Manager exécute les événements associés à l'appartenance d'un rôle de provisionnement dans un ordre spécifique. Toutes les actions Ajouter sont combinées en une seule opération et envoyées au serveur de provisionnement pour traitement. Une fois le traitement des actions Ajouter terminé, CA Identity Manager combine les actions Supprimer en une seule opération qu'il envoie au serveur de provisionnement. L'événement unique AccumulatedProvisioningRoleEvent est généré pour exécuter les événements dans cet ordre.

Remarque : Pour plus d'informations sur l'événement AccumulatedProvisioningRoleEvent, consultez le *Manuel d'administration*.

Organization for Creating Inbound Users (Organisation pour la création d'utilisateurs entrants)

Définit le chemin d'accès complet au référentiel d'utilisateurs que CA Identity Manager utilise. Ce champ s'affiche uniquement lorsque le référentiel d'utilisateurs inclut une organisation.

Administrateur entrant

Définit un compte d'administrateur CA Identity Manager qui peut exécuter des tâches mappées vers des mappages entrants. Ces tâches sont incluses dans le rôle Provisionnement du gestionnaire de synchronisations. L'administrateur doit pouvoir exécuter chaque tâche sur tous les utilisateurs CA Identity Manager.

Annuaire de provisionnement

L'annuaire de provisionnement est un référentiel permettant le provisionnement d'informations, y compris le domaine, les utilisateurs globaux, les types de terminal, les terminaux, les comptes et les modèles de compte. Lorsque vous le sélectionnez, d'autres options s'affichent pour mapper le référentiel d'utilisateurs CA Identity Manager vers cet annuaire.

Activation de la mise en pool des sessions

Pour améliorer les performances, CA Identity Manager peut affecter un nombre de sessions mises en pool pour les communications avec le serveur de provisionnement.

Si l'option Session Pools (Pool de sessions) est désactivée, CA Identity Manager crée des sessions et les supprime selon les besoins.

Pour un nouvel environnement, les pools de sessions sont activés par défaut. Pour les environnements existants, vous pouvez activer les pools de sessions.

Procédez comme suit:

1. Dans la console de gestion, sélectionnez Advanced Parameters (Paramètres avancés), Provisioning (Provisionnement).
2. Sélectionnez Use Session Pool (Utiliser un pool de sessions).
3. Définissez le nombre minimum de sessions disponibles dans le pool au démarrage.
4. Définissez le nombre maximum de sessions dans le pool.
5. Cliquez sur Enregistrer.
6. Redémarrez le serveur d'applications.

   Le pool de sessions est activé selon les paramètres définis.

Activation de la synchronisation de mots de passe

Le serveur de provisionnement permet la synchronisation des mots de passe entre les utilisateurs CA Identity Manager et les comptes d'utilisateurs de terminal associés. En d'autres termes, lorsqu'un utilisateur comprenant des rôles de provisionnement est créé ou modifié dans CA Identity Manager, l'utilisateur de provisionnement est défini de façon à permettre les modifications de mots de passe à partir des comptes du terminal.

Remarque : Lorsque vous activez cette fonctionnalité dans la console de gestion, *tous* les utilisateurs dans l'environnement sont autorisés à modifier les mots de passe à partir des comptes du terminal.

Pour activer la synchronisation de mots de passe :

1. Dans la console de gestion, sélectionnez Advanced Parameters (Paramètres avancés), Provisioning (Provisionnement).
2. Sous Endpoint Accounts, sélectionnez Enable Password Changes (Activer les modifications de mot de passe).
3. Cliquez sur Enregistrer.
4. Redémarrez le serveur d'applications.

Mappages d'attributs

Les mappages d'attributs associent les attributs d'utilisateur des tâches d'administration en rapport avec le provisionnement, comme Provisionnement de la création d'utilisateur, avec les attributs correspondants dans le serveur de provisionnement. Vous pouvez mapper un attribut de provisionnement unique vers plusieurs attributs dans le référentiel d'utilisateurs CA Identity Manager.

Des mappages par défaut existent pour les attributs dans les tâches par défaut, qui sont répertoriés dans la section Mappages entrants. Si vous modifiez l'une de ces tâches d'administration de façon à utiliser différents attributs, mettez à jour les mappages d'attributs de manière appropriée.

Mappages entrants

Les mappages entrants mappent les événements générés par le serveur de provisionnement à une tâche d'administration. Ces mappages sont prédéfinis et ne peuvent pas être modifiés.

Mappages sortants

Les mappages sortants associent des événements générés par les tâches d'administration aux événements qui sont appliqués à l'annuaire de provisionnement. Des mappages par défaut existent pour les événements qui affectent les attributs d'utilisateur.

Console d'utilisateur

La console d'utilisateur est une application Web qui vous permet d'accéder à un environnement CA Identity Manager pour effectuer des tâches d'administration. Vous définissez les propriétés de la console d'utilisateur que les administrateurs utilisent pour accéder à un environnement dans la page User Console (Console d'utilisateur) de la console de gestion.

Cette page contient les champs suivants :

General Properties (Propriétés générales)

Permet de définir les propriétés qui s'appliquent à un environnement.

Show Recently Completed Tasks (Afficher les tâches terminées récemment)

Détermine si CA Identity Manager affiche un message de statut lorsqu'une tâche est terminée.

Lorsque cette option est sélectionnée, les utilisateurs doivent cliquer sur OK pour effacer le message de statut affiché par CA Identity Manager.

Pour désactiver le message et éviter aux utilisateurs de devoir cliquer sur OK à chaque message, désélectionnez cette option.

Show About Link (Afficher le lien A propos de)

Détermine si un lien A propos de s'affiche dans le coin inférieur droit de la console d'utilisateur. Lorsque cette option est sélectionnée, les utilisateurs CA Identity Manager peuvent cliquer sur le lien A propos de pour afficher des informations sur la version des composants CA Identity Manager.

Activation du changement de langue

Détermine si CA Identity Manager inclut une liste déroulante Choisir la langue dans la fenêtre de connexion et dans la console d'utilisateur. Lorsque ce champ est sélectionné, les utilisateurs CA Identity Manager peuvent changer la langue dans la console d'utilisateur en sélectionnant une nouvelle langue dans la liste.

Remarque : Pour afficher le champ Choose Language (Choisir la langue), vérifiez que l'option Enable Language Switching (Activer le changement de langue) est sélectionnée *et* configurez CA Identity Manager de façon à permettre la prise en charge de plusieurs langues.

Pour plus d'informations, reportez-vous au *Manuel de conception de la console d'utilisateur*.

Job Timeout (Délai d'expiration de job)

Détermine la durée d'attente après la soumission d'une tâche avant qu'un message de statut s'affiche.

Lorsque la tâche se termine dans le délai spécifié, CA Identity Manager affiche le message suivant :

Tâche terminée

Si la tâche prend plus de temps ou se trouve sous le contrôle du flux de travaux, CA Identity Manager affiche le message suivant :

"Task has been submitted for processing on *date_actuelle*" (La tâche a été soumise pour traitement le)

Remarque : Les modifications peuvent ne pas prendre effet immédiatement.

Theme Properties (Propriétés de thème)

Ces propriétés permettent de personnaliser l'icône et le titre de la console d'utilisateur dans un environnement. Par exemple, vous pouvez ajouter le logo et le nom de votre société à des fenêtres de la console d'utilisateur.

Les propriétés de thème incluent les paramètres suivants :

Icon (Icône) (URI)

Définit l'icône à l'aide d'un URI vers une image disponible sur le serveur d'applications.

Exemple : http://myserver.mycompany.com/images/front/logo.gif

Icon Link (Lien d'icône) (URI)

Définit le lien de navigation vers l'image à l'aide d'un URI.

Icon Title (Titre d'icône)

Définit l'info-bulle qui s'affiche lorsque vous passez la souris sur l'icône.

Titre

Spécifie le texte personnalisé affiché à côté de l'icône en haut de la console d'utilisateur.

Remarque : Si vous avez défini une apparence personnalisée, vous pouvez spécifier une icône ou un titre en référençant un fichier de propriétés pour l'apparence. Par exemple, si l'entrée de l'image d'icône dans le fichier de propriétés pour une apparence personnalisée est image/logo.gif, vous pouvez entrer cette même chaîne dans le champ Icon (Icône).

Login Properties (Propriétés de connexion)

Spécifiez la méthode d'authentification et l'emplacement de la page de connexion vers laquelle les utilisateurs sont redirigés lorsqu'ils accèdent à un environnement.

Authentication Provider module class name (Nom de classe du module de fournisseur d'authentification)

Spécifie le nom de classe du module de fournisseur d'authentification.

Page de connexion

Spécifie la page vers laquelle les utilisateurs sont redirigés lorsqu'ils accèdent à un environnement.

Services Web

Le service Web d'exécution des tâches de CA Identity Manager active les applications clientes de tiers pour la soumission des tâches à CA Identity Manager afin de les exécuter à distance.

La fenêtre Web Services Properties (Propriétés des services Web) vous permet de configurer le service Web d'exécution des tâches pour un environnement. Dans cette fenêtre, vous pouvez effectuer les tâches suivantes :

- Activer le service Web d'exécution des tâches pour un environnement CA Identity Manager.
- Générer les documents WSDL propres à une tâche.
- Permettre l'emprunt d'identité.
- Indiquer que le mot de passe d'administrateur est requis pour l'authentification.
- Configurer l'authentification SiteMinder.
- Configurer SiteMinder pour sécuriser l'URL de services Web, si l'intégration de CA Identity Manager avec SiteMinder est prise en charge.
- Spécifier l'authentification du jeton de nom d'utilisateur des services de sécurité Web.
- Spécifier l'un des trois types d'authentification possibles.

Pour plus d'informations sur la génération de demandes CA Identity Manager distantes via le service Web d'exécution des tâches, consultez le manuel *Programming Guide for Java*.

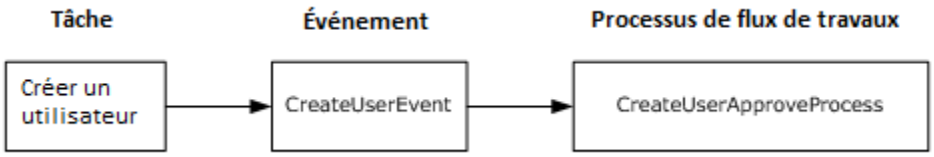
Workflow Properties (Propriétés des flux de travaux)

Si la fonctionnalité de flux de travaux est activée, elle vous permet de contrôler l'exécution d'une tâche CA Identity Manager associée à un processus de flux de travaux.

Un processus de flux de travaux est un ensemble d'étapes qui sont effectuées pour accomplir un objectif métier, comme par exemple la création d'un compte d'utilisateur. En général, l'une de ces étapes implique l'approbation ou le rejet de la tâche.

Une tâche d'administration est associée à un ou plusieurs événements, qui peuvent déclencher un ou plusieurs processus de flux de travaux. Une fois que le processus de flux de travaux est terminé, CA Identity Manager effectue la tâche ou la rejette selon les résultats de ce processus.

L'illustration suivante présente la relation entre une tâche CA Identity Manager, un événement associé et un processus de flux de travaux :



Propriétés des flux de travaux

Utilisez la case à cocher pour activer ou désactiver le flux de travaux pour l'environnement CA Identity Manager.

Work Item Delegation (Délégation de tâches)

Si la délégation de tâches est activée, elle permet à un participant (le délégant) d'indiquer qu'un autre utilisateur (le délégué) obtiendra les autorisations d'approbation des tâches de la liste de travail du délégant. Un participant peut affecter des tâches à un autre approbateur pendant les périodes d'absence du délégant. Les délégants conservent l'accès complet à leurs tâches pendant la période de délégation.

La délégation utilise l'attribut connu suivant :

%DELEGATORS%

Cet attribut connu stocke les noms des utilisateurs qui délèguent à l'utilisateur à l'aide de l'attribut, ainsi que l'heure de création de la délégation.

Remarque : Pour plus d'informations sur la délégation des tâches, consultez le *Manuel d'administration*.

Outils de résolution des participants de flux de travaux

Les activités contenues dans un processus de flux de travaux, comme l'approbation ou le rejet d'une tâche, sont effectués par des *participants.*

L'outil de résolution de participants de flux de travaux vous permet de mapper un outil de résolution de participants personnalisé vers une classe Java d'outil de résolution de participants complète.

Un *outil de résolution de participants personnalisé* est un objet Java qui détermine les participants pour une activité de flux de travaux et renvoie une liste à CA Identity Manager. CA Identity Manager transfère la liste au moteur de flux de travaux.

En général, vous écrivez uniquement un outil de résolution personnalisé si aucun outil de résolution de participants standard ne peut fournir la liste des participants requise pour une activité.

Remarque : Pour plus d'informations sur le développement d'outils de résolution de participants personnalisés, consultez le manuel *Programming Guide for Java*. Pour plus d'informations sur les outils de résolution de participants standard, consultez le *Manuel d'administration*.

Paramètres d'importation/d'exportation personnalisés

A partir de la fenêtre Advanced Settings (Paramètres avancés) de la console de gestion, appliquez les paramètres avancés à plusieurs environnements, comme suit :

- Configurez les paramètres avancés dans un environnement.
- Exportez les paramètres avancés dans un fichier XML.
- Importez ce fichier dans les environnements requis.

Erreurs de mémoire insuffisante de la machine virtuelle Java

Symptôme :

Je reçois des erreurs de mémoire insuffisante de la machine virtuelle Java pendant les périodes de charge élevées qui affectent la fonctionnalité du serveur CA Identity Manager.

Solution :

Il est recommandé de définir les options de débogage de la machine virtuelle Java pour être alerté des conditions de mémoire insuffisante.

Remarque : Pour plus d'informations sur la définition des options de débogage de la machine virtuelle Java, consultez la rubrique Debugging Options in Java HotSpot VM Options sur le site http://www.oracle.com.

Chapitre 8: Audit

Ce chapitre traite des sujets suivants :

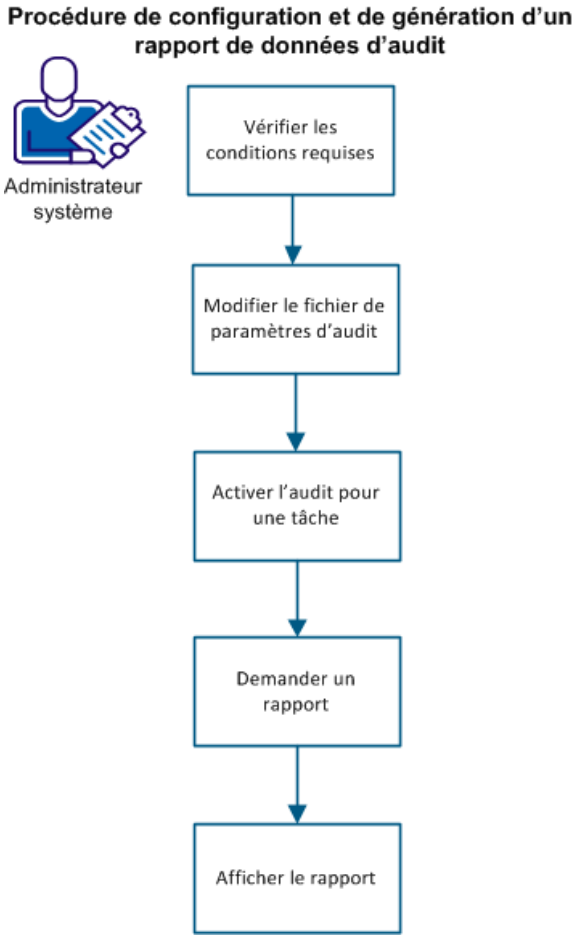
Procédure de configuration et de génération de rapports sur les données d'audit

Les données d'audit contiennent un enregistrement sous forme d'historique des opérations réalisées dans un environnement. Lorsque vous configurez et activez l'audit, le système enregistre des informations sur les tâches d'une base de données d'audit. Les informations d'audit permettent de générer des rapports. Les données d'audit peuvent inclure les points suivants :

- Les activités du système pendant une période spécifiée
- Les événements de connexion et de déconnexion des utilisateurs lors d'un accès à un environnement
- Les tâches qu'un utilisateur effectue.
- Une liste des objets modifiés pendant une période spécifiée
- Les rôles affectés à l'utilisateur
- Les opérations effectuées par un compte d'utilisateur

Les données d'audit sont générées pour des *événements* CA Identity Manager Un événement est une opération générée par une tâche CA Identity Manager. Par exemple, la tâche Créer un utilisateur peut inclure un événement AssignAccessRoleEvent.

Le diagramme suivant décrit la procédure que suit un administrateur système pour configurer l'audit et générer un rapport sur les données d'audit :



Connectez-vous en tant qu'administrateur et effectuer les opérations suivantes :

1. Vérification des conditions préalables (page 251)
2. Modification du fichier de paramètres d'audit (page 251)
3. Activation de l'audit pour une tâche (page 256)
4. Demande de rapport (page 257)
5. Affichage du rapport (page 260)

Vérification des conditions préalables

Vérifiez que les configurations suivantes sont remplies avant de configurer les paramètres d'audit :

- Une instance de base de données distincte est créée pour le stockage des données liées à l'audit. Par défaut, le fichier de schéma de base de données CA Identity Manager se trouve à l'emplacement suivant :
  - **Windows** : <chemin_installation>\Identity Manager\tools\db
- Configurez la connexion au serveur de rapports de sorte que le rapport d'audit soit demandé et affiché.
- Ajoutez un objet de connexion pour le rapport d'audit. Procédez comme suit :
  a. Connectez-vous à la console d'utilisateur avec des droits d'administrateur.
  b. Accédez à Rôles et tâches, Tâches d'administration et recherchez un rapport d'audit à modifier.
  c. Entrez le nom de connexion suivant dans le champ Objet de connexion pour le rapport :
  `rptParamConn`

Modification du fichier de paramètres d'audit

Configurez des paramètres d'audit dans le fichier de paramètres d'audit pour définir le type d'informations que CA Identity Manager doit auditer. Vous pouvez configurer un fichier de paramètres d'audit pour effectuer les tâches suivantes :

- Auditer certains ou tous les événements générés par les tâches d'administration.
- Enregistrer les informations d'événement correspondant à un état, par exemple, lorsqu'un événement se termine ou est annulé.
- Journaliser les informations sur les attributs impliqués dans un événement. Par exemple, vous pouvez journaliser les attributs modifiés au cours d'un événement ModifyUserEvent.

- Définir le niveau d'audit pour la journalisation d'attribut.

Le fichier des paramètres d'audit est un fichier XML que vous créez en exportant des paramètres d'audit. Le schéma du fichier est le suivant :

```
<Audit enabled="" auditlevel="" datasource="">
  <AuditEvent name="" enabled="" auditlevel="">
    <AuditProfile objecttype="" auditlevel="">
      <AuditProfileAttribute name="" auditlevel="" />
    </AuditProfile>
    <EventState name="" severity=""/>
  </AuditEvent>
</Audit>
```

Pour plus d'informations sur le schéma et les éléments d'audit, consultez les commentaires dans le fichier des paramètres d'audit.

Les éléments AuditProfileAttribute désignent les attributs audités par CA Identity Manager. Les attributs s'appliquent à l'objet spécifié dans l'élément AuditProfile.

Remarque : Si aucun attribut de profil d'audit n'est spécifié, tous les attributs de l'objet spécifié dans l'élément AuditProfile sont journalisés.

Le tableau suivant résume les attributs valides pour les types d'objet CA Identity Manager :

Attributs valides pour les types d'objet CA Identity Manager

Type d'objet	Attributs valides
ACCESS ROLE	■ name : nom du rôle visible par l'utilisateur ■ description : commentaire facultatif décrivant le but du rôle ■ members : utilisateurs qui peuvent utiliser le rôle. ■ administrators : utilisateurs qui peuvent affecter des membres de rôle ou des administrateurs. ■ owners : utilisateurs qui peuvent modifier le rôle. ■ enabled : indique si le rôle est activé ou non. ■ assignable : indique si le rôle peut être affecté par un administrateur. ■ tasks : tâches d'accès associées au rôle.

Attributs valides pour les types d'objet CA Identity Manager	
Type d'objet	**Attributs valides**
ACCESS TASK	■ name : nom de la tâche visible par l'utilisateur ■ description : commentaire facultatif décrivant le but de la tâche ■ application : application associée à la tâche. ■ tag : identificateur unique de la tâche. ■ reserved1, reserved2, reserved3, reserved4 : valeurs des champs réservés pour la tâche
ADMINISTRATIVE ROLE	■ name : nom du rôle visible par l'utilisateur ■ description : commentaire facultatif décrivant le but du rôle ■ members : utilisateurs qui peuvent utiliser le rôle. ■ administrators : utilisateurs qui peuvent affecter des membres de rôle ou des administrateurs. ■ owners : utilisateurs qui peuvent modifier le rôle. ■ enabled : indique si le rôle est activé ou non. ■ assignable : indique si le rôle peut être affecté par un administrateur. ■ tasks : tâches associées au rôle.

Attributs valides pour les types d'objet CA Identity Manager	
Type d'objet	**Attributs valides**
ADMINISTRATIVE TASK	■ name : nom de la tâche visible par l'utilisateur ■ description : commentaire facultatif décrivant le but de la tâche ■ tag : identificateur unique de la tâche. ■ category : catégorie de l'interface utilisateur CA Identity Manager dans laquelle la tâche est affichée. ■ primary_object : objet sur lequel la tâche opère. ■ action : opération effectuée sur l'objet. ■ hidden : indique si la tâche est *masquée* dans les menus. ■ public : indique si la tâche peut être utilisée par les utilisateurs qui ne sont pas connectés à CA Identity Manager. ■ auditing : indique si la tâche enregistre les informations d'audit. ■ external : indique si la tâche est une tâche externe. ■ url : URL vers laquelle l'utilisateur est redirigé lorsqu'une tâche externe est exécutée. ■ workflow : indique si les événements CA Identity Manager associés à la tâche déclenchent le flux de travaux. ■ webservice : indique si la tâche est une tâche pour laquelle une sortie WSDL (Web Services Description Language) peut être générée via la console de gestion CA Identity Manager.
GROUP	Tous les attributs valides définis pour l'objet GROUP dans le fichier de configuration d'annuaire (directory.xml).
ORGANIZATION	Tous les attributs valides définis pour l'objet ORGANIZATION dans le fichier de configuration d'annuaire (directory.xml).
PARENTORG	

Attributs valides pour les types d'objet CA Identity Manager	
Type d'objet	**Attributs valides**
RELATIONSHIP	■ %CONTAINER% : identificateur unique de l'objet parent. Par exemple, si l'objet RELATIONSHIP décrit l'appartenance à un rôle, le rôle est le conteneur. ■ %CONTAINER_NAME% : nom du groupe parent visible par l'utilisateur ■ %ITEM% : identificateur unique de l'objet contenu dans l'objet parent. Par exemple, si l'objet RELATIONSHIP décrit l'appartenance à un rôle, les membres du rôle sont les éléments. ■ %ITEM_NAME% : nom du groupe imbriqué visible par l'utilisateur
USER	Tous les attributs valides définis pour l'objet USER dans le fichier de configuration d'annuaire (directory.xml).
AUCUN	Aucun attribut

Remarque : Les points suivants s'appliquent au tableau précédent :

- Les valeurs des attributs enabled, assignable, auditable, workflow, hidden, webservice et public sont journalisées comme vraies ou fausses.
- Lors d'un audit de tâches pour des rôles, le nom visible par l'utilisateur est journalisé.
- La base de données stocke les stratégies de membre, d'administrateur et de propriété au format XML compilé. Ce format est différent de l'interface utilisateur dans laquelle chaque stratégie s'affiche en tant qu'expression.

Procédez comme suit:

1. Connectez-vous à la console de gestion, sélectionnez l'environnement, Paramètres avancés, puis cliquez sur Audit.
2. Cliquez sur Exporter.

   Les paramètres d'audit actuels sont exportés dans un fichier XML de paramètres d'audit.

3. Modifiez les paramètres d'audit dans le fichier XML que vous avez exporté à l'étape précédente. Effectuez les tâches suivantes :
   a. Définissez la valeur d'Audit sur enabled ="true" et spécifiez la valeur de Nom JNDI iam_im_<auditdb>.xml pour la source de données de l'élément.
   b. Spécifiez le nom JNDI ci-dessous :
      `java:/auditDbDataSource`

      Remarque : La source de données se trouve à l'emplacement suivant :
      `iam/im/jdbc/auditDbDataSource`
   c. Ajoutez, modifiez ou supprimez des éléments dans le fichier.
   d. Vous pouvez également modifier le niveau des informations enregistrées pour chaque événement.
4. Répétez les étapes 1 et 2. Cliquez sur Importer et chargez le fichier XML des paramètres d'audit modifié.
5. Redémarrez l'environnement.

Le fichier des paramètres d'audit a été mis à jour.

Activation de l'audit pour une tâche

Activez l'audit pour les tâches pour lesquelles vous avez configuré l'audit dans le fichier des paramètres d'audit.

Procédez comme suit:

1. Connectez-vous à la console d'utilisateur avec des droits d'administrateur système.
2. Créez ou modifiez la tâche pour laquelle vous voulez activer l'audit.
3. Dans l'onglet Profil, vérifiez que la case Activer l'audit est cochée.
4. Cliquez sur Soumettre.

L'audit est activé pour la tâche.

Demande de rapport

Pour afficher un rapport, demandez-le à un utilisateur avec des droits d'administration de rapports. Sélectionnez le rapport approprié qui suit les données d'audit. Si votre demande de rapport requiert une approbation, le système envoie une alerte par courriel.

Avant de planifier un rapport, procédez comme suit :

1. Connectez-vous à la console d'utilisateur avec des droits d'administrateur.
2. Accédez à Rôles et tâches, Modifier la tâche d'administration et recherchez un rapport d'audit à modifier.
3. Sélectionnez l'onglet Onglets et cliquez sur le planificateur du serveur de rapports IAM à modifier.
4. Cochez la case Activer l'option de récurrence.
5. Cliquez sur OK, puis sur Soumettre.

Procédez comme suit:

1. Connectez-vous à la console d'utilisateur avec des droits d'utilisateur pour les tâches de rapport.
2. Sélectionnez Rapports, Tâches de génération de rapports, Demander un rapport.

   Une liste de rapports s'affiche.
3. Sélectionnez un rapport basé sur un audit.

   Une fenêtre de paramètres s’affiche.
4. Cliquez sur Planifier un rapport et sélectionnez une planification pour votre rapport.

   Maintenant

   Spécifie que le rapport est exécuté immédiatement.

   Une fois

   Spécifie que le rapport s'exécute une fois, pendant une période spécifique. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin pour la génération du rapport.

   (Rapport d'audit uniquement) Toutes les heures

   Spécifie que le rapport est généré à l'heure de début, puis toutes les n heures par la suite ; n indiquant un intervalle entre les rapports successifs. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin et l'intervalle entre deux rapports successifs.

(Rapport d'audit uniquement) Tous les jours

Spécifie que le rapport est généré à l'heure de début, puis toutes les n jours par la suite ; n indiquant un intervalle entre les rapports successifs. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin et l'intervalle entre deux rapports successifs.

(Rapport d'audit uniquement) Toutes les semaines

Spécifie que le rapport est généré toutes les semaines le jour sélectionné à compter de la date de début. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin pour la génération du rapport.

(Rapport d'audit uniquement) Tous les mois

Spécifie que le rapport est généré tous les mois à compter de la date de début, puis toutes les n mois par la suite. "n" désigne l'intervalle entre deux rapports consécutifs. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin et l'intervalle entre deux rapports successifs.

(Rapport d'audit uniquement) Exécuter le rapport le jour N du mois

Spécifie que le rapport est généré le jour précis que vous avez indiqué dans le mois. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin pour la génération du rapport.

(Rapport d'audit uniquement) Premier lundi

Spécifie que le rapport est généré tous les premiers lundis de chaque mois. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin pour la génération du rapport.

(Rapport d'audit uniquement) Dernier jour du mois

Spécifie que le rapport est généré le dernier jour du mois. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin pour la génération du rapport.

(Rapport d'audit uniquement) Jour X de la semaine N du mois

Spécifie que le rapport est généré le jour précis de la semaine précise de chaque mois. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin pour la génération du rapport. Par exemple, vous pouvez générer un rapport le vendredi de la 3e semaine de chaque mois.

5. Cliquez sur Soumettre.

   La demande de rapport est soumise. Selon la configuration de votre environnement, la demande s'exécute immédiatement ou suite à l'approbation d'un administrateur.

   Généralement, un administrateur système ou un autre utilisateur avec des droits d'administration de rapports doit approuver une demande de rapport avant que le système ne la réalise. L'approbation est requise, car l'exécution de certains rapports peut requérir un long délai ou des ressources système importantes. Si votre demande de rapport requiert une approbation, vous recevrez une alerte par courriel.

   Remarque : Activez CA WorkFlow pour l'environnement si l'approbation est requise.

Affichage du rapport

Selon la configuration de votre environnement, un rapport s'affiche lorsqu'un administrateur approuve la demande pour ce rapport. Si votre demande de rapport est en attente d'approbation, vous recevrez une alerte par courriel. Le rapport que vous voulez afficher apparaîtra dans la liste de recherche uniquement lorsqu'il sera approuvé.

Remarque : Pour afficher des rapports dans CA Identity Manager à l'aide de la tâche Afficher mes rapports, activez les cookies de session tiers dans votre navigateur.

Procédez comme suit:

1. Dans la console d'utilisateur, accédez à Rapports, Tâches de génération de rapports, puis cliquez sur Afficher mes rapports.
2. Recherchez le rapport généré à afficher.

   Les rapports de récurrence et les instances de rapport à la demande s'affichent.

   Remarque : Si le statut du rapport est En attente/Récurrent, le rapport n'est pas généré et peut se terminer après un délai.
3. Sélectionnez le rapport à afficher.
4. (Facultatif) Cliquez sur Exporter ce rapport (coin gauche supérieur) pour exporter le rapport dans les formats suivants :
   - Crystal Report
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003) données uniquement
   - Microsoft Excel (97-2003) modifiable
   - Rich Text Format (RTF)
   - Separated Values (CSV)
   - XML

Nettoyage de la base de données d'audit

Il se peut que la base de données d'audit cumule des enregistrements qui ne sont plus nécessaires. Pour supprimer ces enregistrements, exécutez la procédure de base de données suivante dans le répertoire db\auditing :

`garbageCollectAuditing12` *`ID_environnement MM/JJ/AAAA`*

ID_environnement

Définit l'ID de l'environnement CA Identity Manager.

MM/JJ/AAAA

Définit la date limite de suppression des enregistrements d'audit.

Chapitre 9: Environnements de production

Cette section fournit une description fonctionnelle détaillée de la procédure de migration des parties de fonctionnalité. Assurez-vous que cette procédure n'est utilisée que lorsque des modifications limitées et appropriées ont été apportées à l'environnement de développement.

Ce chapitre traite des sujets suivants :

Migration des définitions de rôles et de tâches d'administration

Vous pouvez personnaliser les rôles et les tâches CA Identity Manager pour répondre aux besoins de votre société. La personnalisation implique la création ou la modification des rôles et des tâches d'administration, ou l'utilisation de tâches Créer ou Modifier pour un rôle ou une tâche d'administration.

Une méthode alternative, bien que *non recommandée*, consiste à modifier les rôles et les tâches dans le fichier roledefinition.xml. Utilisez cette méthode pour des modifications limitées à cause du risque d'erreurs encouru.

Ce processus migrera uniquement les définitions de rôle et de tâche d'administration. Si les rôles sont associés à des organisations, considérez la migration de l'environnement CA Identity Manager entier.

Important : Si vous avez modifié les définitions de rôle ou de tâche dans l'environnement de production, ces modifications sont ignorées lorsque vous importez les définitions de rôle ou de tâche d'un environnement de développement. L'importation de définitions de rôle et de tâche remplace les définitions de rôle et de tâche existantes portant les mêmes noms.

Exportation des définitions de rôle et de tâche d'administration

Si les modifications ont été effectuées directement dans le fichier roledefinition.xml, vous pouvez directement importer ce fichier dans l'environnement de production. Dans le cas contraire, pour exporter les définitions de rôle et de tâche, procédez comme suit :

1. Si vous avez un cluster de serveurs de stratégies, vérifiez qu'un seul serveur de stratégies s'exécute.
2. Arrêtez tous les noeuds CA Identity Manager sauf un.
3. Connectez-vous à la console de gestion.
4. Cliquez sur CA Identity Manager environments (Environnements).
5. Sélectionnez l'environnement CA Identity Manager à partir duquel exporter les définitions de rôle et de tâche.
6. Cliquez sur Roles (Rôles), puis cliquez sur Export (Exporter) et spécifiez un nom pour le fichier.
7. Pour importer ce fichier, suivez les instructions de la procédure suivante.

Importation de définitions de rôle et de tâche d'administration

Procédez comme suit:

1. Copiez le fichier créé dans la procédure précédente dans l'environnement de production.
2. Connectez-vous à la console de gestion dans l'environnement de production.
3. Cliquez sur CA Identity Manager environments (Environnements).
4. Sélectionnez l'environnement CA Identity Manager approprié.
5. Cliquez sur Roles (Rôles).
6. Cliquez sur Import (Importer) et spécifiez le nom du fichier XML généré lors de l'exportation.
7. Une fois ces étapes effectuées, démarrez les serveurs de stratégies supplémentaires et les noeuds CA Identity Manager que vous avez arrêtés.

   Remarque : S'il y a encore des modifications à effectuer dans un environnement CA Identity Manager, répétez l'étape 6.

Vérification de l'importation de rôle et de tâche

Pour vérifier que les rôles et les tâches ont été importés correctement, connectez-vous à CA Identity Manager sous un compte d'administrateur qui peut utiliser les tâches suivantes :

- Modifier un rôle d'administration
- Modifier la tâche d'administration

Exécutez ces tâches et vérifiez que les rôles et les tâches reflètent les définitions de rôle importées.

Migration des apparences CA Identity Manager

Vous pouvez personnaliser les apparences CA Identity Manager pour donner une apparence spéciale à l'application. Si vous avez modifié ou créé des apparences pour un ensemble d'utilisateurs, suivez les étapes suivantes pour migrer les apparences de l'environnement de développement vers l'environnement de production.

Si vous modifiez une apparence, copiez les fichiers modifiés.

Procédez comme suit:

1. Copiez les nouveaux fichiers et les fichiers modifiés de l'environnement de développement vers le serveur de production, notamment les fichiers d'image, les feuilles de style, les fichiers de propriétés et la page de console (index.jsp).
2. Si plusieurs apparences sont utilisées, configurez la réponse SiteMinder.

   Remarque : Pour plus d'informations sur l'utilisation de plusieurs apparences, reportez-vous au *Manuel de configuration*.

Pour vérifier la migration des apparences, connectez-vous à la console d'utilisateur et vérifiez que l'apparence s'affiche correctement.

Mise à jour de CA Identity Manager dans un environnement de production

Après avoir migré CA Identity Manager de l'environnement de développement à celui de production, vous devrez peut-être effectuer des mises à jour incrémentielles. Pour migrer une nouvelle fonctionnalité CA Identity Manager de l'environnement de développement vers celui de production, procédez comme suit :

1. Migrez les environnements CA Identity Manager.
2. Copiez le fichier iam_im.ear.
3. Migrez les définitions de processus de flux de travaux.

Migration d'un environnement CA Identity Manager

Vous créez un environnement CA Identity Manager à partir de la console de gestion. L'environnement CA Identity Manager inclut des définitions de rôle et de tâche, des définitions de flux de travaux, des fonctionnalités personnalisées créées à l'aide des API CA Identity Manager et d'un annuaire CA Identity Manager.

Procédez comme suit:

1. Si l'intégration de CA Identity Manager avec SiteMinder est configurée et que vous disposez d'un cluster de serveurs de stratégies, vérifiez qu'un seul serveur de stratégies est en cours d'exécution.
2. Arrêtez tous les noeuds CA Identity Manager sauf un.
3. Exportez les environnements CA Identity Manager à partir de la console de gestion dans l'environnement de développement.
4. Importez les environnements exportés dans la console de gestion de l'environnement de production.
5. Si l'intégration de CA Identity Manager avec SiteMinder est configurée, reprotégez les domaines CA Identity Manager dans l'interface utilisateur du serveur de stratégies.

   Le domaine de stratégie n'est pas exporté à partir du référentiel des stratégies lorsque vous exportez un environnement CA Identity Manager.
6. Redémarrez le serveur de stratégies et les noeuds CA Identity Manager que vous avez arrêtés.

Lors de la migration d'un environnement CA Identity Manager, les activités suivantes sont effectuées :

- Si le même objet existe aux deux emplacements, les modifications apportées sur le serveur de développement remplacent celles apportées sur le serveur de production.
- Si des objets sont créés dans l'environnement de développement, ils sont ajoutés au serveur de production.
- Si des objets sont créés sur le serveur de production, ils sont conservés.

Exportation d'un environnement CA Identity Manager

Pour déployer un environnement CA Identity Manager sur un système de production, exportez cet environnement à partir d'un système de développement ou de stockage intermédiaire et importez-le vers le système de production.

Remarque : Lors de l'importation d'un environnement préalablement exporté, CA Identity Manager affiche un journal dans une fenêtre de statut de la console de gestion. Pour consulter des informations de validation et de déploiement pour chaque objet géré et ses attributs dans ce journal, *avant d'exporter* l'environnement, sélectionnez le champ Enable Verbose Log Output (Activer la sortie de journal détaillé) dans la page des propriétés d'environnement. Veillez à ce que ce champ n'entraîne aucun problème de performance significatif lors de l'importation.

Procédez comme suit:

1. Dans la console de gestion, cliquez sur Environnements.

   La fenêtre d'environnements CA Identity Manager s'affiche et contient une liste d'environnements CA Identity Manager.
2. Sélectionnez l'environnement à exporter.
3. Cliquez sur le bouton Exporter.

   Une fenêtre File Download (Téléchargement de fichier) s'affiche.
4. Enregistrez le fichier .zip à un emplacement accessible au système de production.
5. Cliquez sur Terminer.

   Les informations de l'environnement sont exportées vers un fichier .zip que vous pouvez importer dans un autre environnement.

Importation d'un environnement CA Identity Manager

Après avoir exporté un environnement CA Identity Manager à partir d'un système de développement, vous pouvez l'importer dans un système de production.

Procédez comme suit:

1. Dans la console de gestion, cliquez sur Environnements.

   La fenêtre d'environnements CA Identity Manager s'affiche et contient une liste d'environnements CA Identity Manager.

2. Cliquez sur Importer.

   La fenêtre Import Environment (Importer un environnement) s'affiche.

3. Pour importer un environnement, accédez au fichier .zip requis.

4. Cliquez sur Terminer.

L'environnement est importé dans CA Identity Manager.

Vérification de la migration d'environnement CA Identity Manager

Pour vérifier que la migration de l'environnement CA Identity Managera bien été effectuée, confirmez que l'environnement CA Identity Manager apparaît dans l'interface utilisateur du serveur de stratégies dans l'environnement de production.

Dans l'interface utilisateur du serveur de stratégies, vérifiez les points suivants :

- Les paramètres d'annuaire d'utilisateurs CA Identity Manager sont corrects.
- Le nouveau domaine CA Identity Manager existe.
- Les schémas d'authentification appropriés protègent les domaines CA Identity Manager.

Lors de la connexion à la console de gestion, vérifiez également que l'environnement CA Identity Manager s'affiche lorsque vous sélectionnez les environnements.

Migration du fichier iam_im.ear pour JBoss

Redéployez le fichier iam_im.ear à chaque migration de la fonctionnalité de l'environnement de développement vers celui de production. La migration du fichier EAR entier permet de s'assurer que l'environnement de production est identique à celui de développement.

Procédez comme suit:

1. Copiez le fichier iam_im.ear de l'environnement de développement dans un emplacement accessible à partir de l'environnement de production.
2. Dans la copie du fichier iam_im.ear, modifiez les informations de connexion au serveur de stratégies, pour qu'elles correspondent à l'environnement de production.

   Pour cela, copiez le fichier *répertoire_installation_jboss*/server/default/iam_im.ear/policyserver_rar/META-INF/ra.xml de l'environnement de production dans le fichier iam_im.ear.
3. Remplacez le fichier iam_im.ear installé par la copie de votre environnement de développement, comme suit :
   a. Dans le serveur de production, supprimez le fichier iam_im.ear :

      répertoire_installation_cluster_noeuds_jboss\server\default\deploy\iam_im.ear
   b. Remplacez les fichiers supprimés par la copie du fichier iam_im.ear modifiée à partir de l'environnement de développement.
4. Répétez cette procédure pour chaque noeud du cluster.

Migration du fichier iam_im.ear pour WebLogic

Redéployez le fichier iam_im.ear à chaque migration de la fonctionnalité de l'environnement de développement vers celui de production. La migration du fichier EAR entier permet de s'assurer que l'environnement de production est identique à celui de développement.

Procédez comme suit:

1. Conservez les informations de connexion au serveur de stratégies.

   Ces informations sont stockées dans le fichier ra.xml, dans le répertoire policyserver_rar/WEB-INF. Copiez ce fichier dans un autre emplacement, pour pouvoir le remplacer dans le fichier iam_im.ear avant de le redéployer.
2. Copiez le fichier iam_im.ear dans un emplacement disponible du serveur d'administration WebLogic.

3. Remplacez les informations de connexion au serveur de stratégies.

   Dans le fichier iam_im.ear, remplacez le fichier policyserver_rar/WEB-INF/ra.xml par celui conservé à l'étape 1.

4. Redéployez le fichier iam_im.ear.

   a. Connectez-vous à la console WebLogic.

   b. Cliquez sur Deployments (Déploiements), Application, Identity Manager.

Dans l'onglet Deploy (Déployer), sélectionnez Deploy (Re-Deploy) Application (Déployer (redéployer) une application).

Migration du fichier iam_im.ear pour WebSphere

Procédez comme suit:

1. Copiez le script *imsInstall.jacl* sous *was_im_tools_dir**WebSphere-tools* dans le répertoire *deployment_manager_dir* *bin* où :

   - *was_im_tools_dir* est le répertoire sur le système de développement dans lequel les outils CA Identity Manager pour WebSphere sont installés.
   - *deployment_manager_dir* est l'emplacement d'installation du gestionnaire de déploiements.

2. Dans le système de développement à partir duquel vous avez configuré l'application CA Identity Manager, copiez *was_im_tools_dir* *WebSphere-tools**imsExport.bat* ou *imsExport.sh* vers *was_home**bin*.

3. Dans la ligne de commande, accédez à *was_home**bin*.

4. Assurez-vous que le serveur d'applications WebSphere est en cours d'exécution.

5. Pour exporter l'application CA Identity Manager déployée, effectuez les opérations suivantes :

   Pour Windows, entrez la commande :

   ```
   imsExport.bat "chemin_accès_fichier_ear_exporté"
   ```

   où *chemin_accès_fichier_ear_exporté* est le chemin complet et le nom de fichier créé par l'utilitaire imsExport.

   Pour les systèmes Windows, utilisez des barres obliques (/) au lieu de barres obliques inversée (\) lorsque vous spécifiez le chemin d'accès au fichier was_im.ear. Exemple :

   ```
   imsExport.bat "c:/program files/CA/CA Identity Manager/
   exported_ear/iam_im.ear"
   ```

   Pour UNIX, entrez la commande :

   ```
   ./wsadmin -f imsExport.jacl -conntype RMI -port 2809
   chemin_accès_fichier_ear_exporté
   ```

   où *chemin_accès_fichier_ear_exporté* est le chemin complet incluant le nom de fichier du fichier EAR exporté.

6. Copiez le fichier EAR exporté de l'emplacement du système de développement dans lequel vous l'avez exporté vers un emplacement du système sur lequel le gestionnaire de déploiements est installé.

7. Remplacez le fichier *was_im_tools_dir*/WebSphere-ear/iam_im.ear/policyserver_rar/META-INF/ra.xml par celui de l'environnement de production.

   Le fichier ra.xml contient les informations de connexion au serveur de stratégies.

8. Dans le système sur lequel le gestionnaire de déploiements est installé, déployez le fichier EAR Identity Manager :

   a. Dans la ligne de commande, accédez à :

      deployment_manager_dir \bin.

   b. Assurez-vous que le serveur d'applications WebSphere est en cours d'exécution.

   c. Exécutez le script imsInstall.jacl, comme suit :

   Remarque : L'exécution du script imsInstall.jacl peut prendre plusieurs minutes.

   Windows :

   wsadmin -f imsInstall.jacl *"chemin_accès_fichier_ear_copié" nom_cluster*

   où *chemin_accès_fichier_ear_copié* est le chemin d'accès complet incluant le nom du fichier Identity Manager EAR copié sur le système du gestionnaire de déploiements.

   Exemple :

   wsadmin -f imsInstall.jacl "c:\Program Files\CA\Identity Manager\WebSphere-tools\was_im.ear" im_cluster

UNIX :

./wsadmin -f imsInstall.jacl *chemin_accès_fichier_ear_copié nom_cluster*

où *chemin_accès_fichier_ear_copié* est le chemin d'accès complet incluant le nom du fichier Identity Manager EAR copié sur le système du gestionnaire de déploiements.

Exemple :

./wsadmin -f imsInstall.jacl /opt/CA/Identity Manager/WebSphere-tools/was_im.ear im_cluster

9. Si l'intégration de CA Identity Manager avec SiteMinder est configurée, vérifiez les points suivants :
   - Les agents SiteMinder peuvent se connecter au référentiel de stratégies.
   - Le serveur de stratégies peut se connecter au référentiel d'utilisateurs.
   - Les domaines CA Identity Manager ont été créés.

Migration des définitions de processus de flux de travaux

Si vous avez utilisé un flux de travaux dans l'environnement de développement, exportez les définitions de flux de travaux et importez-les dans l'environnement de production. Configurez le flux de travaux dans chacun des noeuds de serveur.

Exportation des définitions de processus

Dans l'environnement de développement, exportez les définitions de processus de flux de travaux.

Procédez comme suit:

1. Assurez-vous que le serveur d'applications est en cours d'exécution.
2. Accédez au répertoire *outils_admin*\Workpoint\bin\ et exécutez le fichier Archive.bat pour Windows ou Archive.sh pour UNIX, comme suit :
   a. Dans la boîte de dialogue Importer, sélectionnez l'objet racine.
   b. Cliquez sur Ajouter.
   c. Spécifiez le nom du fichier à générer.

d. Cliquez sur Exporter.

e. Cliquez sur OK.

outils_admin fait référence aux outils d'administration, qui se trouvent par défaut dans l'un des emplacements suivants :

- **Windows :** <chemin_installation>\tools
- **UNIX :** <chemin_installation2>/tools

3. Suivez les instructions de la section suivante, Importation de définitions de processus (page 273).

Importation de définitions de processus

Dans l'environnement de production, importez les définitions de processus de flux de travaux.

Procédez comme suit:

1. Redémarrez le serveur d'applications.
2. Vous pouvez également créer une copie de sauvegarde des définitions actuelles en les exportant au moyen de la procédure précédente.
3. Accédez au répertoire *outils_admin*\Workpoint\bin\ et exécutez le script Archive, comme suit :

   a. Dans la boîte de dialogue Importer, sélectionnez tous les éléments à importer.

   b. Lorsque vous êtes invité à sélectionner l'ancien ou le nouveau format, conservez l'ancien format.

      Le nouveau format ne prend pas en charge CA Identity Manager.

   c. Spécifiez le nom du fichier généré par l'exportation.

   d. Cliquez sur OK.

   outils_admin fait référence aux outils d'administration, qui se trouvent par défaut dans l'un des emplacements suivants :

   - **Windows :** <chemin_installation>\tools
   - **UNIX :** <chemin_installation2>/tools

Chapitre 10: Journaux CA Identity Manager

Ce chapitre traite des sujets suivants :

Suivi des problèmes dans CA Identity Manager

CA Identity Manager inclut les méthodes suivantes pour l'enregistrement de statut et le suivi des problèmes :

Afficher les tâches soumises

Affiche le statut de tous les événements et des tâches d'un environnement CA Identity Manager. Les administrateurs utilisent cette tâche dans la console d'utilisateur.

L'option Afficher les tâches soumises fournit les types d'informations suivants :

- La liste des événements qui se produisent et des tâches effectuées dans l'environnement.
- La liste d'attributs associés à un événement.
- Les événements réussis et les échecs d'événement
- Les événements qui se trouvent dans un état En attente ou Bloqué.
- Les événements rejetés, y compris la raison du rejet
- Le statut de synchronisation du compte
- Le statut de synchronisation de la stratégie d'identité
- Les informations de provisionnement (lorsque le provisionnement est activé)

Les journaux de serveur d'applications

Affichent des informations sur tous les composants d'une installation CA Identity Manager et fournissent des détails sur toutes les opérations effectuées dans CA Identity Manager.

L'emplacement et le type de fichier journal dépend du type de serveur d'applications que vous utilisez :

- WebLogic : les informations CA Identity Manager sont écrites dans la sortie standard. Par défaut, la sortie standard est la fenêtre de console dans laquelle l'instance de serveur s'exécute.
- JBoss : Les informations CA Identity Manager sont écrites dans la fenêtre de console dans laquelle l'instance de serveur s'exécute, ainsi que dans *répertoire_installation_jboss*\server\log\server.log
- WebSphere : Les informations CA Identity Manager sont écrites dans la fenêtre de console dans laquelle l'instance de serveur s'exécute, ainsi que dans *répertoire_installation_was*\AppServer\logs*nom_serveur*\SystemOut.

Pour plus d'informations, reportez-vous à la documentation de votre serveur d'applications.

Fichier journal du serveur d'annuaire

Contient des informations sur les activités menées dans l'annuaire d'utilisateurs.

Le type d'informations enregistrées et l'emplacement du fichier journal dépendent du type de serveur d'annuaire que vous utilisez. Pour plus d'informations, reportez-vous à la documentation de votre serveur d'annuaire.

Fichier journal du serveur de stratégies

Affiche les informations suivantes lorsque CA Identity Manager est intégré à SiteMinder :

- Problèmes de connexion SiteMinder
- Problèmes d'authentification SiteMinder
- Informations sur les objets CA Identity Manager gérés dans le référentiel de stratégies SiteMinder.
- Evaluation de la stratégie de mot de passe

Pour plus d'informations sur la configuration des journaux SiteMinder, consultez le manuel *SiteMinder Web Access Manager Policy Server Administration Guide*.

Profileur de serveur de stratégies

Si l'intégration de CA Identity Manager avec SiteMinder est configurée, vous pouvez suivre les diagnostics internes du serveur de stratégies et les fonctions de traitement, y compris les fonctions liées à CA Identity Manager.

Pour plus d'informations, consultez la rubrique Suivi des champs de composants et de données (page 277).

Fichiers journaux de l'agent Web

Si l'intégration de CA Identity Manager avec SiteMinder est configurée, les agents Web enregistrent les informations dans les deux journaux suivants :

- Journal d'erreurs : contient les erreurs des programmes et les erreurs de niveau opérationnel ; par exemple, l'impossibilité de l'agent Web à communiquer avec le serveur de stratégies.
- Journal de suivi : contient des messages d'information et d'avertissement, tels que les messages de suivi et les messages d'état de flux. Des données telles que les détails d'en-tête et les variables de cookie y sont également incluses.

Remarque : Pour plus d'informations sur les fichiers journaux de l'agent Web, consultez le manuel *SiteMinder Web Access Manager Web Agent Configuration Guide*.

Suivi des champs de composants et de données

Lorsque CA Identity Manager est intégré à SiteMinder, vous pouvez utiliser le profileur de serveur de stratégies SiteMinder pour suivre les champs de composants et de données des extensions CA Identity Manager pour le serveur de stratégies. Le profileur vous permet de configurer des filtres pour la sortie du suivi afin que seules les valeurs d'un champ de composant ou de données soient capturées.

Remarque : Pour obtenir des instructions sur l'utilisation du profileur de serveur de stratégies, consultez le manuel *SiteMinder Web Access Manager Policy Server Administration Guide*.

Vous pouvez activer le suivi pour les composants suivants :

Function_Begin_End

Fournit des instructions de suivi de niveau inférieur lorsque certaines méthodes des extensions CA Identity Manager pour le serveur de stratégies sont exécutées.

IM_Error

Suit les erreurs d'exécution dans les extensions CA Identity Manager pour le serveur de stratégies SiteMinder.

IM_Info

Fournit des informations de suivi générales aux extensions CA Identity Manager.

IM_Internal

Suit des informations générales sur les opérations CA Identity Manager internes.

IM_MetaData

Fournit des informations de suivi lorsque CA Identity Manager traite les métadonnées d'annuaire.

IM_RDB_Sql

Fournit des informations de suivi pour les bases de données relationnelles.

IM_LDAP_Provider

Fournit des informations de suivi pour des annuaires LDAP.

IM_RuleParser

Suit le processus d'analyse et d'évaluation des stratégies de membre, de propriété et d'administration, qui sont définis dans un fichier XML interprété lors de l'exécution.

IM_RuleEvaluation

Suit l'évaluation des règles de membre, d'administrateur, de propriétaire et de portée.

IM_MemberPolicy

Suit l'évaluation des stratégies de membre, y compris l'appartenance et la portée.

IM_AdminPolicy

Suit l'évaluation des stratégies d'administration.

IM_OwnerPolicy

Suit l'évaluation des stratégies de propriété.

IM_RoleMembership

Suit les informations relatives à l'appartenance à un rôle, comme la liste de rôles d'un utilisateur et la liste des membres d'un rôle.

IM_RoleAdmins

Suit les informations relatives à l'administration de rôle, comme la liste de rôles qu'un utilisateur gère et la liste des administrateurs d'un rôle.

IM_RoleOwners

Suit les informations relatives à la propriété de rôle, comme la liste de rôles d'un utilisateur et la liste des propriétaires d'un rôle.

IM_PolicyServerRules

Suit l'évaluation des règles de membre, telles que RoleMember, RoleAdmin et RoleOwner que le serveur de stratégies a résolues, et les règles de portée, comme les règles All et AccessTaskFilter pour AccessTasks.

IM_LLSDK_Command

Suit les communications entre le kit de développement logiciel CA Identity Manager interne et le serveur de stratégies. Le support technique utilise ce composant de suivi.

IM_LLSDK_Message

Les messages de suivi sont explicitement envoyés par le code Java au serveur de stratégies à partir du kit de développement logiciel CA Identity Manager interne. Le support technique utilise ce composant de suivi.

IM_IdentityPolicy

Suit l'évaluation et l'application des stratégies d'identité.

IM_PasswordPolicy

Suit l'évaluation des stratégies de mots de passe.

IM_Version

Fournit des informations sur la version de CA Identity Manager.

IM_CertificationPolicy

Suit l'évaluation des stratégies de certification.

IM_InMemoryEval

Suit le traitement des stratégies CA Identity Manager, notamment les stratégies de membre, d'administration, de propriété et d'identité. Le support technique utilise ce composant de suivi.

IM_InMemoryEvalDetail

Fournit des détails supplémentaires sur le traitement des stratégies CA Identity Manager, notamment les stratégies de membre, d'administration, de propriété et d'identité. Le support technique utilise ce composant de suivi.

Les champs de données pour lesquels vous configurez le suivi sont répertoriés dans le manuel *SiteMinder Web Access Manager Policy Server Administration Guide*.

Chapitre 11: Protection CA Identity Manager

Ce chapitre traite des sujets suivants :

Sécurité de la console d'utilisateur

La console d'utilisateur est l'interface utilisateur qui permet aux administrateurs de gérer des objets, tels que les utilisateurs, les groupes et les organisations dans un environnement CA Identity Manager. Un ensemble de rôles et de tâches associés sont affectés à ces objets. Lorsqu'un administrateur se connecte à la console d'utilisateur, les tâches associées à l'administrateur sont affichées dans cet environnement.

Par défaut, CA Identity Manager protège l'accès à la console d'utilisateur à l'aide de l'authentification native. Les administrateurs CA Identity Manager entrent un nom d'utilisateur et un mot de passe valides pour se connecter à un environnement CA Identity Manager. CA Identity Manager authentifie le nom et le mot de passe par rapport au référentiel d'utilisateurs géré par CA Identity Manager.

Si CA Identity Manager est intégré à SiteMinder, l'authentification de base SiteMinder est utilisée *automatiquement* pour protéger l'environnement. Aucune configuration supplémentaire n'est requise pour l'utilisation de l'authentification de base. Vous pouvez configurer des méthodes d'authentification avancées à l'aide de l'interface d'administration de SiteMinder.

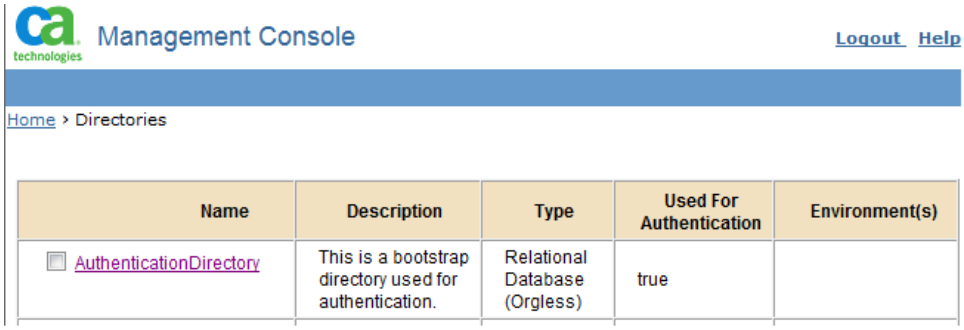
Remarque : Pour plus d'informations, consultez le manuel *SiteMinder Web Access Manager Policy Server Administration Guide*.

Sécurité de la console de gestion

La console de gestion permet aux administrateurs de créer et de gérer des annuaires et des environnements CA Identity Manager. Les administrateurs peuvent également utiliser la console de gestion pour configurer une fonctionnalité personnalisée pour un environnement.

L'installation CA Identity Manager inclut une option permettant de sécuriser la console de gestion. Cette option est sélectionnée par défaut. Pendant l'installation, vous spécifiez des informations d'identification que CA Identity Manager utilise pour authentifier l'administrateur qui peut accéder à la console de gestion. CA Identity Manager crée un utilisateur avec les informations d'identification que vous fournissez dans l'annuaire de démarrage AuthenticationDirectory. Vous pouvez afficher cet annuaire dans la console de gestion.

Remarque : Vous ne pouvez pas utiliser la sécurité native pour protéger la console de gestion lorsque CA Identity Manager est intégré à SiteMinder.



Ajout d'administrateurs de console de gestion supplémentaires

Par défaut, une console de gestion protégée par la sécurité CA Identity Manager native a un compte d'administrateur, qui est créé dans un nouvel annuaire CA Identity Manager pendant l'installation.

Pour ajouter des administrateurs supplémentaires, spécifiez un annuaire CA Identity Manager qui contient des utilisateurs devant accéder à la console de gestion. Utiliser un annuaire existant vous permet d'attribuer l'accès à la console de gestion aux utilisateurs de votre organisation, sans devoir créer de nouveaux comptes.

Vous pouvez uniquement spécifier un annuaire pour l'authentification. Vous ne pouvez pas supprimer un annuaire pendant sa configuration pour l'authentification.

Procédez comme suit:

1. Connectez-vous à la console de gestion avec les informations d'identification de l'utilisateur fournies pendant l'installation.
2. Cliquez sur Directories (Annuaires) et cliquez sur l'annuaire contenant les utilisateurs qui requièrent l'accès à la console de gestion.
3. Cliquez sur Update Authentication (Mettre à jour l'authentification).
4. Sélectionnez l'option Used for Authentication (Utilisé pour l'authentification).
5. Entrez le nom de connexion pour le premier utilisateur et cliquez sur Add (Ajouter).
6. Continuez d'ajouter des utilisateurs qui requièrent l'accès à la console de gestion jusqu'à ce que tous les utilisateurs aient été ajoutés. Cliquez ensuite sur Save (Enregistrer).

   Les utilisateurs que vous avez spécifiés peuvent désormais utiliser leur nom d'utilisateur et leur mot de passe pour accéder à la console de gestion.

Désactivation de la sécurité native pour la console de gestion

Si vous avez activé la sécurité native pour la console de gestion et que vous voulez utiliser une application différente pour la protéger, désactivez la sécurité native avant d'implémenter l'autre méthode de sécurisation.

Procédez comme suit:

1. Désactivez la sécurité native pour la console de gestion dans le fichier web.xml, comme suit :
   a. Ouvrez le fichier *chemin_installation_CA Identity Manager*\iam_im.ear\management_console.war\WEB-INF\web.xml dans un éditeur de texte.
   b. Définissez la valeur du paramètre Enable sur False pour l'attribut ManagementConsoleAuthFilter, comme suit :
   ```
   <filter>
   <filter-name>ManagementConsoleAuthFilter</filter-name>
   <filter-
   class>com.netegrity.ims.manage.filter.ManagementConsoleAuth
   Filter</filter-class>
   <init-param>
   <param-name>Enable</param-name>
   <param-value>false</param-value>
   </init-param>
   </filter>
   ```
   c. Enregistrez le fichier web.xml.
2. Redémarrez le serveur CA Identity Manager.

   La console de gestion n'est plus protégée par la sécurité native.

Utilisation de SiteMinder pour sécuriser la console de gestion

Pour protéger la console de gestion, vous pouvez créer une stratégie SiteMinder.

Une stratégie SiteMinder identifie une ressource que vous voulez protéger, comme la console de gestion, et attribue un ensemble d'accès utilisateur à cette ressource.

Procédez comme suit:

1. Désactivez la sécurité native (page 284) pour la console de gestion.
2. Connectez-vous à l'une des interfaces suivantes en tant qu'administrateur avec des droits sur le domaine :
   - Pour SiteMinder r12 ou version ultérieure, connectez-vous à l'interface d'administration.
   - Pour SiteMinder 6.0 SP*x*, connectez-vous à l'interface utilisateur du serveur de stratégies.

   Remarque : Pour plus d'informations sur l'utilisation de ces interfaces, consultez la documentation de la version de SiteMinder que vous utilisez.
3. Identifiez le domaine de stratégie pour l'environnement CA Identity Manager approprié.

   Ce domaine est créé automatiquement lorsque CA Identity Manager est intégré à SiteMinder. Le nom de domaine est au format suivant :

   *environnement_Identity_Manager*Domaine

   Dans ce format, *environnement_Identity_Manager* spécifie le nom de l'environnement que vous modifiez. Par exemple, lorsque le nom est *employés*, le nom de domaine est *employés*Domaine.
4. Créez un domaine avec le filtre de ressources suivant :

   /iam/immanage/
5. Créez une règle pour le domaine. Spécifiez un astérisque (*) comme filtre pour protéger toutes les pages de la console de gestion.
6. Créez une stratégie et associez-la à la règle que vous avez créée à l'étape précédente.

   Vérifiez que les utilisateurs que vous associez peuvent accéder à la console de gestion via la stratégie.
7. Redémarrez le serveur d'applications.

Protection d'un environnement existant après la mise à niveau

Après avoir procédé à la mise à niveau de CA Identity Manager 12.6 ou d'une version ultérieure, vous pouvez protéger la console de gestion à l'aide de la sécurité native.

Remarque : Vous ne pouvez pas utiliser la sécurité native de CA Identity Manager pour protéger la console de gestion lorsque CA Identity Manager est intégré à SiteMinder.

Procédez comme suit:

1. Activez la sécurité native pour la console de gestion dans le fichier web.xml, comme suit :
   a. Ouvrez le fichier *chemin_installation_CA Identity Manager*\iam_im.ear\management_console.war\WEB-INF\web.xml dans un éditeur de texte.
   b. Définissez la valeur du paramètre Enable sur True pour l'attribut ManagementConsoleAuthFilter, comme suit :
   ```
   <filter>
   <filter-name>ManagementConsoleAuthFilter</filter-name>
   <filter-
   class>com.netegrity.ims.manage.filter.ManagementConsoleAuth
   Filter</filter-class>
   <init-param>
   <param-name>Enable</param-name>
   <param-value>true</param-value>
   </init-param>
   </filter>
   ```
   c. Enregistrez le fichier web.xml.
2. Créez la table IM_AUTH_USER dans le référentiel d'objets CA Identity Manager.

   La table IM_AUTH_USER stocke les informations sur les administrateurs de la console de gestion.
   a. Accédez au référentiel CA\Identity Manager\IAM Suite\Identity Manager\tools\db\objectstore.
   b. Exécutez l'un des scripts suivants sur le référentiel d'objets :
      - sql_objectstore.sql
      - oracle_objectstore.sql

   Remarque : Pour plus d'informations sur l'exécution d'un script sur une base de données existante, consultez la documentation de cette base de données.

3. Utilisez l'outil de modification de mots de passe pour chiffrer le mot de passe de l'utilisateur.

   L'outil de modification de mots de passe est installé avec les outils CA Identity Manager à l'emplacement suivant :

Windows : C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\PasswordTool

UNIX : /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/PasswordTool

   PasswordTool

   Exécutez l'outil de modification de mots de passe à l'aide de la commande suivante :

   `pwdtools -JSAFE -p mot_passe`

   L'option JSAFE chiffre une valeur de texte brut à l'aide de l'algorithme PBE.

1. Insérez les informations d'utilisateur de démarrage dans la table IM_AUTH_USER. Spécifiez des valeurs pour toutes les colonnes de cette table.

   Exemple :

   USER_NAME: admin1

   PASSWORD: *mot_de_passe*

   DISABLED: 0

   ID:1

2. Redémarrez le serveur CA Identity Manager.

   La console de gestion est protégée par la sécurité native.

Protection contre les attaques CSRF

CA Identity Manager offre une fonctionnalité pour améliorer la résistance aux attaques de falsification de demande intersites (CSRF). Par défaut, cette fonctionnalité est désactivée.

Pour l'activer, procédez comme suit

1. Ouvrez le fichier web.xml situé à l'emplacement suivant :

   serveur_applications/iam_im.ear/user_console.war/WEB-INF

2. Recherchez l'élément <context-param> avec la balise <param-name> csrf-prevention-on.
3. Définissez <param-value> sur True.
4. Redémarrez le serveur d'applications.

Chapitre 12: Intégration avec SiteMinder

Ce chapitre traite des sujets suivants :

SiteMinder et CA Identity Manager

Lorsque CA Identity Manager est intégré à SiteMinder, la fonctionnalité SiteMinder suivante est ajoutée à l'environnement CA Identity Manager :

Authentification avancée

CA Identity Manager inclut une authentification native pour les environnements CA Identity Manager par défaut. Les administrateurs CA Identity Manager entrent un nom d'utilisateur et un mot de passe valides pour se connecter à un environnement CA Identity Manager. CA Identity Manager authentifie le nom et le mot de passe par rapport au référentiel d'utilisateurs géré par CA Identity Manager.

Si CA Identity Manager est intégré à SiteMinder, CA Identity Manager utilise l'authentification de base SiteMinder pour protéger l'environnement. Lorsque vous créez un environnement CA Identity Manager, un domaine de stratégie et un schéma d'authentification sont créés dans SiteMinder pour protéger l'environnement.

Lorsque l'intégration est configurée, vous pouvez également utiliser l'authentification SiteMinder pour protéger la console de gestion.

Tâches et rôles d'accès

Les rôles d'accès permettent aux administrateurs CA Identity Manager d'affecter des droits dans les applications protégées par SiteMinder. Ces rôles d'accès représentent une action unique qu'un utilisateur peut effectuer dans une application métier, telle que la génération d'un bon de commande dans une application financière.

Mappage d'annuaires

Un administrateur peut devoir gérer des utilisateurs dont les profils existent dans un référentiel d'utilisateurs différent de celui utilisé pour authentifier l'administrateur. Lors de la connexion à l'environnement CA Identity Manager, l'administrateur est authentifié à l'aide d'un annuaire et un autre annuaire est utilisé pour l'autoriser à gérer des utilisateurs.

Lorsque CA Identity Manager est intégré à SiteMinder, vous pouvez configurer un environnement CA Identity Manager de façon à utiliser des annuaires différents pour l'authentification et pour l'autorisation.

Apparences pour différents ensembles d'utilisateurs

Une apparence permet de personnaliser la console d'utilisateur. Lorsque CA Identity Manager est intégré à SiteMinder, vous pouvez autoriser des ensembles d'utilisateurs à afficher des apparences différentes. Pour cela, vous utilisez une réponse SiteMinder vous permettant d'associer une apparence à un ensemble d'utilisateurs. La réponse est associée avec une règle dans une stratégie, qui est associée à un ensemble d'utilisateurs. Lorsque la règle se déclenche, une réponse contenant les informations sur l'apparence CA Identity Manager est envoyée pour permettre la création de la console d'utilisateur.

Remarque : Pour plus d'informations, consultez le *Manuel de conception de la console d'utilisateur*.

Préférences des paramètres régionaux dans un environnement localisé

Lorsque CA Identity Manager est intégré à SiteMinder, vous pouvez définir des préférences de paramètres régionaux pour un utilisateur à l'aide d'un en-tête HTTP imlanguage. Dans le serveur de stratégies SiteMinder, vous définissez cet en-tête dans une réponse SiteMinder et spécifiez un attribut d'utilisateur comme valeur de celui-ci. Cet en-tête imlanguage est défini comme la préférence de paramètres régionaux prioritaire pour un utilisateur.

Remarque : Pour plus d'informations, consultez le *Manuel de conception de la console d'utilisateur*.

Protection des ressources

L'authentification avancée requiert l'utilisation d'un serveur de stratégies SiteMinder dans votre implémentation. Le serveur d'applications hébergeant le serveur CA Identity Manager est exécuté dans un environnement d'exploitation différent du serveur Web. Pour fournir des services de transfert, le serveur Web requiert :

- Un module d'extension de serveur d'applications d'un fournisseur.
- Un agent SiteMinder pour protéger les ressources CA Identity Manager, comme la console d'utilisateur, l'auto-enregistrement et la fonctionnalité de mot de passe oublié.

L'agent Web contrôle l'accès des utilisateurs qui demandent des ressources CA Identity Manager. Une fois que les utilisateurs sont authentifiés et autorisés, l'agent Web permet au serveur Web de traiter les demandes.

Lorsque le serveur Web reçoit la demande, le module d'extension du serveur d'applications l'envoie au serveur d'applications hébergeant le serveur CA Identity Manager.

L'agent Web protège les ressources CA Identity Manager auxquelles les utilisateurs et les administrateurs ont accès.

Présentation de l'intégration de SiteMinder et CA Identity Manager

Lorsque l'administrateur de stratégie et l'administrateur d'identité travaillent ensemble pour intégrer SiteMinder dans une installation CA Identity Manager existante, l'architecture CA Identity Manager est étendue de manière à inclure les composants suivants :

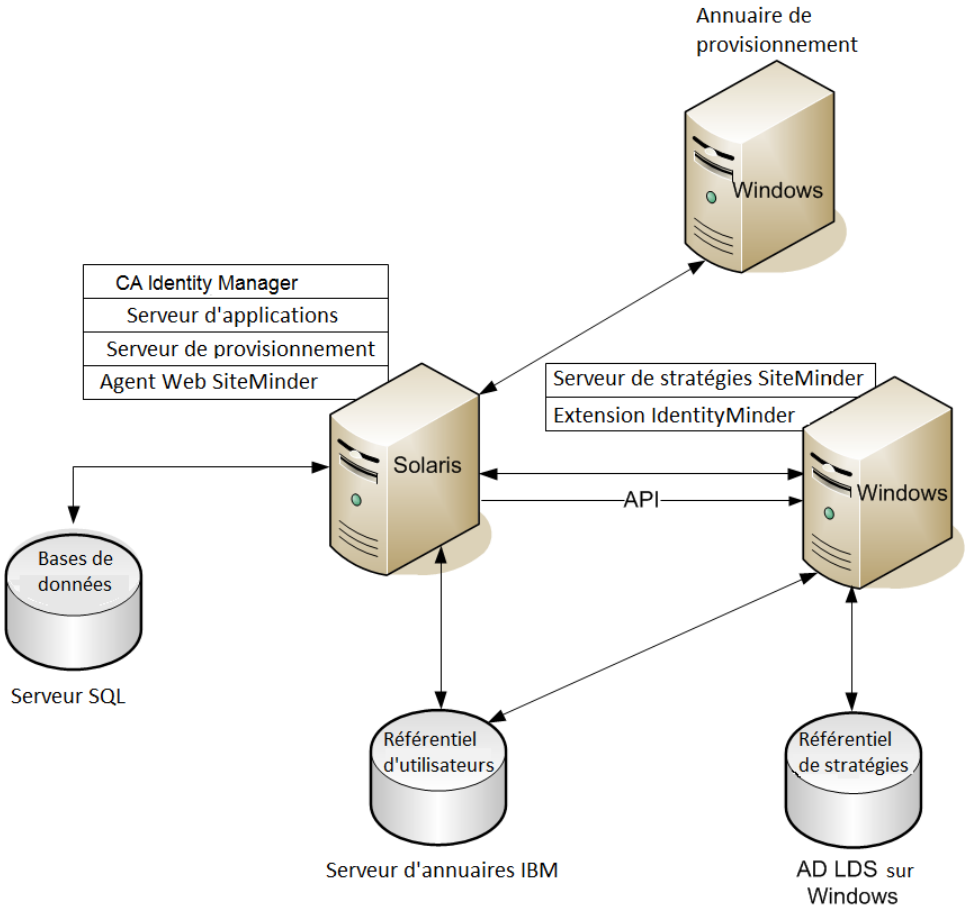
Agent Web SiteMinder

Protège le serveur CA Identity Manager. L'agent Web est installé sur le système comprenant le serveur CA Identity Manager.

Serveur de stratégies SiteMinder

Permet l'authentification et l'autorisation avancées pour CA Identity Manager.

L'illustration suivante est un exemple d'installation CA Identity Manager comprenant un serveur de stratégies et l'agent Web SiteMinder :

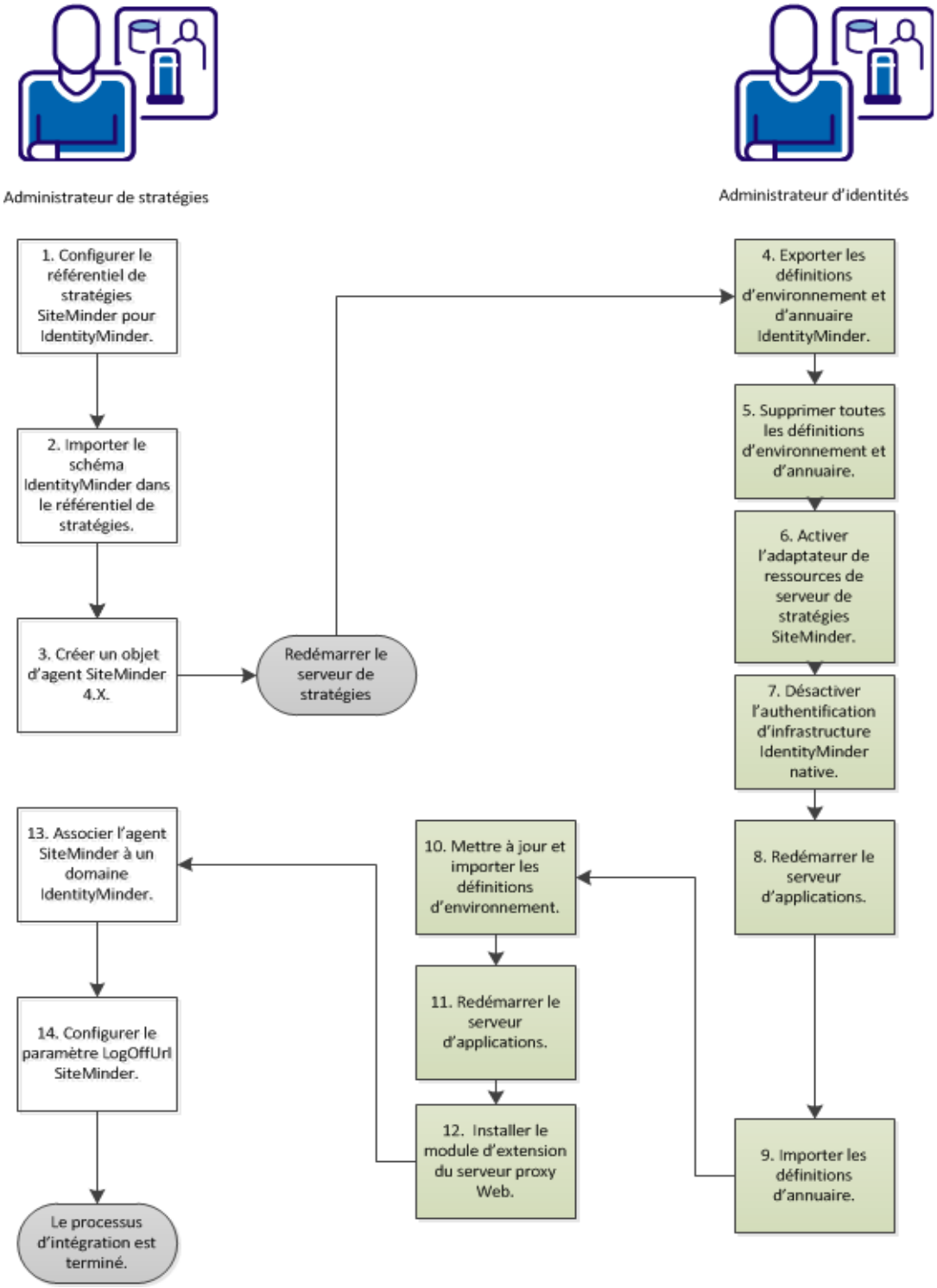


Remarque : Les composants sont installés sur des plates-formes différentes à des fins d'exemple. Toutefois, vous pouvez choisir d'autres plates-formes. Les bases de données CA Identity Manager se trouvent sur le serveur Microsoft SQL Server et le référentiel d'utilisateurs se trouve sur le serveur d'annuaire IBM. Le référentiel de stratégies SiteMinder se trouve sur le serveur AD LDS Windows.

Pour effectuer cette procédure, deux rôles sont requis : l'administrateur d'identité CA Identity Manager et l'administrateur de stratégie SiteMinder. Dans certaines organisations, une personne remplit ces deux rôles. Lorsque deux personnes sont nécessaires, une collaboration étroite est de mise pour effectuer les procédures de ce scénario. L'administrateur de stratégie commence et termine le processus, alors que toutes les étapes intermédiaires incombent à l'administrateur d'identité.

Important : Pour les installations CA Identity Manager à partir de la version 12.5 SP7, les bibliothèques Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files sont requises. Téléchargez-les à partir du site Web d'Oracle, puis chargez-les dans le dossier suivant : <Java_path>\<jdk_version>\jre\lib\security\.

Le diagramme suivant illustre le processus complet d'intégration de SiteMinder dans CA Identity Manager :



Procédez comme suit:

1. Configurez le référentiel de stratégies SiteMinder pour CA Identity Manager. (page 296)
2. Importez le schéma CA Identity Manager dans le référentiel de stratégies. (page 302)
3. Créez un objet d'agent 4.X SiteMinder. (page 302)
4. Exportez les annuaires et les environnements CA Identity Manager. (page 304)
5. Supprimez toutes les définitions d'annuaire et d'environnement. (page 305)
6. Activez l'adaptateur de ressource de serveur de stratégies SiteMinder. (page 306)
7. Désactivez le filtre d'authentification de structure CA Identity Manager natif. (page 307)
8. Redémarrez le serveur d'applications. (page 308)
9. Configurez une source de données pour SiteMinder. (page 308)
10. Importez les définitions d'annuaire. (page 309)
11. Mettez à jour et importez les définitions d'environnement. (page 310)
12. Redémarrez le serveur d'applications. (page 308)
13. Installez le module d'extension de serveur proxy Web. (page 310)
14. Associez l'agent SiteMinder à un domaine CA Identity Manager. (page 330)
15. Configurez le paramètre SiteMinder LogOffUrl. (page 330)

Configuration du référentiel de stratégies SiteMinder pour CA Identity Manager

Le rôle d'administrateur de stratégie vous amène à utiliser les outils d'administration CA Identity Manager pour accéder aux scripts SQL ou au texte de schéma LDAP afin d'ajouter le schéma de solution de gestion des identités au référentiel de stratégies. L'administrateur d'identité a installé ces outils dans le dossier Outils d'administration. Suivez l'*une* des procédures suivantes pour configurer le référentiel de stratégies :

Configurer une base de données relationnelles (page 296)

Configurer Sun Java Systems Directory Server ou IBM Directory Server (page 297)

Configurer Microsoft Active Directory (page 297)

Configurer Microsoft ADAM (page 298)

Configurer un serveur CA Directory (page 299)

Configurer un serveur Novell eDirectory (page 300)

Configurer Oracle Internet Directory (OID) (page 301)

Configurer une base de données relationnelles

Une fois la configuration effectuée, vous pouvez utiliser la base de données relationnelles comme référentiel de stratégies SiteMinder.

Procédez comme suit:

1. Configurez la base de données comme référentiel de stratégies SiteMinder pris en charge.

   Remarque : Pour obtenir des instructions de configuration, consultez le manuel *SiteMinder Policy Server Installation Guide.*

2. Exécutez le script approprié pour votre base de données :

   - **SQL :** <chemin_installation>\tools\policystore-schemas\MicrosoftSQLServer\ims8_mssql_ps.sql
   - **Oracle :** <chemin_installation2>/tools/policystore-schemas/OracleRDBMS/ims8_oracle_ps.sql

   Les chemins d'accès précédents sont des emplacements d'installation par défaut. L'emplacement pour votre installation peut varier.

Configuration de Sun Java Systems Directory Server ou IBM Directory Server

Pour configurer un serveur d'annuaire Java ou IBM, appliquez le fichier de schéma approprié.

Procédez comme suit:

1. Configurez l'annuaire en tant que référentiel de stratégies CA SiteMinder pris en charge.

   Remarque : Pour obtenir des instructions de configuration, consultez le *Manuel d'installation du serveur de stratégies CA SiteMinder.*

2. Ajoutez le fichier de schéma LDIF approprié à l'annuaire. L'emplacement Windows par défaut pour les fichiers LDIF est <chemin_installation>\tools\policystore-schemas.

   Ajoutez les fichiers de schéma suivants pour votre annuaire :

   - **Serveur IBM Directory Server :**

     IBMDirectoryServer\V3.identityminder8

   - **Serveur Sun Java Systems Directory Server (iPlanet) :**

     SunJavaSystemDirectoryServer\sundirectory_ims8.ldif

Configuration de Microsoft Active Directory

Pour configurer un référentiel de stratégies Microsoft Active Directory, appliquez le script activedirectory_ims8.ldif.

Procédez comme suit:

1. Configurez l'annuaire en tant que référentiel de stratégies CA SiteMinder pris en charge.

   Remarque : Pour obtenir des instructions de configuration, consultez le *Manuel d'installation du serveur de stratégies CA SiteMinder.*

2. Modifiez le fichier de schéma activedirectory_ims8.ldif comme suit :

   a. Dans un éditeur de texte, ouvrez le fichier activedirectory_ims8.ldif. Par défaut, il se trouve à l'emplacement Windows suivant :

      <chemin_installation>\tools\policystore-schemas\MicrosoftActiveDirectory

   b. Remplacez toutes les instances de {root} par l'organisation racine de l'annuaire.

      L'organisation racine doit correspondre à celle que vous avez spécifiée lors de la configuration du référentiel de stratégies dans la console de gestion du serveur de stratégies.

Par exemple, si la racine est dc=myorg,dc=com, remplacez dn: CN=imdomainid6,CN=Schema,CN=Configuration,{root} par dn: CN=imdomainid6,CN=Schema,CN=Configuration,dc=myorg,dc=com.

c. Enregistrez le fichier.

3. Ajoutez le fichier de schéma suivant la méthode décrite dans la documentation de votre annuaire.

Configuration de Microsoft ADAM

Pour configurer un référentiel de stratégies Microsoft ADAM, appliquez le script adam_ims8.ldif.

Procédez comme suit:

1. Configurez l'annuaire en tant que référentiel de stratégies CA SiteMinder pris en charge.

   Remarque : Pour obtenir des instructions de configuration, consultez le *Manuel d'installation du serveur de stratégies CA SiteMinder.*

   Notez la valeur du nom commun (GUID).

2. Modifiez le fichier de schéma adam_ims8.ldif comme suit :

   a. Ouvrez le fichier adam_ims8.ldif\.ldif dans un éditeur de texte. Par défaut, il se trouve à l'emplacement Windows suivant :

      <chemin_installation>\tools\policystore-schemas\MicrosoftActiveDirectory

   b. Remplacez toutes les références cn={guid} par la chaîne que vous avez obtenue lors de la configuration du référentiel de stratégies SiteMinder à l'étape 1 de cette procédure.

      Par exemple, si la chaîne de GUID est CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8}, remplacez toutes les références cn={guid} par cette chaîne.

   c. Enregistrez le fichier.

3. Ajoutez le fichier de schéma suivant la méthode décrite dans la documentation de votre annuaire.

Configuration de CA Directory Server

Pour configurer un serveur CA Directory, créez un fichier de schéma personnalisé. Dans les étapes qui suivent, *répertoire_installation_dxserver* est le répertoire d'installation de CA Directory. L'emplacement source par défaut pour ce fichier sur Windows est <chemin_installation>\tools\policystore-schemas\eTrustDirectory.

Procédez comme suit:

1. Configurez l'annuaire en tant que référentiel de stratégies CA SiteMinder pris en charge.

   Remarque : Pour obtenir des instructions de configuration, consultez le *Manuel d'installation du serveur de stratégies CA SiteMinder.*

2. Copiez etrust_ims8.dxc dans *répertoire_installation_dxserver*\config\schema.

3. Créez un fichier de configuration de schéma personnalisé comme suit :

   a. Copiez le fichier *répertoire_installation_dxserver*\config\schema\default.dxg dans *répertoire_installation_dxserver*\config\schema*nom_société*-schema.dxg.

   b. Modifiez le fichier *répertoire_installation_dxserver*\config\schema*nom_société*-schema.dxg en ajoutant les lignes suivantes au bas du fichier :

   ```
   # Identity Manager Schema
   source "etrust_ims8.dxc";
   ```

4. Modifiez le fichier *répertoire_installation_dxserver*\bin\schema.txt en ajoutant le contenu du fichier etrust_ims_schema.txt en bas du fichier. L'emplacement source par défaut pour ce fichier sur Windows est <chemin_installation>\tools\policystore-schemas\eTrustDirectory.

5. Créez un fichier de configuration de limites personnalisé comme suit :

   a. Copiez le fichier *répertoire_installation_dxserver*\config\limits\default.dxc dans *répertoire_installation_dxserver*\config\limits*nom_société*-limits.dxc.

   b. Augmentez la limite de taille par défaut à 5000 dans le fichier *répertoire_installation_dxserver*\config\limits*nom_société*-limits.dxc, comme suit :

   ```
   set max-op-size=5000
   ```

   Remarque : La mise à niveau de CA Directory remplace le fichier limits.dxc. Par conséquent, assurez-vous de réinitialiser le paramètre max-op-size sur 5000 à la fin de la mise à niveau.

6. Modifiez le fichier *répertoire_installation_dxserver*\config\servers*nom_dsa*.dxi comme suit :

```
# schema
source "nom_société-schema.dxg";

#service limits
source "nom_société-limits.dxc";
```

où *nom_dsa* est le nom de l'appliance de stockage de données qui utilise les fichiers de configuration personnalisés.

7. Exécutez l'utilitaire dxsyntax.
8. Arrêtez et redémarrez l'appliance de stockage de données en tant qu'utilisateur dsa pour appliquer les modifications apportées au schéma, comme suit :

```
dxserver stop nom_dsa
dxserver start nom_dsa
```

Configuration d'un serveur Novell eDirectory

Pour configurer un référentiel de stratégies Novell eDirectory, appliquez le script novell_ims8.ldif.

Procédez comme suit:

1. Configurez l'annuaire en tant que référentiel de stratégies CA SiteMinder pris en charge.

   Remarque : Pour obtenir des instructions de configuration, consultez le *Manuel d'installation du serveur de stratégies CA SiteMinder.*

2. Déterminez le nom unique de la variable NCPServer du serveur Novell eDirectory en entrant les informations suivantes dans une fenêtre de commande dans le système sur lequel le serveur de stratégies est installé :

```
ldapsearch -h nom_hôte -p port -b conteneur -s sub
-D info_connexion_admin -w mot_passe objectClass=ncpServer dn
```

   Exemple :

```
ldapsearch -h 192.168.1.47 -p 389 -b "o=nwqa47container" -s sub -D
"cn=admin,o=nwqa47container" -w password objectclass=ncpServer dn
```

3. Ouvrez le fichier novell_ims8.ldif.
4. Remplacez toutes les variables NCPServer par la valeur obtenue à l'étape 2.

   L'emplacement par défaut pour novell_ims8.ldif sur Windows est :

   <chemin_installation>\tools\policystore-schemas\NovelleDirectory

   Par exemple, si la valeur de nom unique est cn=servername,o=servercontainer, vous remplacez toutes les instances de *NCPServer* par cn=servername,o=servercontainer.

5. Mettez à jour le serveur eDirectory avec le fichier novell_ims8.ldif.

   Pour obtenir des instructions, consultez la documentation de Novell eDirectory.

Configuration d'Oracle Internet Directory (OID)

Pour configurer un annuaire Oracle Internet Directory, mettez à jour le fichier oracleoid ldif.

Procédez comme suit:

1. Configurez l'annuaire en tant que référentiel de stratégies CA SiteMinder pris en charge.

   Remarque : Pour obtenir des instructions de configuration, consultez le *Manuel d'installation du serveur de stratégies CA SiteMinder.*

2. Mettez à jour le serveur Oracle Internet Directory avec le fichier oracleoid_ims8.ldif. L'emplacement d'installation par défaut pour ce fichier sur Windows est :

   chemin_installation\policystore-schemas\OracleOID\

   Pour obtenir des instructions, consultez la documentation Oracle Internet Directory.

Vérification du référentiel de stratégies

Pour vérifier le référentiel de stratégies, confirmez les points suivants :

- Le journal du serveur de stratégies ne contient aucune section d'avertissement qui commence par le code suivant :

  ```
  *** IMS NO SCHEMA BEGIN
  ```

  Cet avertissement s'affiche uniquement si vous avez installé les extensions pour le serveur de stratégies SiteMinder sans étendre le schéma du référentiel de stratégies.

- Les objets CA Identity Manager existent dans l'annuaire ou dans la base de données du référentiel de stratégies. Les objets CA Identity Manager commencent par un préfixe ims.

Importation du schéma CA Identity Manager dans le référentiel de stratégies

L'administrateur de stratégie importe le schéma CA Identity Manager dans le référentiel de stratégies. Cette tâche permet de créer, de mettre à jour et de supprimer des objets de stratégie dans CA Identity Manager, notamment des objets d'annuaire, des domaines, des règles, des stratégies et les objets de stratégie qui activent les tâches et les rôles d'accès.

Procédez comme suit:

1. Dans le serveur de stratégies SiteMinder, arrêtez le service du serveur de stratégies.
2. Exécutez le programme d'installation CA Identity Manager pour la version que vous utilisez.
3. Lorsque vous êtes invité à confirmer les composants à installer, sélectionnez les extensions pour SiteMinder, si SiteMinder est installé localement.
4. Vérifiez que le service de serveur de stratégies a redémarré avant de poursuivre.

Création d'un objet d'agent 4.X SiteMinder

L'administrateur de stratégie crée un agent Web 4.x SiteMinder. Cet agent permet d'activer les communications entre SiteMinder et CA Identity Manager. L'administrateur d'identité référence l'agent pendant la configuration CA Identity Manager.

Procédez comme suit:

1. Connectez-vous à l'interface d'administration SiteMinder.

   Les onglets s'affichent selon les droits d'administrateur dont vous disposez.
2. Cliquez sur Infrastructure, Agents, Agent, Créer un agent.

   La boîte de dialogue Créer un agent s'affiche.
3. Sélectionnez Créer un objet de type Agent, puis cliquez sur OK.

   La boîte de dialogue Créer un agent s'affiche.
4. Saisissez un nom et une description facultative.

   Remarque : Utilisez un nom que vous pouvez facilement associer à l'assistant de connexion SharePoint correspondant.

5. Sélectionnez SiteMinder.
6. Dans la liste déroulante, sélectionnez Agent Web.
7. Activez la fonctionnalité 4.x avec les étapes suivantes :
   a. Cochez la case Prise en charge des agents 4.x.

      Les champs de paramètres de confiance s'affichent.

   b. Ajoutez les paramètres de confiance en remplissant les champs suivants :

      Adresse IP

      Indique l'adresse IP du serveur de stratégies.

      Secret partagé

      Spécifiez le mot de passe associé à l'objet d'agent 4.x. L'assistant de connexion SharePoint requiert également ce mot de passe.

      Confirmer le secret

      Confirmez le mot de passe associé à l'objet d'agent 4.x. L'assistant de connexion SharePoint requiert également une confirmation du mot de passe.
8. Cliquez sur Soumettre.

   La tâche de création d'objet d'agent est soumise pour traitement et un message de confirmation s'affiche.

Exportation des annuaires et des environnements CA Identity Manager

Le processus d'intégration supprime toutes les définitions d'environnement et d'annuaires actuelles. Pour conserver ces informations, l'administrateur d'identité doit exporter les environnements à l'aide de la console de gestion CA Identity Manager. Une fois l'intégration terminée, les définitions permettent de restaurer les annuaires et les environnements.

Procédez comme suit:

1. Ouvrez la console de gestion CA Identity Manager.
2. Cliquez sur Directories (Annuaires).
3. Cliquez sur le premier annuaire de la liste et cliquez sur Export (Exporter).
4. Enregistrez et archivez le fichier XML de l'annuaire.
5. Répétez cette procédure pour les annuaires restants.
6. Cliquez sur Home (Accueil), puis sur Environments (Environnements).
7. Sélectionnez le premier environnement.
8. Cliquez sur Exporter.
9. Répétez cette procédure pour les environnements restants.

   Remarque : Ce processus peut prendre plusieurs minutes pour chaque environnement.

Suppression de toutes les définitions d'annuaire et d'environnement

Pour préparer la protection de CA Identity Manager par SiteMinder, l'administrateur d'identité supprime les définitions d'annuaire et d'environnement à l'aide de la console de gestion CA Identity Manager.

Procédez comme suit:

1. Ouvrez la console de gestion CA Identity Manager.
2. Cliquez sur Environnements.
3. Sélectionnez le premier environnement.
4. Cliquez sur Supprimer.
5. Répétez ce processus pour les environnements restants.

   Remarque : Supprimez les environnements avant de supprimer les annuaires, car les environnements référencent les annuaires.
6. Revenez à la section Directories (Annuaires).
7. Sélectionnez tous les annuaires répertoriés.
8. Cliquez sur Supprimer.

Activation de l'adaptateur de ressource de serveur de stratégies SiteMinder

L'administrateur d'identité active l'adaptateur de ressource de serveur de stratégies SiteMinder. Le but de cet adaptateur est de valider le cookie SMSESSION. Une fois la validation effectuée, SiteMinder crée le contexte d'utilisateur.

Procédez comme suit:

1. Accédez au dossier \policysever.rar\META-INF situé dans le fichier iam_im.ear du serveur d'applications qui exécute CA Identity Manager.
2. Ouvrez le fichier ra.xml dans un éditeur.
3. Recherchez la propriété de configuration Enabled, puis changez sa valeur sur True, comme dans l'exemple suivant :

```
        <config-property-name>validateSmHeadersWithPS</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
    </config-property>
    <config-property>
        <config-property-name>Enabled</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
    </config-property>
    <!-- Set FIPS Mode to true if SiteMinder is in FIPS Only Mode -->
    <config-property>
        <config-property-name>FIPSMode</config-property-name>
```

4. Recherchez la propriété ConnectionURL et indiquez le nom d'hôte du serveur de stratégies SiteMinder. Utilisez un nom de domaine complet.
5. Recherchez la propriété UserName et spécifiez le compte à utiliser pour les communications avec SiteMinder. SiteMinder est la valeur par défaut pour ce compte.
6. Recherchez la propriété AdminSecret. Spécifiez le mot de passe chiffré. Copiez le mot de passe à partir du fichier directory.xml que vous avez exporté et collez-le dans le fichier ra.xml. Si vous n'êtes pas sûr de disposer d'un mot de passe commun, chiffrez votre mot de passe à l'aide de l'outil de modification de mots de passe CA Identity Manager.
7. Collez le mot de passe chiffré dans le fichier ra.xml.
8. Spécifiez le nom de l'agent 4.x que l'administrateur de stratégie a créé lors de la configuration de SiteMinder.
9. Spécifiez le mot de passe chiffré. Utilisez l'outil de modification de mots de passe pour chiffrer le mot de passe, si nécessaire.
10. Enregistrez les modifications apportées dans le fichier ra.xml.

L'adaptateur de ressource de serveur de stratégies SiteMinder est activé.

Informations complémentaires :

Modification d'un mot de passe ou d'un secret partagé SiteMinder (page 363)

Désactivation du filtre d'authentification de structure CA Identity Manager natif

Une fois que vous avez mis en place l'adaptateur SiteMinder, le filtre d'authentification de structure n'est plus nécessaire. L'administrateur d'identité peut désactiver le filtre.

Procédez comme suit:

1. Recherchez et modifiez le fichier web.xml dans le dossier \user_console.war\WEB-INF sous iam_im.ear.
2. Recherchez le filtre FrameworkAuthFilter et remplacez la valeur du paramètre init-param Enable par False.

   Si vous utilisez CA Identity Manager r12.5 SP7 ou une version ultérieure, vérifiez que les bibliothèques Java Cryptographic Extension Unlimited Strength Jurisdiction Policy Files sont téléchargées dans \<chemin_accès_Java>\<version_jdk>\jre\lib\security dans l'environnement CA Identity Manager. Ces fichiers permettent les connections entre CA Identity Manager et SiteMinder.

   Si les bibliothèques JCE sont installées, les messages suivants sont affichés lors du démarrage de l'application CA Identity Manager :

   ```
   2012-07-06 11:23:56,079 WARN  [ims.default] (main) * Startup Step 2 :
   Attempting to start PolicyServerService
   2012-07-06 11:23:56,081 WARN  [ims.default] (main) Unlimited Strength Java
   Crypto Extensions enabled: TRUE
   ```

   Dans le cas contraire, la valeur de l'entrée Unlimited Strength Java Crypto Extensions enabled est False et un échec de la connexion de CA Identity Manager au serveur de stratégies se produit.

Redémarrage du serveur d'applications

Le redémarrage du serveur d'applications permet d'appliquer les modifications apportées. L'administrateur d'identité valide le basculement opéré et confirme qu'une connexion au serveur de stratégies SiteMinder existe.

Procédez comme suit:

1. Utilisez le panneau de services pour redémarrer CA Identity Manager lorsque votre serveur d'applications est exécuté en tant que service.
2. Pour valider la connexion, reportez-vous au journal server.log.

Configuration d'une source de données pour SiteMinder

Si votre environnement CA Identity Manager utilise une base de données relationnelles pour son référentiel d'identités, l'administrateur d'identité doit exécuter un processus supplémentaire sur le serveur de stratégies SiteMinder. SiteMinder requiert une source de données locale pour communiquer avec la base de données.

Procédez comme suit:

1. Pour les serveurs Windows, ouvrez la console Administrateur de sources de données ODBC qui se trouve sous Outils d'administration.
2. Cliquez sur l'onglet Nom DSN système.
3. Cliquez sur Ajouter et sélectionnez le pilote SiteMinder correspondant pour votre base de données.
4. Fournissez les informations requises pour référencer le référentiel d'utilisateurs de la base de données relationnelles.
5. Avant de poursuivre, testez la connectivité.

Importation des définitions d'annuaire

Pour préparer l'importation des environnements, l'administrateur d'identité importe les annuaires référencés dans les environnements. Importer la définition des annuaires dans CA Identity Manager permet également d'ajoute les informations d'annuaire au référentiel de stratégies SiteMinder.

Procédez comme suit:

1. Vérifiez que CA Identity Manager est en cours d'exécution et connecté à SiteMinder.
2. Accédez à la console de gestion CA Identity Manager.
3. Cliquez sur Directories (Annuaires), puis cliquez sur Create or Update from XML (Créer ou mettre à jour à partir du fichier XML).
4. Sélectionnez le fichier de configuration d'annuaire (directory.xml). Il s'agit du fichier que vous avez exporté à l'étape Exportation des annuaires et des environnements CA Identity Manager (page 304).
5. Cliquez sur Suivant.
6. Cliquez sur Finish (Terminer) et vérifiez le résultat du chargement. Vérifiez que l'annuaire se trouve dans CA Identity Manager et SiteMinder.
7. Répétez ces étapes pour le référentiel de provisionnement et tous les annuaires restants.
8. Connectez-vous à l'interface d'administration SiteMinder pour valider la création des annuaires d'utilisateur.

Mise à jour et importation des définitions d'environnement

L'administrateur d'identité importe les environnements mis à jour dans CA Identity Manager.

Procédez comme suit:

1. Contrairement aux exportations d'annuaire, l'exportation d'environnement s'effectue par l'entremise d'un fichier ZIP. Extrayez une copie du fichier *nom*.xml à partir du fichier ZIP.
2. Copiez le fichier *nom*.xml. Insérez la référence suivante dans l'agent protecteur (pas l'agent 4.x SM) à la fin de l'élément ImsEnvironment, avant la balise /> : *agent="idmadmin"*
3. Enregistrez le fichier et collez-le dans le fichier ZIP.
4. Ouvrez la console de gestion CA Identity Manager et cliquez sur Environments (Environnements), puis Import (Importer).
5. Entrez le nom du fichier ZIP d'environnement mis à jour.
6. Cliquez sur Finish (Terminer) et vérifiez le résultat de l'importation.
7. Répétez ce processus pour tous les environnements restants.
8. Redémarrez le serveur d'applications.

Installation du module d'extension de serveur proxy Web

Selon les applications installées, les administrateurs d'identité installent l'un des modules d'extension suivants que le serveur Web utilise pour envoyer des demandes au serveur d'applications :

- WebSphere (page 311)
- JBoss (page 318)
- WebLogic (page 322)

Installation du module d'extension de proxy sur WebSphere

Le serveur Web sur lequel vous avez installé l'agent Web envoie des demandes au serveur d'applications qui héberge le serveur CA Identity Manager. Le module d'extension de proxy de serveur Web fournit ce service.

Utilisez les procédures applicables à votre déploiement :

1. Configurer le serveur HTTP IBM (page 311) (tous les serveurs Web)
2. Configurer le module d'extension de proxy (page 312) (tous les serveurs Web)
3. L'une des solutions suivantes :
   - Effectuer la configuration sur IIS (page 315)
   - Effectuer la configuration sur iPlanet ou Apache (page 317)

Configuration du serveur HTTP IBM

Pour tous les serveurs Web, vous installez le module d'extension de proxy et utilisez la commande configurewebserver.

Procédez comme suit:

1. Installez le module d'extension de proxy à partir de la zone de lancement de WebSphere.
2. Ajoutez le serveur Web à la cellule WebSphere en exécutant la commande configurewebserver1.bat comme suit :
   a. Ouvrez *répertoire_installation_websphere*\Plugins\bin\configurewebserver1.bat/,sh dans un éditeur de texte.
   b. Ajoutez un nom d'utilisateur et un mot de passe après wsadmin.bat/.sh comme suit :
   ```
   wsadmin.bat -user wsadmin -password mot de passe -f
   configureWebserverDefinition.jacl
   ```
   c. Exécutez configurewebserver1.bat/.sh.

   Remarque : Pour plus d'informations sur la commande configurewebserver, consultez la documentation IBM WebSphere.
3. Poursuivez la procédure de configuration du module d'extension de proxy (page 312).

Configuration du module d'extension de proxy

Pour tous les serveurs Web, mettez à jour le module d'extension à l'aide de la commande GenPluginCfg de WebSphere :

Procédez comme suit:

1. Connectez-vous au système sur lequel WebSphere est installé.
2. A partir de la ligne de commande, accédez à *répertoire_installation_websphere*\bin, où *répertoire_installation_websphere* est l'emplacement d'installation de WebSphere.

   Exemple :

   - **Windows :**

     C:\Program Files\WebSphere\AppServer\profile\AppSrv01\bin

   - **UNIX :**

     /*répertoire_installation*/WebSphere/AppServer/profile/AppSrv01/bin

3. Exécutez la commande GenPluginCfg.bat ou GenPluginCfg.sh.

   L'exécution de cette commande génère un fichier plugin-cfg.xml à l'emplacement suivant :

   répertoire_installation_websphere\AppServer\profiles\AppSrv01\config\cells

4. Effectuez l'une des procédures suivantes :

   - Effectuer la configuration sur IIS (page 315)
   - Effectuer la configuration sur iPlanet ou Apache (page 317)

Configuration sur IIS (7.x)

Avant de commencer cette procédure, vérifiez que vous utilisez la version 6.1.0.9 ou une version ultérieure du module d'extension de serveur Web. Les versions antérieures de ce module d'extension ne prennent pas en charge Windows Server 2008.

Procédez comme suit:

1. Installez IIS version 7.x avec les composants de compatibilité de gestion d'IIS 6.0. Ces composants ne sont pas installés par défaut.
2. Effectuez la procédure suivante pour configurer la fenêtre du gestionnaire de serveurs sur Windows Server 2008 :
    1. Cliquez sur Démarrer, Outils d'administration, Gestionnaire de serveur.
    2. Cliquez sur Action, Ajouter des rôles, puis sur Suivant.
    3. Dans la page Sélectionner des rôles de serveurs, sélectionnez le rôle Serveur Web (IIS), puis cliquez sur Suivant.
    4. Lorsqu'une invite pour la fonctionnalité Service d'activation des processus Windows s'affiche, cliquez sur Ajouter une fonctionnalité, Suivant.
    5. Dans la page d'accueil d'IIS, cliquez sur Suivant .
3. Lorsque la fenêtre Services de rôle s'affiche, vérifiez que les options suivantes sont sélectionnées en plus des options déjà sélectionnées par défaut.
    - Internet Information Services : Outils de gestion
    - IIS 6 Management Compatibility : Console de gestion IIS 6, Outils de script IIS 6, Compatibilité WMI d'IIS 6 et Compatibilité avec la métabase de données IIS 6
    - Développement d'applications : Extensions ISAPI, Filtres ISAPI
4. Cliquez sur Suivant pour activer les options sélectionnées, puis sur Installer dans la fenêtre suivante pour lancer l'installation.
5. Une fois que l'installation est terminée, cliquez sur Fermer dans la fenêtre Résultats de l'installation.
6. Ouvrez l'invite de commande et accédez à :\Program Files\IBM\WebSphere\AppServer\profiles\Dmgr01\bin.
7. Exécutez la commande GenPluginCfg.bat.

    Le fichier plugin-cfg.xml sera généré à l'emplacement C:\Program Files\IBM\WebSphere\AppServer\profiles\Dmgr01\config\cells.
8. Créez un répertoire sous c:\, par exemple, c:\plugin.
9. Copiez le fichier plugin-cfg.xml
10. et le fichier iisWASPlugin_http.dll dans ce répertoire.

11. Sélectionnez Démarrer, Tous les programmes, Outils d'administration, Gestionnaire des services Internet (IIS) sur Windows Serveur 2008. Cette action démarre l'application IIS et crée un nouveau répertoire virtuel pour l'instance de site Web. Ces instructions supposent que vous utilisez le site Web par défaut.
12. Développez l'arborescence à gauche jusqu'à l'option Site Web par défaut.
13. Cliquez avec le bouton droit de la souris sur Site Web par défaut, Ajouter, Répertoire virtuel pour créer le répertoire avec une installation par défaut.
14. Entrez setPlugins dans le champ Alias dans la fenêtre Alias du répertoire virtuel de l'Assistant Création de répertoire virtuel.
15. Accédez au répertoire c:\plugin dans le champ Chemin d'accès physique de la fenêtre Répertoire de contenu du site Web de l'Assistant, puis cliquez sur OK.
16. Cliquez sur Tester les paramètres. Si le test des paramètres renvoie un échec, vous pouvez modifier les autorisations du répertoire physique. Vous pouvez également sélectionnez Se connecter en tant que et permettre à IIS de se connecter sous un compte d'utilisateur Windows qui dispose des droits sur les fichiers de ce chemin d'accès physique.
17. Cliquez sur OK pour ajouter le répertoire virtuel setPlugins à votre site Web.
18. Dans l'arborescence de navigation, sélectionnez le répertoire virtuel setPlugins que vous avez créé.
19. Double-cliquez sur Mappages de gestionnaire, puis cliquez sur Modifier les autorisations de fonction dans le panneau Actions.
20. Sélectionnez Script et Exécuter, si ces options ne sont pas déjà sélectionnées.
21. Cliquez sur OK.
22. Retournez à la fenêtre du gestionnaire IIS et développez le dossier Sites Web dans l'arborescence de navigation sur la gauche.
23. Sélectionnez Site Web par défaut dans l'arborescence de navigation.
24. Effectuez les étapes suivantes dans le panneau Propriétés du site Web par défaut pour ajouter le filtre ISAPI :
    1. Double-cliquez sur l'onglet Filtres ISAPI.
    2. Cliquez pour ouvrir la boîte de dialogue Ajouter/modifier les propriétés du filtre.
    3. Entrez iisWASPlugin dans le champ de nom Filtre.
    4. Cliquez sur Parcourir pour sélectionner le fichier de module d'extension situé dans le répertoire c:\plugin\iisWASPlugin_http.dll.
    5. Cliquez sur OK pour fermer la boîte de dialogue.
25. Sélectionnez le noeud de serveur de niveau supérieur dans l'arborescence de navigation.

26. Double-cliquez sur Restrictions ISAPI et CGI dans le panneau Fonctionnalités.

    Pour déterminer la valeur à spécifier pour la propriété Chemin ISAPI ou CGI , accédez au même fichier de module d'extension que vous avez sélectionné à l'étape précédente, puis sélectionnez-le. Par exemple : c:\plugin\iisWASPlugin_http.dll.

27. Cliquez sur Ajouter dans le panneau Actions.

28. Entrez WASPlugin dans le champ Description , sélectionnez Autoriser l'exécution du chemin de l'extension, puis cliquez sur OK pour fermer la boîte de dialogue Restrictions ISAPI et CGI .

29. Créez le fichier plugin-cfg.loc à l'emplacement c:\plugin. Définissez la valeur dans le fichier plugin-cfg.loc sur l'emplacement du fichier de configuration. L'emplacement par défaut est C:\plugin\plugin-cfg.xml.

Mise à jour de l'agent Web

Après avoir configuré IIS 7.x, effectuez les modifications suivantes sur l'agent Web :

1. Cliquez sur Pool d'applications et remplacez le mode du pool d'applications par défaut par le mode Classique.
2. Cliquez sur Soumettre.
3. Vérifiez que la priorité de l'agent est plus élevée que celle du module d'extension pour le serveur d'applications utilisé par CA Identity Manager dans la liste de priorités des filtres ISAPI.
4. Redémarrez IIS 7.x et votre profil WebSphere Application Server.

Configuration sur IIS

Après avoir configuré le serveur HTTP IBM et le module d'extension de proxy, assurez-vous que le fichier plugin-cfg.xml du proxy se trouve à l'emplacement correct, puis effectuez les étapes de configuration de fichier de module d'extension supplémentaires.

Procédez comme suit:

1. Copiez le fichier plugin-cfg.xml comme suit :
   a. Connectez-vous au système sur lequel l'agent Web est installé.
   b. Créez un dossier sans espaces sous le lecteur C:. Par exemple : C:\plugin.
   c. Copiez le fichier plugin-cfg.xml dans ce dossier.
2. Créez un fichier appelé plugin-cfg.loc dans le dossier C:\plugin et ajoutez-y la ligne suivante :

   C:\plugin\plugin-cfg.xml

3. Téléchargez le programme d'installation du module d'extension WebSphere à partir de www.ibm.com sur le système sur lequel WebSphere est installé.
4. Accédez à l'emplacement du programme d'installation du module d'extension WebSphere.
5. Générez le fichier iisWASPlugin_http.dll à l'aide de la commande :

   ```
   install is:javahome "c:\IBM\WebSphere\AppServer\Java
   ```

   Répondez aux questions qui s'affichent en fonction de votre configuration.

   Lorsque l'assistant se termine, le fichier iisWASPlugin_http.dll est enregistré dans le dossier C:\IBM\WebSphere\Plugs\bin. Recherchez un sous-dossier 32 ou 64 bits.
6. Copiez le fichier iisWASPlugin_http.dll dans le dossier C:\plugin du système avec l'agent Web.
7. Créez un répertoire virtuel comme suit :
   a. Ouvrez le gestionnaire IIS.
   b. Avec le bouton droit de la souris, cliquez sur Site Web par défaut.
   c. Cliquez sur Nouveau répertoire virtuel et fournissez ces valeurs :

      Alias : sePlugins (respectez la casse)

      Chemin d'accès : c:\plugin

      Autorisation : Lecture + Exécution (ISAPI ou CGI)
8. Ajoutez un filtre ISAPI comme suit :
   a. Cliquez avec le bouton droit de la souris sur Site Web par défaut.
   b. Cliquez sur Propriétés.
   c. Cliquez sur Ajouter dans l'onglet Filtre ISAPI.
   d. Spécifiez les valeurs suivantes :

      Nom du filtre : sePlugins

      Exécutable : c:\plugin\ iisWASPlugin_http.dll
9. Créez une extension de service Web comme suit :
   a. Dans le gestionnaire IIS6, développez le nom de l'ordinateur.
   b. Créez une extension de service Web et définissez-la sur Autorisé.

      Nom d'extension : WASPlugin

      Chemin d'accès : C:\plugin\ iisWASPlugin_http.dll
   c. Cliquez avec le bouton droit de la souris sur chaque extension de service Web pour changer son statut sur Autorisé.

10. Redémarrez le serveur Web IIS.

    Dans le service WWW principal, vérifiez que le module d'extension WebSphere (sePlugin) s'affiche après le module d'extension de l'agent Web SiteMinder et qu'il a démarré correctement.

Configuration sur iPlanet ou Apache

Après avoir configuré le serveur HTTP IBM et le module d'extension de proxy, assurez-vous que le fichier plugin-cfg.xml du proxy se trouve à l'emplacement correct, puis redémarrez le serveur Web.

Procédez comme suit:

1. Copiez le plugin-cfg.xml dans le système sur lequel vous avez installé le module d'extension de proxy à l'emplacement suivant :

   répertoire_installation_websphere\AppServer\profiles*nom_serveur*\config\cells*cellule_websphere*\nodes\webserver1_node\servers\webserver1\

2. Vérifiez que le module d'extension WebSphere (libns41_http.so) est chargé après le module d'extension d'agent Web SiteMinder (NSAPIWebAgent.so) sur tous les serveurs Web iPlanet.

3. Vérifiez l'ordre des modules d'extension dans le fichier *répertoire_installation_iplanet*/https-*instance*/config/magnus.conf pour les serveurs Web IPlanet 6.0.

4. Copiez les lignes suivantes de *répertoire_installation_iplanet*/https-*instance*/config/magnus.conf dans *répertoire_installation_iplanet*/https-*instance*/config/obj.conf (serveurs Web IPlanet 5.x) :

   ```
   Init fn="load-modules" funcs="as_init,as_handler,as_term"
   shlib="/export/WebSphere/AppServer/bin/libns41_http.so"

   Init fn="as_init"
   bootstrap.properties="/export/WebSphere/AppServer/config/cells/plugin-cfg.xml"
   ```

   Ajoutez le code suivant après AuthTrans fn="SiteMinderAgent" dans le fichier obj.conf :

   ```
   Service fn="as_handler"
   ```

5. Vérifiez que le module d'extension d'agent Web SiteMinder (mod2_sm.so) est chargé avant le module d'extension WebSphere (mod_ibm_app_server_http.so) sur les serveurs Web Apache. Cette commande se trouve dans la section Dynamic Shared Object (DSO) Support du fichier *répertoire_installation_apache*/config/httpd.conf.

6. Redémarrez le serveur Web.

Installation du module d'extension de proxy pour JBoss

Une fois que l'agent Web SiteMinder authentifie et autorise une demande de ressource CA Identity Manager, le serveur Web l'envoie au serveur d'applications qui héberge le serveur CA Identity Manager. Pour permettre l'envoi de ces demandes, installez et configurez un connecteur JK sur le système dans lequel l'agent Web SiteMinder est installé. Pour plus d'informations sur le connecteur JK, reportez-vous au site Web de Jakarta Project :

http://community.jboss.org/wiki/usingmodjk12withjboss

Les outils d'administration CA Identity Manager incluent des exemples de fichiers de configuration que vous pouvez utiliser pour configurer le connecteur JK. Pour obtenir des instructions, consultez le fichier readme.txt dans le répertoire affiché dans la table suivante :

Plate-forme	Emplacement
Serveur Web IIS sur un système Windows	<chemin_installation>\tools\samples\ConnectorConfiguration\windows\IIS_JBoss*
Serveur Sun Java System Web server sur un système Solaris	<chemin_installation2>/tools/samples/ConnectorConfiguration/solaris/Iplanet_JBoss*
Serveur Web Apache sur un système Solaris	<chemin_installation2>/tools/samples/ConnectorConfiguration/solaris/apache_JBoss*

Installation et configuration d'un module d'extension d'application JBoss (IIS 7.x)

Cette procédure décrit la configuration du module d'extension Apache JBoss sur IIS 7.0.

Procédez comme suit:

1. Déployez et mettez à jour les filtres ISAPI sur le système de fichiers.

   Déployez le dossier ISAPI à la racine du lecteur C.

2. Modifiez le fichier jakarta.reg situé dans le dossier décompressé.

   Si vous avez placé le dossier ISAPI à la racine du lecteur C:\, ne modifiez pas ce fichier. Si vous l'avez placé dans un dossier différent, indiquez-le aux lignes 9, 11 et 12.

3. Enregistrez vos modifications, puis double-cliquez sur le registre pour le mettre à jour.

4. Modifiez le fichier workers.properties en spécifiant l'emplacement du serveur d'applications JBoss. Ne modifiez pas le port et le type.

5. Installez IIS 7 ou IIS 7.5 sur Windows 2008.
6. Ouvrez l'administrateur système et vérifiez que le filtre ISAPI et l'extension ISAPI d'IIS sont installés.
7. Démarrez inetmgr dans la fenêtre d'exécution.
8. Sélectionnez le nom m/c et double-cliquez sur Restrictions ISAPI et CGI.
9. Cliquez sur Ajouter dans le panneau droit.
10. La fenêtre Ajouter une restriction ISAPI ou CGI s'affiche.
11. Sélectionnez isapi_redirect.dll et entrez la description ISAPI.
12. Sélectionnez Autoriser l'exécution du chemin de l'extension.
13. Cliquez sur OK dans la fenêtre Ajouter une restriction ISAPI ou CGI.
14. Développez les sites de la section Connexion, sélectionnez WebSite par défaut, puis cliquez avec le bouton droit de la souris sur Ajouter un répertoire virtuel.
15. Entrez l'alias jakarta et l'emplacement du fichier isap_redirect.dll (c:\ajp) dans le chemin d'accès physique.
16. Cliquez sur Tester les paramètres :
    - Si l'authentification et l'autorisation sont effectuées, cliquez sur OK.
    - Si l'autorisation renvoie un échec, cliquez sur Se connecter en tant que.
17. Sélectionnez l'utilisateur et fournissez le nom d'administrateur et le mot de passe.
18. Cliquez à nouveau sur Tester les paramètres. Cette fois l'autorisation devrait être validée.
19. Cliquez sur Site Web par défaut à gauche et double cliquez sur le filtre ISAPI.
20. Cliquez sur Ajouter dans le panneau droit.
21. Entrez le nom et indiquez l'emplacement du fichier isapi_redirect.dll.
22. Cliquez sur OK.
23. Développez le site Web par défaut et cliquez sur le répertoire virtuel jakarta.
24. Double-cliquez sur Mappages de gestionnaires.
25. Sélectionnez ISAPI-dll, puis cliquez sur Modifier les autorisations de fonction.

26. Vérifiez que toutes les autorisations (Lecture, Script, Exécution) sont sélectionnées.
27. Cliquez sur OK.

Mise à jour de l'agent Web

Après avoir configuré IIS 7.x, effectuez les modifications suivantes sur l'agent Web :

1. Cliquez sur Pool d'applications et remplacez le mode du pool d'applications par défaut par le mode Classique.
2. Cliquez sur Soumettre.
3. Vérifiez que la priorité de l'agent est plus élevée que celle du module d'extension pour le serveur d'applications utilisé par CA Identity Manager dans la liste de priorités des filtres ISAPI.

Le module d'extension JBoss est configuré.

Installation et configuration d'un module d'extension d'application JBoss (IIS 6.0)

Cette intégration suppose que SiteMinder authentifie et autorise un utilisateur avant qu'il puisse se connecter à CA Identity Manager. Un cookie SMSESSION doit être associé à un utilisateur avant qu'il puisse se connecter à CA Identity Manager. Utilisez un module d'extension d'application (redirection via proxy) protégé par un agent Web SiteMinder. Cette configuration permet d'authentifier un utilisateur auprès de SiteMinder, puis de le rediriger vers CA Identity Manager après la création d'un cookie SMSESSION.

Effectuez la procédure suivante pour le déploiement et la configuration du module d'extension Apache de JBoss vers IIS 6.0 :

Procédez comme suit:

1. Déployez et mettez à jour les filtres ISAPI sur le système de fichiers.

   Déployez le dossier ISAPI à la racine du lecteur C.
2. Modifiez le fichier jakarta.reg situé dans le dossier décompressé.

   Si vous avez placé le dossier ISAPI à la racine du lecteur C:\, ne modifiez pas ce fichier. Si vous l'avez placé dans un dossier différent, indiquez-le dossier aux lignes 9, 11 et 12.
3. Enregistrez vos modifications, puis double-cliquez sur le registre pour le mettre à jour.
4. Modifiez le fichier workers.properties en spécifiant l'emplacement du serveur d'applications JBoss. Ne modifiez pas le port et le type.
5. Déployez le filtre ISAPI sur IIS.
6. Ouvrez le gestionnaire IIS à partir des outils d'administration.

7. Développez les niveaux jusqu'à ce que l'option Site Web par défaut soit affichée. Cliquez avec le bouton droit de la souris et sélectionnez Nouveau, Répertoire virtuel.
8. Entrez l'alias *jakarta*.
9. Référencez le chemin d'accès sur lequel vous avez installé le module d'extension ISAPI.
10. Sélectionnez les autorisations Lecture, Exécuter les scripts (tels que ASP) et Exécuter (par exemple, applications CGI ou ISAPI).
11. Cliquez sur Suivant pour continuer et terminer l'assistant.
12. Cliquez avec le bouton droit de la souris sur le site Web par défaut et sélectionnez les propriétés, puis sélectionnez l'onglet Filtres ISAPI et cliquez sur Ajouter.
13. Entrez *jakarta* comme nom de filtre, puis cliquez sur Parcourir pour sélectionner la bibliothèque isapi_redirect.dll. Cliquez deux fois sur OK.
14. Pour IIS 6.0, activez ce filtre sous les extensions de service Web.
15. Pour cela, sélectionnez le dossier Extensions du service Web. Cliquez sur le lien bleu à gauche pour ajouter une nouvelle extension de service Web.
16. Spécifiez le nom Jakarta-Tomcat. Cliquez sur Ajouter et accédez à la même bibliothèque que mentionnée ci-dessus. Cliquez sur OK, définissez le statut d'extension sur Autorisé, puis cliquez sur OK.
17. Redémarrez le serveur IIS.

Une fois que le proxy est configuré, vous pouvez accéder à CA Identity Manager via IIS. Par exemple, les liens suivants permettent d'accéder à CA Identity Manager avant et après la configuration du proxy :

Avant

http://identitymgr.forwardinc.ca:8080/idmmange
http://identitymgr.forwardinc.ca:8080/idmmange

Après

http://smserver.forwardinc/idmmanage http://smserver.forwardinc/idmmanage

Remarque : Une barre oblique "/" peut être requise à la fin de cette URL pour le bon fonctionnement du proxy. Référencez les journaux de proxy si vous n'êtes pas renvoyé à la console de gestion.

Installation du module d'extension de proxy sur WebLogic

Une fois que l'agent Web authentifie et autorise une demande de ressource CA Identity Manager, le serveur Web l'envoie au serveur d'applications qui héberge le serveur CA Identity Manager.

1. Installez le module d'extension de proxy WebLogic pour votre serveur Web comme décrit dans la documentation WebLogic.

   Remarque : Pour les utilisateurs d'IIS, lorsque vous installez le module d'extension de proxy, assurez-vous de configurer le proxy selon l'extension de fichier et le chemin d'accès. Lorsque vous configurez le proxy selon l'extension de fichier, ajoutez un mappage d'applications dans l'onglet Mappage d'application avec les propriétés suivantes :
   Exécutable : IISProxy.dll
   Extension : .wlforward

2. Configurez le module d'extension de proxy pour CA Identity Manager comme décrit dans l'une des sections suivantes :

   - Module d'extension de proxy IIS (page 325)
   - Module d'extension de proxy iPlanet (page 326)
   - Module d'extension de proxy Apache (page 329)

Configuration du module d'extension de proxy pour IIS (7.x)

La procédure suivante décrit les étapes du déploiement et de la configuration du module d'extension de proxy WebLogic pour IIS 7.x.

Remarque : Ces instructions sont destinées aux environnements d'exploitation 32 bits. Les mêmes instructions s'appliquent aux environnements d'exploitation 64 bits. Cependant, l'emplacement du fichier installation.dll est différent :

- %WL_HOME%server\plugin\win\32\
- %WL_HOME%server\plugin\win\64\

Procédez comme suit:

1. Installez l'agent Web et configurez-le sur IIS 7.
2. Créez un dossier plugin dans le lecteur C.
3. Copiez les fichiers suivants dans ce dossier :

   - lisforward.dll
   - lisproxy.dll
   - iisproxy.ini

   Vous pouvez récupérer ces fichiers à partir de l'emplacement \\lodimmaple.ca.com\RegressionHarness\thirdparty\weblogic\Weblogic_Proxy_Files_IIS7.

4. Installez les services de rôle Développement d'applications et Outils de gestion sur IIS7.
5. Ouvrez le gestionnaire Inet et sélectionnez le site Web par défaut.
6. Cliquez sur Mappages de gestionnaires.
7. Double-cliquez sur Fichier statique et modifiez le chemin d'accès de demande sur *.*.
8. Cliquez sur Restrictions des demandes.
9. Dans l'onglet Mappages, sélectionnez Appeler le gestionnaire seulement si une demande est mappée à un fichier ou un dossier.
10. Dans la boîte de dialogue Mappages de gestionnaires, cliquez sur Ajouter un mappage de scripts dans le menu de droite. Saisissez les valeurs suivantes :
    - Chemin d'accès à la demande : *
    - Exécutable : IISProxy.dll
    - Nom : proxy
11. Cliquez sur Restrictions des demandes.
12. Désélectionnez l'option Appeler le gestionnaire uniquement si la demande est mappée.
13. Cliquez sur Oui à l'invite pour autoriser cette extension IASPI.
14. Cliquez sur le noeud racine (nom d'ordinateur) de l'arborescence du gestionnaire IIS et cliquez sur Restrictions ISAPI et CGI.
15. Cliquez sur Ajouter dans le volet Actions et entrez les valeurs suivantes :
    - Chemin ISAPI ou CGI : C:\plugin\ iisproxy.dll.
    - Description : WebLogic
    - Sélectionnez Autoriser l'exécution du chemin de l'extension.
16. Cliquez sur le noeud racine (nom d'ordinateur) de l'arborescence du gestionnaire IIS et cliquez sur Restrictions ISAPI et CGI. Sélectionnez l'option WebLogic et cliquez sur Modifier les paramètres de fonction dans le volet droit.
17. Sélectionnez Autoriser les modules ISAPI non spécifiés et Autoriser les modules CGI non spécifiés.
18. Effectuez la même opération pour l'agent Web.
19. Dans la vue Fonctionnalités du site Web par défaut, double-cliquez sur Mappages de gestionnaires.

20. Dans le volet Actions de la page Mappages de gestionnaires, cliquez sur Ajouter un mappage de scripts et entrez les valeurs suivantes :
    - Chemin d'accès à la demande : .jsp
    - Exécutable : iisproxy.dll
    - Nom : JSP
21. Cliquez sur Restrictions des demandes.
22. Dans l'onglet Mappage, sélectionnez Appeler le gestionnaire seulement si une demande est mappée à un fichier.
23. Cliquez sur OK.
24. Cliquez sur Ajouter un mappage de scripts et entrez les valeurs suivantes :
    - Chemin d'accès à la demande : .do
    - Exécutable : C:\plugin\iisproxy.dll
25. Cliquez sur Restrictions des demandes. Les paramètres sont les mêmes .jsp.
26. Cliquez sur OK.
27. Cliquez sur Ajouter un mappage de scripts et entrez les valeurs suivantes :
    - Chemin d'accès à la demande : .wlforward
    - Exécutable : C:\plugin\iisproxy.dll
28. Cliquez sur Restrictions des demandes. Les paramètres sont les mêmes que pour le fichier .jsp.
29. Cliquez sur Site Web par défaut et double-cliquez sur Filtres ISAPI.
30. Cliquez sur View Order List (Afficher la liste de tri) dans le volet droit.
31. Placez l'exécutable de l'agent SiteMinder à la deuxième place de la liste. Après cette entrée, seul l'exécutable de WebLogic se trouve dans la liste.

    Remarque : Si l'exécutable de l'agent SiteMinder s'affiche après l'exécutable de WebLogic, déplacez l'agent SiteMinder à l'aide de l'action Déplacer vers le haut.
32. Cliquez sur Pool d'applications et remplacez le mode du pool d'applications par défaut par le mode Classique.

Le module d'extension WebLogic est configuré.

Configuration du module d'extension de proxy IIS 6.0

Cette procédure s'applique aux configurations du module d'extension de proxy WebLogic pour IIS 6.0.x :

Procédez comme suit:

1. Créez un dossier sur le système dans lequel l'agent Web est installé. Par exemple : c:\weblogic_proxy.
2. Connectez-vous au système sur lequel le serveur CA Identity Manager est exécuté.
3. Accédez au dossier *répertoire_installation_Weblogic*\wlserver_11\server\plugin.
4. Copiez les fichiers suivants dans le dossier de proxy WebLogic créé à l'étape 1.
   - iisforward.dll
   - iisproxy.dll
5. Créez un fichier nommé iisproxy.ini dans le même dossier et incluez le contenu suivant :

   ```
   # This file contains initialization name/value pairs
   # for the IIS/WebLogic plug-in.
   WebLogicHost=nom_hôte
   WebLogicPort=7001
   ConnectTimeoutSecs=20
   ConnectRetrySecs=2
   WlForwardPath=/castylesr5.1.1,/iam,/im , /ca/Odata/
   WLLogFile= c:\weblogic_proxy \proxy.log
   DebugConfigInfo=ON
   ```

   Remplacez *nom_hôte* par le nom d'hôte réel.
6. Démarrez le gestionnaire IIS.
7. Développez les sites Web.
8. Cliquez avec le bouton droit de la souris sur Site Web par défaut.
9. Sélectionnez Propriétés.
10. Ajoutez un filtre comme suit :
    a. Cliquez sur Filtres ISAPI.
    b. Cliquez sur Ajouter et remplissez la boîte de dialogue comme suit :

       Nom du filtre : WebLogic

       Exécutable : chemin d'accès à la bibliothèque iisforward.dll

11. Indiquez l'emplacement du fichier iisproxy.dll comme suit :
    a. Cliquez sur Répertoire de base.
    b. Cliquez sur Configuration.
    c. Cliquez sur Ajouter.
    d. Entrez le chemin d'accès au fichier iisproxy.dll.
    e. Entrez .jsp dans le champ Extension.
    f. Désactivez l'option Vérifier l'existence du fichier.
12. Répétez l'étape 11 pour les extensions .do et .wlforward.
13. Ajoutez une extension de service Web pour wlforward en minuscules pointant vers l'emplacement du fichier iisforward.dll.

    Définissez le statut d'extension sur Autorisé.
14. Cliquez avec le bouton droit de la souris sur chaque extension de service Web pour changer son statut sur Autorisé.
15. Redémarrez le serveur Web IIS.

Configuration du module d'extension de proxy iPlanet

Pour configurer le module d'extension, modifiez les fichiers de configuration iPlanet suivants :

- magnus.conf
- obj.conf

Les fichiers de configuration iPlanet ont des règles strictes sur le positionnement du texte. Pour éviter les problèmes, tenez compte des points suivants :

- Eliminez les espaces de début et de fin superflus. Ces espaces peuvent entraîner un échec du serveur iPlanet.
- Si vous devez entrer un nombre de caractères supérieur à ce que peut contenir une ligne, entrez une barre oblique inversée (\) à la fin de la ligne et continuez à la ligne suivante. La barre oblique inversée ajoute directement la fin de la première ligne au début de la ligne suivante. Si un espace est nécessaire entre les mots à la fin de la première ligne et au début de la deuxième ligne, insérez un espace à la fin de la première ligne avant la barre oblique inversée ou au début de la deuxième ligne.
- Ne divisez pas les attributs sur plusieurs lignes.

Les fichiers de configuration iPlanet pour votre instance iPlanet se trouvent à l'emplacement suivant :

répertoire_installation_iplanet/https-*nom_instance*/config/

où *répertoire_installation_iplanet* est le répertoire racine de l'installation iPlanet et *nom_instance* votre configuration de serveur.

Procédez comme suit:

1. A partir du répertoire *répertoire_installation_weblogic*/server/lib, copiez le fichier libproxy.so qui correspond à la version de votre serveur Web iPlanet dans le système de fichiers sur lequel vous avez installé iPlanet.
2. Dans un éditeur de texte, modifiez le fichier iPlanet magnus.conf.

   Pour indiquer à iPlanet de charger le fichier libproxy.so comme un module iPlanet, ajoutez les lignes suivantes au début du fichier magnus.conf :

   ```
   Init fn="load-modules" funcs="wl_proxy,wl_init"\
   shlib=chemin_système_fichiers_étape_1/libproxy.so
   Init fn="wl_init"
   ```

   Exemple :

   ```
   Init fn="load-modules" funcs="wl_proxy,wl_init"\
   shlib=/usr/local/netscape/plugins/libproxy.so
   Init fn="wl_init"
   ```

   Les modules de chargement de fonction balisent la bibliothèque partagée pour le chargement lorsque iPlanet démarre. Les valeurs wl_proxy et wl_init identifient les fonctions que le module d'extension exécute.

3. Dans un éditeur de texte, modifiez le fichier iPlanet obj.conf comme suit :
   a. Après la dernière ligne qui commence par le texte suivant :

      NameTrans fn=....

      Ajoutez la directive de service suivante à la section Object name="default" :
      ```
      Service method="(GET|HEAD|POST|PUT)" type=text/jsp fn="wl-proxy"
      ```

      Remarque : Vous pouvez ajouter cette directive dans une ligne à la suite des directives de service existantes.

   b. Ajoutez le code suivant à la fin du fichier :
      ```
      <Object name="idm" ppath="*/iam/*">">
      Service fn="wl-proxy" WebLogicHost="nom_hôte" WebLogicPort="numéro_port"
      PathTrim="/weblogic"
      </Object>
      <Object name="weblogic1" ppath="*/console*">
      Service fn="wl-proxy" WebLogicHost="nom_hôte" WebLogicPort="numéro_port"
      PathTrim="/weblogic"
      </Object>
      ```

      où *nom_hôte* est le nom de serveur et le domaine du système sur lequel vous avez installé WebLogic et *numéro_port* le port WebLogic avec la valeur par défaut 7001.

      Vous pouvez avoir plusieurs entrées d'objet.

      Exemple :
      ```
      <Object name="idm" ppath="*/iam/*">">
      Service fn="wl-proxy" WebLogicHost="MyServer.MyCompany.com"
      WebLogicPort="7001" PathTrim="/weblogic"
      <Object name="weblogic1" ppath="*/console*">
      Service fn="wl-proxy" WebLogicHost="MyServer.MyCompany.com"
      WebLogicPort="7001" PathTrim="/weblogic"
      </Object>
      ```
4. Enregistrez le fichier de configuration iPlanet.
5. Redémarrez l'instance de serveur Web.

Configuration du module d'extension de proxy Apache

La configuration du module d'extension de proxy Apache requiert la modification du fichier http.conf.

Procédez comme suit:

1. Arrêtez le serveur Web Apache après avoir installé un agent Web sur Solaris et copiez le fichier mod_wl_20.so de l'emplacement suivant :

   répertoire_installation_weblogic/server/lib/solaris

   vers

   répertoire_installation_apache/modules

2. Modifiez le fichier http.conf situé dans *répertoire_installation_apache*/conf et apportez les modifications suivantes :

   a. Dans la section du module de chargement, ajoutez le code suivant :
   ```
   LoadModule weblogic_module      modules/mod_wl_20.so
   ```

   b. Modifiez le nom de serveur avec le nom du système de serveur Apache.

   c. Ajoutez un bloc If à la fin du fichier comme suit :
   ```
   <IfModule mod_weblogic.c>
     WebLogicHost serveur_weblogic.com
     WebLogicPort 7001
     MatchExpression /iam
     MatchExpression /castylesr5.1.1
     MatchExpression /ca/Odata
   </IfModule>
   ```

3. Enregistrez le fichier http.conf.

4. Redémarrez le serveur Web Apache.

Association de l'agent SiteMinder à un domaine CA Identity Manager

L'administrateur de stratégie associe l'agent SiteMinder à un domaine CA Identity Manager après avoir effectué les tâches CA Identity Manager. Lors du chargement des environnements dans CA Identity Manager, référencez l'agent 4.X. SiteMinder utilise cet agent lors de la création du domaine sur le serveur de stratégies SiteMinder. Cet agent valide les cookies SMSESSION. Mettez à jour le domaine et référencez l'agent qui se trouve sur le serveur Web dans son intégralité pour accéder à CA Identity Manager. Ce serveur Web est le point d'accès à CA Identity Manager qui permet de créer des cookies SMSESSION.

Procédez comme suit:

1. Connectez-vous à l'interface d'administration SiteMinder.
2. Accédez à Stratégies, Domaines.
3. Modifiez le domaine pour votre environnement.
4. Dans l'onglet Domaines d'authentification, modifiez le premier domaine d'authentification répertorié : XXX_ims_realm.
5. Recherchez et sélectionnez l'agent sur votre proxy.

   Remarque : Si aucun agent proxy (agent de serveur Web) n'existe, créez-en un. Vérifiez qu'un serveur Web et un proxy sont bien placés avant CA Identity Manager.
6. Cliquez sur OK deux fois, puis répétez ce processus pour le domaine public XXX_pub_realm.
7. Après avoir mis à jour les deux domaines, cliquez sur Soumettre.
8. Patientez jusqu'à la fin de l'actualisation de l'agent ou redémarrez le serveur Web sur lequel se trouve l'agent proxy.

Configuration du paramètre LogOffUrI de SiteMinder

Après avoir ajouté SiteMinder à l'environnement, le paramètre logoff de CA Identity Manager ne sert plus à rien. Pour réactiver cette fonctionnalité, mettez à jour l'objet de configuration de l'agent sur le proxy.

Procédez comme suit:

1. Connectez-vous à l'interface d'administration SiteMinder. Cliquez sur l'onglet Infrastructure, Agents, développez la configuration d'agent, puis cliquez sur Modifier la configuration d'agent.
2. Recherchez l'objet de configuration d'agent, puis le paramètre #LogoffUri. Cliquez sur le bouton de lecture (flèche pointant vers la droite) à gauche de ce paramètre.

3. Supprimez le dièse du nom dans le champ Valeur et entrez /idm/logout.jsp.
4. Cliquez sur OK, puis sur Soumettre pour mettre à jour l'objet de configuration d'agent.

   Lorsque l'agent récupère sa configuration à partir du serveur de stratégies la fois suivante, le nouveau paramètre est propagé.

Dépannage

Les rubriques suivantes décrivent les erreurs communes susceptibles de se produire. Lorsque cela est possible, une solution a été associée avec l'erreur afin de vous aider à dépanner votre intégration.

Fichiers DLL Windows manquants

Symptôme :

Fichiers DLL Windows manquants (MSVCP71.dll)

JBoss peut renvoyer une erreur Java après l'activation de la connexion SiteMinder indiquant que la bibliothèque MSVCP71.dll est manquante.

Remarque : Cette erreur peut ne pas s'afficher si JBoss est exécuté en tant que service. Si vous le pouvez, testez la configuration sans exécuter JBoss en tant que service.

Solution :

Procédez comme suit:

1. Recherchez la bibliothèque MSVCP71.dll sur le serveur de stratégies SiteMinder, s'il est exécuté sur Windows.
2. Copiez le fichier MSVCP71.dll dans le dossier \Windows\system32.
3. Une fois que vous avez placé ce fichier dans l'emplacement correct, enregistrez-le dans le système d'exploitation.
4. Pour cela, ouvrez la fenêtre de commande et exécutez la commande regsvr32. Une fois que le fichier est chargé, l'erreur devrait être résolue.
5. Redémarrez le serveur d'applications.

Emplacement incorrect du serveur de stratégies SiteMinder

Symptôme :

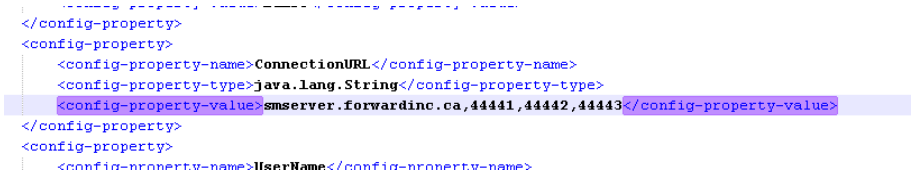
L'emplacement du serveur de stratégies SiteMinder est incorrect.

Solution :

Un emplacement incorrect est référencé dans le fichier ra.xml et l'erreur suivant apparaît : Cannot connect to policy server: xxx (Connexion au serveur de stratégies impossible : xxx).

Procédez comme suit:

1. Vérifiez le nom d'hôte spécifié dans le fichier ra.xml.



2. Dans la propriété ConnectionURL, spécifiez le nom d'hôte du serveur de stratégies SiteMinder. Utilisez un nom complet.

Nom d'administrateur incorrect

Symptôme :

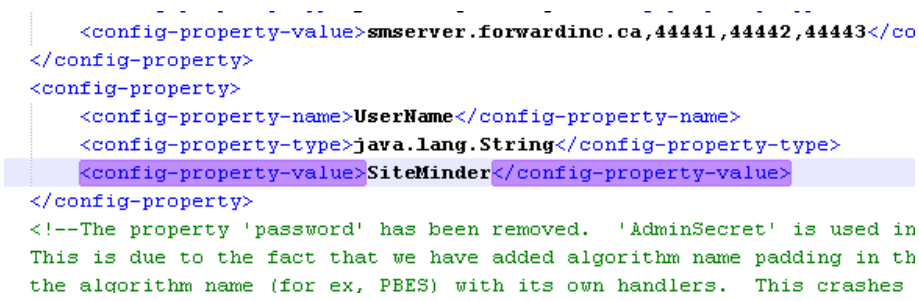
Nom d'administrateur incorrect

Solution :

Un administrateur incorrect est référencé dans le fichier ra.xml et l'erreur suivante apparaît : Unknown administrator (Administrateur inconnu).

Procédez comme suit:

1. Vérifiez la propriété UserName dans le fichier ra.xml.



2. Dans la propriété UserName, spécifiez le compte utilisé pour les communications avec SiteMinder. Par exemple, utilisez le compte SiteMinder (valeur par défaut).

Secret d'administrateur incorrect

Symptôme :

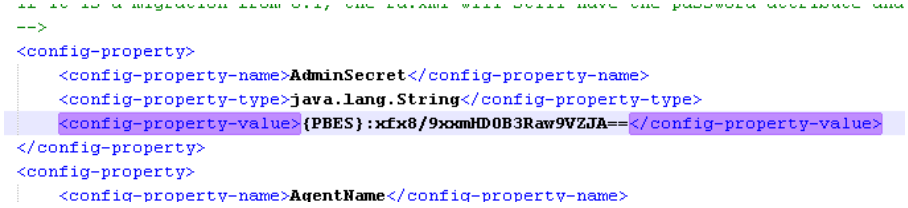
Secret d'administrateur incorrect

Solution :

Un secret d'administrateur incorrect est utilisé dans le fichier ra.xml et l'erreur suivante apparaît : Cannot connect to the policy server: Invalid credentials (Connexion au serveur de stratégies impossible : informations d'identification non valides).

Procédez comme suit:

1. Vérifiez la propriété AdminSecret dans le fichier ra.xml.




```
<config-property>
    <config-property-name>AdminSecret</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>{PBES}:xfx8/9xxmHD0B3Raw9VZJA==</config-property-value>
</config-property>
<config-property>
    <config-property-name>AgentName</config-property-name>
```

2. Dans la propriété AdminSecret, spécifiez le mot de passe chiffré pour le nom d'utilisateur référencé dans la propriété UserName.

Informations complémentaires :

Modification d'un mot de passe ou d'un secret partagé SiteMinder (page 363)

Nom d'agent incorrect

Symptôme :

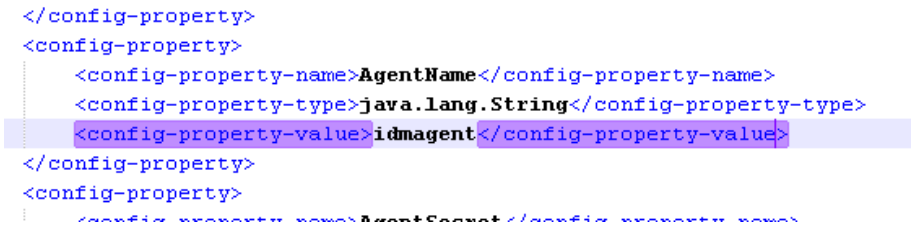
Nom d'agent incorrect

Solution :

Un nom d'agent incorrect est utilisé dans le fichier ra.xml et l'erreur suivante apparaît : Cannot connect to the policy server: Failed to init Agent API: -1 (Connexion au serveur de stratégies impossible : échec de l'initialisation de l'API d'agent -1).

Procédez comme suit:

1. Vérifiez la propriété AgentName dans le fichier ra.xml.



2. Spécifiez le nom d'agent 4.X que vous avez créé à la troisième étape des configurations SiteMinder.

Secret d'agent incorrect

Symptôme :

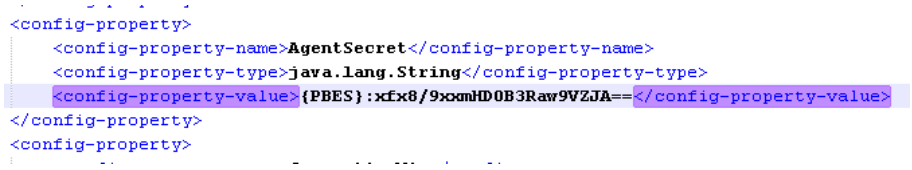
Secret d'agent incorrect

Solution :

Un secret d'agent incorrect est utilisé dans le fichier ra.xml et l'erreur suivante apparaît : Cannot connect to the policy server: Failed to init Agent API: -1 (Connexion au serveur de stratégies impossible : échec de l'initialisation de l'API d'agent -1).

Procédez comme suit:

1. Vérifiez la propriété AgentSecret dans le fichier ra.xml.



2. Spécifiez le mot de passe chiffré qui a été utilisé lors de la création de l'agent.

Informations complémentaires :

Modification d'un mot de passe ou d'un secret partagé SiteMinder (page 363)

Aucun contexte d'utilisateur dans CA Identity Manager

Symptôme :

Il n'y a aucun contexte d'utilisateur dans CA Identity Manager.

Si un utilisateur tente d'accéder à CA Identity Manager sans cookie SMSESSION, CA Identity Manager ne peut pas l'authentifier. Dans ce cas, l'interface utilisateur CA Identity Manager sera vide.

Si les flux de travaux sont activés dans l'environnement, un échec se produira.

```
Exception during page display:

java.lang.IllegalArgumentException
        at com.netegrity.webapp.bean.WorkList.(WorkList.java:84)
        at com.netegrity.webapp.bean.WorkList.(WorkList.java:70)
        at com.netegrity.webapp.bean.WorkList.getConsoleWorkListFromRequest(WorkList.java:109)
        at com.netegrity.taglib.skin.TagUtilLocal.getWorkItems(TagUtilLocal.java:660)
        at com.netegrity.taglib.skin.TagUtilLocal.hasWorkItems(TagUtilLocal.java:846)
        at com.netegrity.taglib.skin.IfWorkItemsTag.doStartTag(IfWorkItemsTag.java:73)
        at idm_jsp.app.ca12.home_jsp._jspService(Unknown Source)
        at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:654)
        at org.apache.catalina.core.ApplicationDispatcher.doInclude(ApplicationDispatcher.java:557)
        at org.apache.catalina.core.ApplicationDispatcher.include(ApplicationDispatcher.java:481)
        at org.apache.jasper.runtime.JspRuntimeLibrary.include(JspRuntimeLibrary.java:968)
        at idm_jsp.app.ca12.index_jsp._jspx_meth_skin_ifhomepage_0(Unknown Source)
        at idm_jsp.app.ca12.index_jsp._jspService(Unknown Source)
        at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:654)
        at org.apache.catalina.core.ApplicationDispatcher.processRequest(ApplicationDispatcher.java:445)
        at org.apache.catalina.core.ApplicationDispatcher.doForward(ApplicationDispatcher.java:379)
        at org.apache.catalina.core.ApplicationDispatcher.forward(ApplicationDispatcher.java:292)
        at com.netegrity.webapp.filter.ConsolePageFilter.doFilter(ConsolePageFilter.java:521)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:235)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at com.netegrity.webapp.page.jsf.FacesFilter.doFilter2(FacesFilter.java:180)
```

Solution :

Plusieurs facteurs peuvent être la cause de ce problème, mais habituellement, il s'agit de l'un des facteurs suivants :

- Vous avez accédé directement à CA Identity Manager.
- L'agent SiteMinder du proxy est désactivé, c'est-à-dire qu'aucune protection n'est activée et que le cookie SMSESSION n'est pas créé.
- Le domaine SiteMinder de l'environnement CA Identity Manager est configuré de manière incorrecte.

Les deux premières causes sont assez simples. Assurez-vous que les transactions sont routées vers le serveur Web et que l'agent Web soit activé et totalement fonctionnel. Si c'est déjà le cas, vous devez modifier le domaine.

Procédez comme suit:

1. Connectez-vous à l'interface d'administration SiteMinder.
2. Recherchez le domaine CA Identity Manager et cliquez sur les couches pour le modifier. Cliquez sur l'onglet Domaine, puis sur le premier domaine de la liste.
3. L'emplacement par défaut de la barre oblique est sous le domaine. Supprimez-la.
4. Cliquez sur la règle sous ce domaine.

   La ressource en vigueur par défaut pour la règle est un astérisque (*).
5. Ajoutez la barre oblique en face de l'astérisque.

   Vous avez déplacé la barre oblique du domaine vers la règle. La protection est la même, mais SiteMinder la traite différemment.

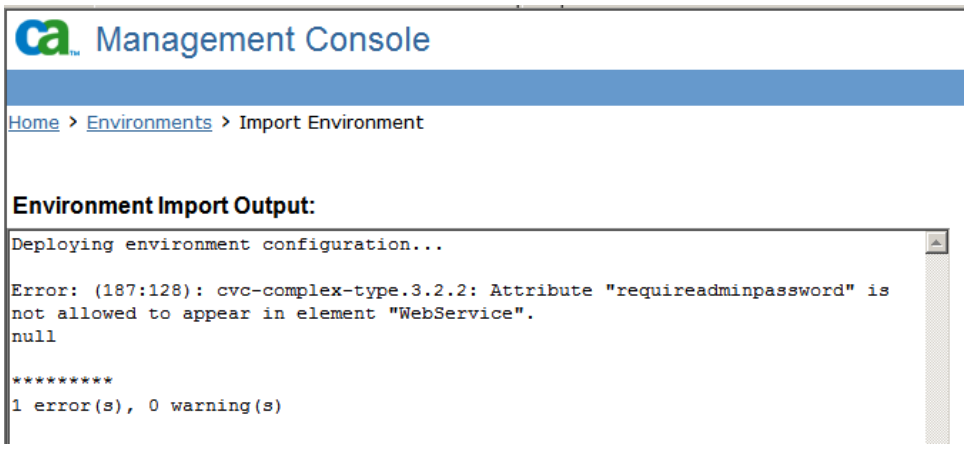
   Vous pouvez vous connecter correctement à CA Identity Manager via SiteMinder. Pour valider la protection appropriée, consultez les journaux de l'agent SiteMinder.

Erreur lors du chargement des environnements

Symptôme :

Lorsque vous importez un environnement dans CA Identity Manager après avoir configuré l'intégration de SiteMinder, une erreur s'affiche pour l'attribut requireadminpassword et l'élément WebService.

Remarque : Ce problème peut également se produire lorsque SiteMinder n'est pas inclus dans le déploiement.



Solution :

Cette erreur permet un déploiement partiel de l'environnement. Le déploiement partiel peut créer des éléments vides dans le référentiel d'objets CA Identity Manager. Corrigez l'un des fichiers XML de l'environnement et réimportez-le.

Procédez comme suit:

1. Recherchez le fichier ZIP archivé et ouvrez-le.
2. Créez une copie du fichier XXX_environment_settings.xml.
3. Modifiez ce fichier et recherchez l'élément WebService.
4. Supprimez la balise requireadminpassword="false".

   Remarque : Supprimez la balise *et* la valeur. Ne supprimez pas uniquement la valeur.
5. Enregistrez les modifications et placez le fichier dans le fichier ZIP à nouveau.
6. Réimportez le fichier ZIP d'environnement archivé.

   Ne supprimez pas l'environnement créé lors de l'échec du déploiement. Réimporter un fichier corrigé permet de corriger les erreurs rencontrées lors de l'échec du déploiement.

Impossible de créer un annuaire ou un environnement CA Identity Manager

Symptôme :

La création d'un annuaire ou d'un environnement CA Identity Manager est impossible lorsque l'intégration avec SiteMinder est activée.

Solution :

Ce problème peut être dû à une entrée manquante dans le registre.

Vérifiez que le paramètre de registre suivant existe sur le serveur de stratégies SiteMinder :

- Solaris ou Linux :

  Vérifiez que l'entrée suivante existe dans sm.registry :
  ImsInstalled=8.0; REG_SZ

- Windows :

  Vérifiez que le paramètre ImsInstalled=8.0; REG_SZ existe à l'emplacement suivant :
  HKLM\SOFTWARE\Netegrity\SiteMinder\CurrentVersion

  Remarque : Si le chemin d'accès au registre \Netegrity\SiteMinder\CurrentVersion n'existe pas, créez-le manuellement.

Si vous modifiez le registre, assurez-vous de redémarrer le serveur de stratégies de façon à appliquer les modifications.

Important : Avant de modifier le registre, effectuez une sauvegarde complète du système.

Connexion de l'utilisateur impossible

Symptôme :

Un nouvel utilisateur ne peut pas se connecter à un environnement avec un mot de passe en texte clair.

Solution :

Vérifiez que la classification de données suivante n'est pas incluse dans la définition d'attribut de mot de passe du fichier de configuration d'annuaire (directory.xml) :

<DataClassification name="AttributeLevelEncrypt"/>

Dans les environnements qui incluent les composants suivants, l'activation de l'attribut de chiffrement de niveau empêche les utilisateurs de se connecter :

- CA SiteMinder
- Une base de données relationnelles

Configuration des paramètres de l'agent CA Identity Manager

Lorsque l'intégration de CA Identity Manager avec SiteMinder est configurée, CA Identity Manager utilise un agent CA Identity Manager intégré pour communiquer avec le serveur de stratégies SiteMinder. Pour ajuster les performances, configurez les paramètres de connexion suivants pour l'agent CA Identity Manager.

1. Effectuez l'une des étapes suivantes :
   - Si CA Identity Manager s'exécute sur un serveur d'applications WebLogic ou WebSphere, modifiez l'adaptateur de ressource dans le descripteur de connecteur policyserver_rar dans la console du serveur d'applications.
   - Si CA Identity Manager s'exécute sur un serveur d'applications JBoss, ouvrez le fichier policyserver-service.xml à partir de <répertoire_installation_JBoss>\server\default\deploy\iam_im.ear\policyserver_rar\META-INF.
2. Configurez les paramètres comme suit :

   ConnectionMax

   Définit le nombre maximum de connexions au serveur de stratégies. Par exemple : 20.

   ConnectionMin

   Définit le nombre minimum de connexions au serveur de stratégies. Par exemple : 2.

   ConnectionStep

   Définit le nombre de connexions supplémentaires à ouvrir lorsque toutes les connexions de l'agent sont en cours d'utilisation.

   ConnectionTimeout

   Spécifie le délai d'expiration en secondes pour la connexion de l'agent à SiteMinder.
3. Redémarrez le serveur d'applications.

Configuration de la haute disponibilité CA SiteMinder

Si vous avez créé un cluster de serveurs de stratégies SiteMinder, vous pouvez configurer un cluster de serveurs d'applications à des fins d'équilibrage de la charge et de basculement.

Procédez comme suit:

1. Modifiez le fichier ra.xml situé à l'emplacement :
   WebSphere :
   profil_was/config/cells/*nom_cellule*/applications/iam_im.ear/deployments/IdentityMinder/policyserver_rar/META-INF
   Jboss :
   répertoire_installation_jboss/server/all/deploy/iam_im.ear/policyserver_rar/META-INF
   WebLogic : *domaine_wl*/applications/iam_im.ear/policyserver_rar/META-INF
2. Modifiez les éléments selon les explications contenues dans les sections suivantes :
   - Paramètres de connexion pour le serveur de stratégies
   - Nombre de serveurs de stratégies
   - Sélection d'équilibrage de la charge ou de basculement pour le cluster
3. Répétez cette procédure pour chaque serveur CA Identity Manager du cluster.
4. Redémarrez le serveur d'applications pour appliquer les modifications.

Remarque : Lorsque vous créez un annuaire ou un environnement CA Identity Manager, ou lorsque vous modifiez les paramètres d'annuaire ou d'environnement, définissez les paramètres SiteMinder Failover et FailoverServers sur False. Dans le cas contraire, l'objet d'annuaire peut être créé sans être répliqué à temps pour être utilisé. Par exemple, vous créez un annuaire dans le serveur 1. Vous créez ensuite un attribut à l'aide de l'ID d'objet de cet annuaire sur le serveur 2, mais le deuxième annuaire n'existe pas encore. Une erreur Objet introuvable est renvoyée.

Modification des paramètres de connexion du serveur de stratégies

Les informations de connexion du serveur de stratégies doivent mentionner le serveur principal de l'environnement de production. Ces informations comprennent l'attribut ConnectionURL, le nom d'utilisateur et le mot de passe du compte d'administrateur SiteMinder, ainsi que le nom et le secret partagé pour l'agent.

Dans l'exemple suivant, les valeurs modifiables s'affichent en majuscules.

```
<config-property>
        <config-property-name>ConnectionURL</config-property-name>
   <config-property-type>java.lang.String</config-property-type>
        <config-property-
value>DEVELOPMENT.SEVERCOMPANY.COM,VALUE,VALUE,VALUE</config-
                property-value>
</config-property>

<config-property>
        <config-property-name>UserName</config-property-name>
   <config-property-type>java.lang.String</config-property-type>
        <config-property-value>SITEMINDER-ADMIN-NAME</config-property-
                value>
</config-property>

<config-property>
        <config-property-name>AdminSecret</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>ENCRYPTED-PASSWORD</config-
                property-value>
</config-property>
<config-property>
        <config-property-name>AgentName</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>DEVELOPMENT-AGENT-NAME</config-property-
                value>
</config-property>

<config-property>
        <config-property-name>AgentSecret</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>ENCRYPTED-AGENT-SECRET</config-
                property-value>
</config-property>
```

Remarque : Pour les valeurs qui requièrent un texte chiffré, utilisez l'outil de modification de mots de passe CA Identity Manager. Pour plus d'informations, consultez le *Manuel de configuration*.

Ajout de serveurs de stratégies supplémentaires

Pour ajouter des serveurs de stratégies à l'instance d'installation CA Identity Manager, modifiez l'entrée **FailoverServers** dans le fichier ra.xml.

Remarque : Incluez le serveur de stratégies principal et tous les serveurs de basculement dans l'entrée FailoverServers.

Pour chaque serveur de stratégies, entrez une adresse IP et des numéros de port pour les services d'authentification, d'autorisation et de comptabilisation. Utilisez un point-virgule pour séparer les entrées :

```
<config-property>
        <config-property-name>FailoverServers</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>
                172.123.123.123,44441,44442,44443;172.123.123.124,33331,
                33332,33333
        </config-property-value>
</config-property>
```

Sélection de l'équilibrage de la charge ou du basculement

Le comportement par défaut de CA Identity Manager prévoit l'utilisation de l'équilibrage de la charge en tourniquet à l'aide des serveurs identifiés par les attributs ConnectionURL et FailoverServers. L'équilibrage de la charge se produit si FailOver est défini sur False.

Pour activer le basculement, définissez FailOver sur True :

```
<config-property>
        <config-property-name>FailOver</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
</config-property>
```

Suppression de CA SiteMinder d'un déploiement CA Identity Manager existant

Cette section fournit des instructions détaillées pour la suppression de SiteMinder d'un environnement CA Identity Manager existant.

Procédez comme suit:

Important : Les informations d'historique des mots de passe ne seront pas accessibles après la migration.

1. Arrêtez le serveur d'applications.
2. Désactivez le serveur de stratégies dans le fichier ra.xml situé sous \iam_im.ear\policyserver.rar\META-INF en définissant la valeur de la propriété de configuration Enabled sur False.
3. Modifiez le fichier web.xml situé sous \iam_im.ear\User_console.war/WEB-INF et définissez la propriété FrameworkAuthFilter sur Enabled=true.

   Remarque : Pour WebSphere, le fichier web.xml se trouve sous *répertoire_installation_WebSphere*/AppServer/profiles/*nom_profil*/config/cells/*nom_cellule*/applications/iam_im.ear/deployments/IdentityMinder/user_console.war/WEB-INF.
4. Lancez le serveur d'applications.
5. (WebSphere uniquement) Mettez à jour l'objet policyServer dans la console d'administration avec les mêmes valeurs que dans le fichier ra.xml.

Opérations SiteMinder

Les sections suivantes traitent des modifications des fonctionnalités SiteMinder, notamment des domaines de stratégie et des schémas d'authentification, pour la prise en charge de CA Identity Manager :

Collecte des informations d'identification de l'utilisateur à l'aide d'un schéma d'authentification personnalisé (page 344)

Remplace la méthode utilisée par CA Identity Manager pour collecter les informations d'identification des utilisateurs qui tentent d'accéder à un environnement CA Identity Manager.

Configuration des rôles d'accès (page 345)

Accorde l'accès aux fonctions d'une application.

Configuration de l'URL LogOff (page 360)

Empêche l'accès non autorisé à un environnement CA Identity Manager en appliquant une déconnexion complète.

Mise à jour d'un alias dans les domaines SiteMinder (page 362)

Permet de mettre à jour les domaines qui protègent un environnement CA Identity Manager lorsque vous modifiez l'alias de l'environnement.

Mots de passe SiteMinder (page 363)

Permet de changer le mot de passe du compte d'administrateur utilisé par CA Identity Manager pour communiquer avec SiteMinder et le secret partagé pour l'agent SiteMinder qui protège l'environnement CA Identity Manager.

Configuration des paramètres de l'agent CA Identity Manager (page 339)

Ajuste les performances de l'agent CA Identity Manager qui communique avec le serveur de stratégies SiteMinder.

Utilisation d'annuaires différents pour l'authentification et l'autorisation (page 365)

Active les administrateurs qui ont des profils dans un annuaire pour gérer les utilisateurs dans un annuaire différent.

Amélioration des performances opérationnelles des annuaires LDAP (page 367)

Permet d'augmenter le débit des demandes CA Identity Manager dans le référentiel d'utilisateurs en configurant l'ouverture de plusieurs connexions au même annuaire dans SiteMinder.

Collecte des informations d'identification de l'utilisateur à l'aide d'un schéma d'authentification personnalisé

SiteMinder utilise un schéma d'authentification pour collecter les informations d'identification d'utilisateur et pour déterminer l'identité d'un utilisateur lors de la connexion. Une fois qu'un utilisateur est identifié, CA Identity Manager génère une console d'utilisateur personnalisée en fonction des droits de l'utilisateur.

Vous pouvez implémenter un schéma d'authentification SiteMinder pour protéger un environnement CA Identity Manager.

Par exemple, vous pouvez implémenter un schéma d'authentification basé sur un formulaire HTML, qui collecte les informations d'identification dans un formulaire HTML. Un formulaire HTML vous permet de créer une page de connexion qui peut inclure des éléments personnalisés, comme le logo de votre société, et des liens vers les pages d'auto-enregistrement et de mot de passe oublié.

Remarque : Pour plus d'informations sur les schémas d'authentification, consultez le manuel *SiteMinder Policy Server Configuration Guide*.

Procédez comme suit:

1. Connectez-vous à l'une des interfaces suivantes :
   - Pour SiteMinder Web Access Manager r12 ou version ultérieure, connectez-vous à l'interface d'administration.
   - Pour CA eTrust SiteMinder 6.0 SP5, connectez-vous à l'interface utilisateur du serveur de stratégies.

   Remarque : Pour plus d'informations sur l'utilisation de ces interfaces, consultez la documentation de la version de SiteMinder que vous utilisez.
2. Créez un schéma d'authentification comme décrit dans le manuel *SiteMinder Policy Server Configuration Guide*.
3. Modifiez le domaine qui protège l'environnement CA Identity Manager approprié pour utiliser le schéma d'authentification que vous avez créé à l'étape 1.

   Le nom de domaine a le format suivant :

   *environnment_Identity_Manager*_ims_realm

   Remarque : Si vous avez configuré la prise en charge des tâches publiques, le domaine supplémentaire *environnement_Identity_Manager*_pub_realm s'affiche. Ce domaine utilise un schéma d'authentification anonyme pour permettre aux utilisateurs inconnus d'utiliser les fonctionnalités d'auto-enregistrement et de mot de passe oublié sans fournir d'informations d'identification. Ne modifiez pas les schémas d'authentification pour ces domaines.

Importation de définitions de données dans le référentiel de stratégies

Vous pouvez contrôler l'accès d'un utilisateur aux fonctions d'application à l'aide de stratégies SiteMinder. L'installation du serveur de stratégies inclut les définitions de données requises pour permettre ce contrôle. Importez le fichier IdmSmObjects.xdd à partir de :

répertoire_installation\xps\dd

répertoire_installation est le chemin d'installation du serveur de stratégies.

Planification des rôles d'accès

Pour contrôler l'accès aux applications, vous créez des rôles et des tâches d'accès. Une tâche d'accès permet d'accéder à une fonction dans une application. Un rôle d'accès contient une ou plusieurs tâches d'accès pour une ou plusieurs applications. Lorsqu'un rôle d'accès est affecté à un utilisateur, celui-ci peut utiliser les fonctions associées à ce rôle.

Pour obtenir plus d'informations sur le but des rôles d'accès, consultez la rubrique Rôles d'accès à une application.

Les rôles d'accès doivent être configurés dans CA Identity Manager et dans CA SiteMinder. Deux administrateurs doivent être impliqués :

- Administrateur Identity Manager : doit pouvoir créer des rôles et des tâches d'accès dans CA Identity Manager. Les rôles Administrateur système et Responsable des rôles d'accès par défaut incluent ces tâches.
- Administrateur SiteMinder : doit disposer de la portée Système et doit pouvoir gérer les objets système et du domaine. Pour plus d'informations, consultez le manuel *CA eTrust SiteMinder Policy Design*.

Remarque : L'interface utilisateur de conception de stratégie utilise le terme *environnement Identity Manager* pour désigner ce qui est désormais appelé un *environnement Identity Manager*. La documentation SiteMinder fournie avec le produit fait également référence à *Identity Manager*. A partir de la version 8.1, le nom de produit est *CA Identity Manager*.

La procédure suivante présente les étapes nécessaires à la création d'un rôle d'accès :

1. Un administrateur Identity Manager avec le rôle Gestionnaire de rôles d'accès peut effectuer les tâches suivantes :
   a. Créer des tâches d'accès
   b. Créer un rôle d'accès
   c. Communiquer les informations de rôle et de tâche à l'administrateur SiteMinder.
2. Pour créer une stratégie de contrôle d'accès basé sur les rôles, un administrateur SiteMinder :
   a. Affecte un annuaire d'utilisateurs associé à un ou plusieurs environnements Identity Manager à un domaine de stratégie.
   b. Associe un ou plusieurs environnements Identity Manager au domaine de stratégie de l'étape 1.
   c. Crée des domaines et des règles dans le domaine de stratégie, si aucun n'existe. Les domaines et les règles doivent correspondre aux ressources auxquelles les rôles d'accès ont accès.
   d. Crée des stratégies et les lie aux rôles à partir de l'environnement Identity Manager.
   e. (facultatif) Spécifie des réponses qui transfèrent des informations relatives aux droits aux ressources protégées.

   Pour obtenir des instructions sur les étapes précédentes, consultez le manuel *CA eTrust SiteMinder Policy Design*.

Activation de rôles d'accès pour SiteMinder

Pour utiliser des rôles d'accès avec CA SiteMinder, CA Identity Manager met en miroir tous les objets du référentiel d'objets CA Identity Manager relatifs aux rôles d'accès du référentiel de stratégies SiteMinder. Pour cela, vous configurez une propriété dans la console de gestion CA Identity Manager.

Pour activer les rôles d'accès pour SiteMinder :

1. Ouvrez la console de gestion.
2. Sélectionnez Environment (Environnement), *votre_environnement*, Advanced Settings (Paramètres avancés), Miscellaneous (Divers).
3. Ajoutez une nouvelle propriété en fournissant les informations suivantes :
   - Dans le champ Propriété, entrez :

     EnableSMRBAC
   - Dans le champ Valeur, entrez :

     true
4. Cliquez sur Ajouter. Cliquez ensuite sur Save (Enregistrer).

   Un message indiquant que l'environnement doit redémarrer s'affiche.
5. Cliquez sur Restart Environment (Redémarrer l'environnement).

   CA Identity Manager prend désormais en charge l'utilisation des rôles et des tâches d'accès avec CA SiteMinder.

Une fois que vous activez l'utilisation des rôles d'accès avec CA SiteMinder, tenez compte de ce qui suit :

- Si vous avez utilisé des rôles d'accès dans CA Identity Manager r8x, vous devez effectuer une étape de migration supplémentaire pour gérer les rôles d'accès dans la version actuelle de CA Identity Manager. Pour plus d'informations, consultez le *manuel de mise à niveau*.
- Pour désactiver la prise en charge des rôles d'accès dans SiteMinder, supprimez les objets de rôle et de tâche d'accès CA Identity Manager du référentiel de stratégies SiteMinder. Supprimez ensuite la propriété EnableSMRBAC de la liste des propriétés diverses et redémarrez l'environnement.

Ajout d'une tâche d'accès au rôle d'administration

Par défaut, les tâches d'accès ne s'affichent pas sous l'onglet Rôles et tâches. Vous devez ajouter les tâches d'accès au rôle d'administration de l'utilisateur connecté.

Procédez comme suit:

1. Connectez-vous à un compte CA Identity Manager avec un rôle incluant une tâche de création de rôle d'accès.
2. Cliquez sur Rôles et tâches, Modifier un rôle d'administration.
3. Sélectionnez le rôle d'administration de l'utilisateur connecté.
4. Cliquez sur l'onglet Tâches, Filtrer par catégorie et sélectionnez Rôles et tâches dans le menu déroulant.
5. Dans le menu Ajouter une tâche, sélectionnez Créer une tâche d'accès.
6. Cliquez sur Soumettre.

Création d'une tâche d'accès

Une tâche d'accès représente une action unique qu'un utilisateur peut effectuer dans une application métier, telle que la génération d'un bon de commande dans une application financière. Les utilisateurs peuvent effectuer cette action lorsqu'un rôle d'accès qui inclut la tâche d'accès leur est affecté.

Important : Pour créer des tâches d'accès, ajoutez les tâches d'accès (page 348) au rôle d'administration de l'utilisateur connecté.

Procédez comme suit:

1. Sélectionnez Rôles et tâches, Tâches d'accès, Créer une tâche d'accès.
2. Sélectionnez l'une des options suivantes.
   - Créer une tâche d'accès
   - Créer une copie d'une tâche d'accès

3. Remplissez les champs :

   Nom

   Nom unique que vous pouvez affecter à la tâche, comme Générer un bon de commande.

   Balise

   Balise unique pour la tâche. La balise doit commencer par une lettre ou un trait de soulignement et contenir uniquement des lettres, des chiffres ou des traits de soulignement.

   Description

   Remarque facultative sur l'objectif de la tâche.

   ID de l'application

   Définit l'identifiant d'une application, tel que le nom de l'application, associé à la tâche. L'ID de l'application ne doit contenir aucun espace ou caractère non alphanumérique.

   Notez cet ID, car vous en aurez besoin lors de l'activation du rôle dans SiteMinder.

4. Pour terminer la tâche d'accès, cliquez sur Soumettre.

Création d'un rôle d'accès

Un rôle d'accès contient des tâches d'accès, qui permettent d'accéder aux fonctions d'une application. Par exemple, un rôle peut contenir des tâches qui permettent aux membres du rôle de placer une commande dans une application d'achat et de mettre à jour les quantités dans une application de contrôle d'inventaire.

Effectuez les opérations suivantes pour créer un rôle d'accès :

1. Démarrez la création d'un rôle d'accès (page 349)
2. Définissez des propriétés de base pour le rôle d'accès dans l'onglet Profil. (page 350)
3. Sélectionnez des tâches d'accès pour le rôle. (page 350)
4. Définissez des stratégies de membre pour le rôle. (page 351)
5. Définissez des stratégies d'administration pour le rôle. (page 352)
6. Définissez des règles de propriété pour le rôle. (page 353)

Début de la création d'un rôle d'accès

1. Connectez-vous à un compte Identity Manager avec un rôle incluant une tâche de création de rôle d'accès.

2. Cliquez sur Rôles d'accès, puis sur Créer un rôle d'accès.

   Choisissez l'option de création de rôle ou de copie d'un rôle. Si vous sélectionnez Copier, recherchez le rôle.

3. Passez à la section suivante, Définition du profil d'un rôle d'accès.

Définition du profil d'un rôle d'accès

Définition du profil d'un rôle d'accès

1. Entrez un nom et une description, puis spécifiez les attributs personnalisés définis pour le rôle.

   Remarque : Dans l'onglet Profil, vous pouvez spécifier des attributs personnalisés qui indiquent des informations supplémentaires sur les rôles d'accès. Vous pouvez utiliser ces dernières pour faciliter les recherches de rôles dans les environnements comprenant un nombre important de rôles.

2. Sélectionnez Activé si le rôle peut être mis à la disposition des utilisateurs dès qu'il est créé.

3. Passez à la section suivante, Définition de stratégies de membres pour un rôle d'accès.

Sélection de tâches d'accès pour le rôle

Dans l'onglet Tâches :

1. Sélectionnez les tâches à inclure pour ce rôle. Sélectionnez d'abord les applications, puis la tâche. Vous pouvez inclure des tâches de différentes applications.

   Remarque : Si un autre rôle a les tâches dont vous avez besoin, cliquez sur Copier les tâches à partir d'un autre rôle. Vous pouvez modifier la liste qui s'affiche.

   Lors de la création d'un rôle ou d'une tâche, des icônes vous permettent d'ajouter, de modifier et de supprimer des éléments :

   Continuez ou sélectionnez l'élément actuel pour l'afficher ou le modifier.

   Si JavaScript est désactivé, cliquez sur le bouton d'avance rapide pour effectuer une sélection dans une liste déroulante.

   Revenez ou annulez la sélection précédente.

   Insérez un élément, tel qu'une tâche ou une règle.

Supprimez la tâche actuelle ou, dans une règle, l'expression qui suit.

Déplacez l'élément actuel en haut de la liste.

Déplacez l'élément actuel en bas de la liste.

2. Passez à la section suivante, Définition de stratégies de membres pour un rôle d'accès.

Définition de stratégies de membres pour un rôle d'accès

Une stratégie de membre définit une règle de membre et des règles de portée pour un rôle. Vous pouvez définir plusieurs stratégies de membre pour un rôle. Pour chaque stratégie, les utilisateurs qui remplissent la condition de la règle de membre dispose de la portée permettant l'utilisation du rôle défini dans la stratégie.

Procédez comme suit:

1. Cliquez sur l'onglet Membres.
2. Cliquez sur Ajouter pour définir des stratégies de membre.
3. (Facultatif) Dans la page Stratégie de membre, définissez également une règle de membre pour les utilisateurs pouvant utiliser ce rôle.

   Définir une règle de membre affecte automatiquement le rôle aux utilisateurs qui correspondent aux critères de la stratégie de membre.

   Remarque : Définissez des stratégies de membre qui utilisent uniquement des attributs d'annuaire, par exemple title=Manager. Si vous définissez des stratégies de membre qui font référence aux objets non stockés dans l'annuaire d'utilisateurs, comme les rôles d'administration, SiteMinder ne peut pas résoudre la référence.
4. Vérifiez que la stratégie de membre s'affiche dans l'onglet Membres.

   Pour modifier une stratégie, cliquez sur la flèche à gauche. Pour supprimer une stratégie, cliquez sur l'icône moins.
5. Dans l'onglet Membres, cochez la case Les administrateurs peuvent ajouter des membres à ce rôle et les en supprimer.

   Une fois cette fonctionnalité activée, vous définissez les actions Action Ajouter et Action Supprimer. Ces actions définissent les implications de l'ajout ou de la suppression d'un utilisateur comme membre du rôle.

Définition de stratégies de membres pour un rôle d'accès

Une stratégie d'administration définit des règles d'administration, des règles de portée et des droits d'administrateur pour un rôle. Vous pouvez définir plusieurs stratégies d'administration pour un rôle. Chaque stratégie indique que si un administrateur remplit les conditions définies dans la règle d'administration, il dispose de la portée et des droits d'administrateur définis dans la stratégie.

Procédez comme suit:

1. Sélectionnez l'onglet Administrateurs pour le rôle d'accès.
2. Pour activer l'option Gérer les administrateurs, cochez la case Les administrateurs peuvent ajouter des administrateurs à ce rôle et les en supprimer.

   Une fois que vous activez cette fonctionnalité, définissez les actions associées à l'ajout ou à la suppression d'un utilisateur comme administrateur du rôle.
3. Dans l'onglet Administrateurs, ajoutez des stratégies d'administration qui incluent des règles d'administration et de portée, ainsi que des droits d'administration. Chaque stratégie doit inclure un droit au minimum (Gérer les membres ou Gérer les administrateurs).

   Vous pouvez ajouter plusieurs stratégies d'administration avec des règles et des droits différents pour les administrateurs qui correspondent aux critères de la règle.

   Remarque : Définissez des stratégies d'administration qui utilisent uniquement des attributs d'annuaire, par exemple title=Manager. Si vous définissez des stratégies de membre qui font référence aux objets non stockés dans l'annuaire d'utilisateurs, comme les rôles d'administration, SiteMinder ne peut pas résoudre la référence.
4. Pour modifier une stratégie, cliquez sur la flèche à gauche. Pour supprimer une stratégie, cliquez sur l'icône moins.
5. Passez à la section suivante, Définition de règles de propriété pour un rôle d'accès.

Définition de règles de propriété pour un rôle d'accès

Une règle de propriété définit les utilisateurs qui peuvent modifier un rôle. Vous pouvez définir plusieurs règles de propriété pour un rôle.

Procédez comme suit:

1. Sélectionnez l'onglet Propriétaires pour le rôle d'accès.
2. Définissez les règles de propriété, qui déterminent les utilisateurs qui peuvent modifier le rôle.

   Remarque : Définissez des règles de propriété qui utilisent uniquement des attributs d'annuaire, par exemple : title=Manager. Si vous définissez des règles de propriété qui font référence aux objets non stockés dans l'annuaire d'utilisateurs, comme les rôles d'administration, SiteMinder ne peut pas résoudre la référence.
3. Cliquez sur Soumettre.

   Un message s'affiche indiquant que la tâche a été soumise. Un délai peut se produire avant qu'un utilisateur puisse utiliser le rôle.

Activation de rôles d'accès dans SiteMinder

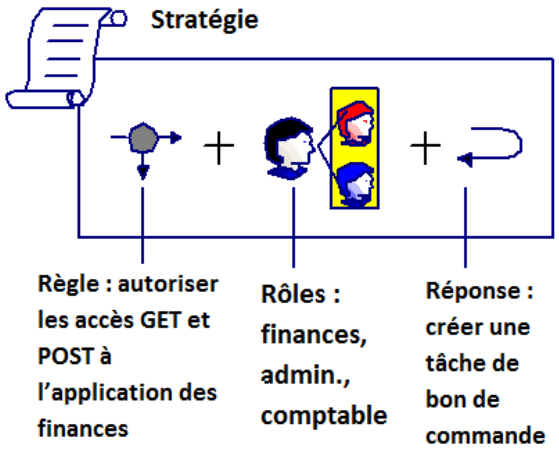
Un administrateur SiteMinder associe des rôles à des stratégies de sécurité qui définissent les interactions des utilisateurs avec des ressources. Les stratégies peuvent associer les objets suivants :

- Utilisateurs et Groupes d'utilisateurs : identifient un ensemble d'utilisateurs affectés par une stratégie.
- Rôles : identifie les utilisateurs auxquels un ensemble de droits a été affecté dans Identity Manager.
- Règles : identifie une ressource et les actions autorisées ou refusées sur la ressource. La ressource est généralement une URL, une application ou un script.
- Réponses : détermine la réaction à une règle. Lorsqu'une règle se déclenche, les réponses sont envoyées à un agent SiteMinder.

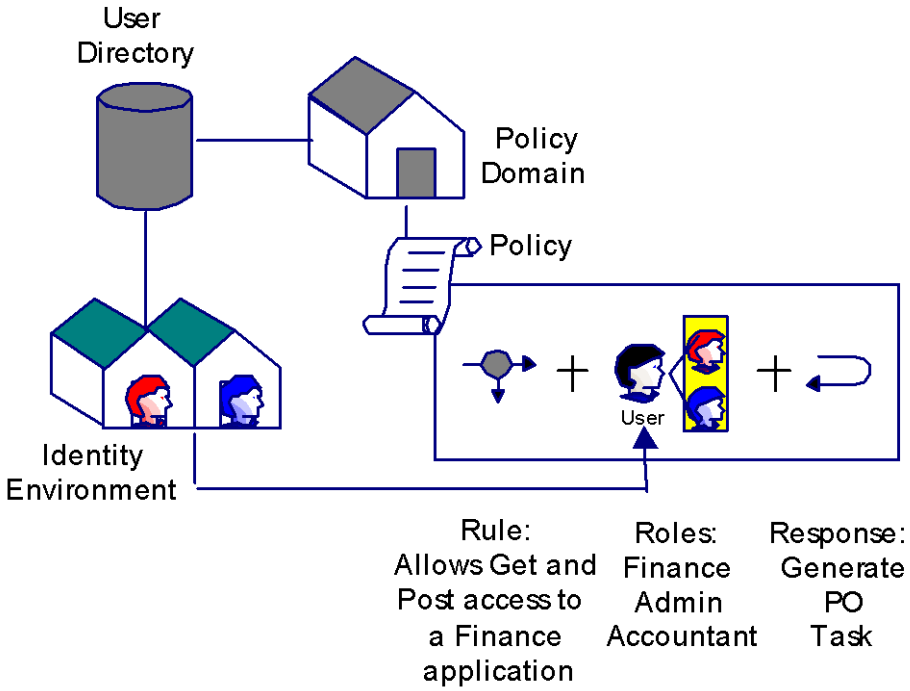
  Identity Manager utilise les réponses SiteMinder pour envoyer des informations sur les tâches et les rôles à une ressource protégée.

Vous pouvez lier les stratégies SiteMinder à des utilisateurs, à des rôles ou à des utilisateurs *et* des rôles. Lorsqu'un utilisateur ou un membre de rôle tente d'accéder à une ressource protégée, SiteMinder utilise les informations de la stratégie pour autoriser ou refuser l'accès, et déclencher des réponses.

Le schéma suivant illustre la relation entre les objets de stratégie dans une stratégie basée sur les rôles.



Les stratégies SiteMinder sont créées dans des domaines de stratégie, qui associent logiquement des annuaires d'utilisateurs aux ressources protégées. Le schéma suivant illustre la relation entre les objets de stratégie dans une stratégie basée sur les rôles.



Pour accorder des droits d'utilisateur à une application protégée, un administrateur SiteMinder associe une règle dans la stratégie de l'application avec une réponse. La réponse contient un attribut de réponse généré par SiteMinder qui récupère des informations sur les droits à partir d'Identity Manager.

Lorsque SiteMinder autorise l'accès d'un membre de rôle à une ressource protégée, les événements suivants ont lieu :

1. La règle de la stratégie s'exécute dans SiteMinder, et déclenche la réponse associée.
2. Le serveur de stratégies obtient les informations sur les droits à inclure dans la réponse à partir d'Identity Manager.
3. Le serveur de stratégies transfère l'attribut de réponse à l'agent Web.
4. L'agent Web met les informations de droit à la disposition de l'application sous la forme d'une variable d'en-tête HTTP ou d'un cookie.

Attributs de réponse générés par SiteMinder

Identity Manager transfère les informations sur les droit aux applications via les réponses de l'agent Web SiteMinder. Ces réponses contiennent des variables d'en-tête HTTP dans les attributs de la réponse, qui peuvent être utilisées par l'application pour déterminer les droits d'accès d'un utilisateur. Les réponses sont incluses dans des stratégies SiteMinder, qui déterminent les relations des utilisateurs avec une ressource protégée.

Les administrateurs SiteMinder peuvent configurer une réponse qui inclut deux types d'attributs de réponse pour transférer des informations à une application :

- SM_USER_APPLICATION_ROLES[:*id_application*] : renvoie une liste de rôles a affecté à un utilisateur.
- SM_USER_APPLICATION_TASKS[:*id_application*] : renvoie une liste de tâches qu'un utilisateur peut effectuer selon les rôles qui lui sont affectés.

L'ID d'application limite l'ensemble des rôles et des tâches demandés à une application spécifique. Par exemple, si vous créez l'attribut de réponse suivant :

SM_USER_APPLICATION_ROLES:Finance_application

SiteMinder renvoie les rôles qui comprennent des tâches dans l'application Finance à l'agent Web, qui transfère alors les informations à l'application Finance.

Remarque : L'*ID d'application* que vous fournissez doit correspondre à l'*ID d'application* fourni lorsque vous avez utilisé l'option Créer une tâche d'accès dans Identity Manager. Si vous n'avez pas encore créé la tâche, l'ID d'application peut être un nom que vous choisissez, mais il ne doit contenir aucun espace ou caractère non alphanumérique.

Vous pouvez spécifier plusieurs ID d'application dans une liste séparés par des virgules pour renvoyer l'ensemble des rôles et des tâches à partir de plusieurs applications dans un attribut de réponse unique. Par exemple, pour renvoyer la liste de rôles qu'un utilisateur a dans les applications Finance et Purchasing, spécifiez le suivant :

SM_USER_APPLICATION_ROLES:Finance, Purchasing

Liste de contrôle pour l'activation des rôles d'accès dans SiteMinder

Remarque : Les étapes suivantes supposent que l'application à laquelle le rôle d'accès que vous créez s'applique est déjà protégée par SiteMinder. Si vous créez un rôle d'accès pour une application qui n'est pas protégée par SiteMinder, consultez le manuel *CA eTrust SiteMinder Policy Design* pour obtenir des instructions sur la configuration de l'application dans SiteMinder.

✓	Etape	Voir
	1. Dans l'interface utilisateur du serveur de stratégies, affectez l'annuaire d'utilisateurs associé à l'environnement Identity Manager à un domaine de stratégie.	*Manuel CA eTrust SiteMinder Policy Design*
	2. Ajoutez l'environnement Identity Manager au domaine SiteMinder qui protège l'application à laquelle le rôle d'accès s'applique.	*Manuel CA eTrust SiteMinder Policy Design*
	3. Dans le domaine de stratégie, créez des domaines et des règles (s'ils n'existent pas déjà) qui correspondent aux ressources auxquelles le rôle d'accès accorde l'accès.	*Manuel CA eTrust SiteMinder Policy Design*
	4. Créez une réponse pour transférer les informations sur les droits à la ressource.	Création d'une réponse SiteMinder (page 358)
	5. Créez une stratégie et associez-la avec : ■ Le rôle que vous avez créé dans Identity Manager. ■ Les domaines et les règles que vous avez créées à l'étape 2. ■ Les réponses que vous avez créées à l'étape 4.	*Manuel CA eTrust SiteMinder Policy Design*

Ajout d'environnements Identity Manager à un domaine de stratégie

Pour permettre à SiteMinder de prendre en charge les rôles d'accès, associez un environnement CA Identity Manager à un annuaire d'utilisateurs et à un domaine de stratégie dans SiteMinder.

Remarque : Ajoutez le référentiel d'utilisateurs associé à l'environnement CA Identity Manager au domaine de stratégie *avant* d'ajouter l'environnement CA Identity Manager au domaine de stratégie.

Pour ajouter un environnement CA Identity Manager à un domaine de stratégie :

1. Dans la boîte de dialogue Domaine de stratégie de l'interface utilisateur du serveur de stratégies, ajoutez le référentiel d'utilisateurs associé à l'environnement CA Identity Manager à un domaine de stratégie comme suit :
   a. Sélectionnez l'onglet Annuaires d'utilisateurs.
   b. Dans la zone déroulante au bas de l'onglet, sélectionnez l'annuaire d'utilisateurs à inclure dans le domaine de stratégie.
   c. Cliquez sur Ajouter.

      L'interface utilisateur du serveur de stratégies ajoute l'annuaire à la liste affichée dans l'onglet Annuaires d'utilisateurs.
   d. Cliquez sur Appliquer.
2. Ajoutez l'environnement CA Identity Manager au domaine de stratégie comme suit :
   a. Sélectionnez l'onglet Environnements CA Identity Manager.
   b. Sélectionnez l'environnement CA Identity Manager que vous voulez associer au domaine de stratégie dans la liste déroulante au bas de l'onglet.
   c. Cliquez sur Ajouter.

      L'interface utilisateur du serveur de stratégies ajoute l'environnement sélectionné à la liste des environnements CA Identity Manager en haut de l'onglet.
3. Pour enregistrer vos sélections et fermer la boîte de dialogue, cliquez sur OK.

   Les environnements CA Identity Manager sélectionnés sont disponibles pour la création de stratégies.

Création d'une réponse SiteMinder

1. Connectez-vous à l'interface utilisateur du serveur de stratégies.
2. Selon les droits d'administration dont vous disposez, effectuez l'une des actions suivantes :
   - Si vous disposez du droit Gérer les objets système et de domaine :
     a. Dans le volet Objet, cliquez sur l'onglet Domaines.
     b. Sélectionnez le domaine de stratégie auquel vous souhaitez ajouter une réponse.
   - Si vous disposez du droit Manage Domain Objects (Gérer les objets de domaine), sélectionnez le domaine de stratégie auquel vous voulez ajouter une réponse dans le volet Objet.
3. Dans la barre de menus, sélectionnez Modifier, <nom_domaine>, Créer une réponse.

   La boîte de dialogue Réponse de CA SiteMinder s'ouvre (voir la rubrique traitant de la boîte de dialogue Réponse).
4. Entrez un nom et une description pour la nouvelle réponse.
5. Dans la zone de groupe Type d'agent, sélectionnez le bouton radio SiteMinder.
6. Sélectionnez l'option Agent Web dans la liste déroulante de la zone de groupe Type d'agent et cliquez sur Appliquer pour enregistrer les modifications.
7. Cliquez sur Créer.

   L'éditeur d'attribut de réponse SiteMinder s'ouvre.
8. Dans la liste déroulante d'attributs, sélectionnez l'attribut de réponse WebAgent-HTTP-Header-Variable.
9. Dans l'onglet Attribute Setup (Configuration d'attributs), sélectionnez le bouton radio Attribut d'utilisateur.
10. Dans le champ Variable, entrez le nom de la variable qui sera transférée à l'application.

    Par exemple, si vous spécifiez la variable TASKS, l'en-tête suivant est renvoyé à l'application :

    HTTP_TASKS

11. Dans le champ Nom de l'attribut, spécifiez l'attribut de réponse comme suit :
    - SM_USER_APPLICATION_ROLES[:*id_application_1, id_application_2, ...id_application_n*] : renvoie une liste des rôles affectés à un utilisateur.
    - SM_USER_APPLICATION_TASKS[:*id_application_1, id_application_2, ...id_application_n*]

    Pour obtenir plus d'informations, reportez-vous à la rubrique Attributs de réponse générés par SiteMinder (page 355).
12. Cliquez sur OK pour enregistrer les modifications et revenir à la fenêtre d'administration de SiteMinder.

Ajout de rôles à une stratégie SiteMinder

Lorsqu'un utilisateur auquel un rôle d'accès approprié a été affecté tente d'accéder à une ressource protégée, le serveur de stratégies SiteMinder vérifie que le rôle d'accès a bien été affecté à l'utilisateur, puis exécute les règles incluses dans la stratégie pour déterminer si l'utilisateur est autorisé à accéder à la ressource.

Pour ajouter des rôles d'accès à une stratégie SiteMinder :

1. Dans la boîte de dialogue Stratégie de SiteMinder, cliquez sur l'onglet Utilisateurs.

   Cet onglet contient des onglets pour chaque annuaire d'utilisateurs et environnement CA Identity Manager inclus dans le domaine de stratégie.
2. Sélectionnez l'environnement CA Identity Manager qui contient les rôles que vous voulez ajouter à la stratégie.
3. Cliquez sur l'option d'ajout/de suppression.

   La boîte de dialogue Rôle d'Identity Manager pour la stratégie SiteMinder s'ouvre.
4. Pour ajouter des rôles à la stratégie, sélectionner une entrée dans la liste des membres disponibles et déplacez-la dans la liste des membres actuels.
5. Cliquez sur OK pour enregistrer les modifications et revenir à la boîte de dialogue Stratégie de SiteMinder.

Exclusion de rôles d'une stratégie

Outre l'utilisation de rôles d'accès pour permettre d'accéder à des applications, vous pouvez les utiliser pour empêcher des membres de rôles d'accès d'accéder à une application. Pour cela, vous excluez les rôles des stratégies SiteMinder. Lorsqu'un utilisateur auquel a été affecté le rôle d'accès exclu dans CA Identity Manager tente d'accéder à une ressource protégée, le serveur de stratégies vérifie l'exclusion du rôle CA Identity Manager pour l'utilisateur affecté. Lors de la vérification, l'accès à la ressource est bloqué.

Procédez comme suit:

1. Dans la boîte de dialogue Stratégie de SiteMinder, cliquez sur l'onglet Utilisateurs.

   Cet onglet contient des onglets pour chaque annuaire d'utilisateurs et environnement CA Identity Manager inclus dans le domaine de stratégie.

2. Cliquez sur l'environnement CA Identity Manager qui contient les rôles que vous voulez exclure de la stratégie.

3. Cliquez sur l'option d'ajout/de suppression.

   La boîte de dialogue Rôle de CA Identity Manager pour la stratégie SiteMinder s'ouvre.

4. Pour ajouter des rôles à la stratégie, sélectionnez une entrée dans la liste des membres disponibles et cliquez sur la flèche vers la gauche pour la transférer dans la liste des membres actuels.

   La procédure contraire supprime les rôles de la liste des membres actuels.

5. Dans la liste des membres actuels, sélectionnez les rôles à exclure, puis cliquez sur Exclure, sous la liste.

   Un cercle rouge avec une barre s'affiche à gauche des rôles exclus.

6. Cliquez sur OK pour enregistrer les modifications et revenir à la boîte de dialogue Stratégie de SiteMinder.

Configuration de l'URI LogOff

Pour renforcer la protection de l'environnement CA Identity Manager, configurez l'agent Web SiteMinder qui le protège de façon à ce qu'il mette fin aux sessions d'utilisateur après leur déconnexion de CA Identity Manager.

L'agent Web met fin à une session d'utilisateur en supprimant les cookies de session et d'authentification SiteMinder du navigateur Web, et en indiquant au serveur de stratégies de supprimer toutes les informations de session.

Pour mettre fin à la session SiteMinder, configurez la fonctionnalité de déconnexion dans le champ LogOffURI de l'objet de configuration d'agent pour l'agent SiteMinder qui protège l'environnement CA Identity Manager.

Remarques :

- Un agent SiteMinder a un URI LogOff. Toutes les applications protégées par l'agent utilisent la même page de déconnexion.
- Lorsque vous configurez des pages de déconnexion personnalisées dans la console de gestion, comme décrit dans la rubrique Configure Custom Logout Pages (Configurer les pages de déconnexion personnalisées), CA Identity Manager envoie la demande de déconnexion à la page de déconnexion personnalisée *et* à l'URI LogOff. Toutefois, CA Identity Manager affiche uniquement la page de déconnexion personnalisée pour l'utilisateur.

Procédez comme suit:

1. Connectez-vous à l'une des interfaces suivantes :
   - Pour SiteMinder r12 ou version ultérieure, connectez-vous à l'interface d'administration.
   - Pour CA eTrust SiteMinder 6.0 SP5, connectez-vous à l'interface utilisateur du serveur de stratégies.

   Remarque : Pour plus d'informations sur l'utilisation de ces interfaces, consultez la documentation de la version de SiteMinder que vous utilisez.
2. Modifiez la propriété #LogOffUri dans l'objet de configuration d'agent pour l'agent qui protège l'environnement CA Identity Manager comme suit :
   - Supprimez le dièse.
   - Dans le champ Valeur, entrez l'URI suivant :

     /iam/im/logout.jsp

   Remarque : Vous sélectionnez un objet de configuration d'agent lors de l'installation de l'agent Web. Pour plus d'informations, consultez le manuel *SiteMinder Web Access Manager Policy Server Administration Guide*.
3. Enregistrez les modifications.
4. Redémarrez le serveur Web.

Alias dans les domaines SiteMinder

Un *alias* est une chaîne unique qui est ajoutée à l'URL pour accéder à un environnement CA Identity Manager. Par exemple, lorsque l'alias d'un environnement est *employés*, l'URL pour accéder à cet environnement est le suivant :

`http://mon_serveur.ma_société.org/iam/im/employés`

mon_serveur.ma_société.org

Définit le nom de domaine complet du serveur sur lequel CA Identity Manager est installé.

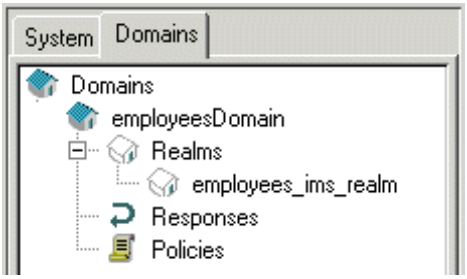
Lorsque vous créez un environnement CA Identity Manager dans la console de gestion, spécifiez un ou plusieurs alias. Vous pouvez également spécifier un alias public.

SiteMinder utilise le nom d'environnement pour nommer les objets qui le protègent. Par exemple, lorsque vous spécifiez le nom *employés*, SiteMinder crée des objets nommés *employéstype_objet*.

type_objet

Définit l'objet SiteMinder, comme employés_ims_realm.

Les illustrations suivantes présente deux objets créés par SiteMinder :



Mise à jour d'un alias dans les domaines SiteMinder

Si vous modifiez l'alias protégé ou public dans la console de gestion, CA Identity Manager tente de mettre à jour les noms d'alias dans le serveur de stratégies. Si CA Identity Manager ne peut pas mettre à jour les noms, vous pouvez les mettre à jour manuellement à partir de l'une des interfaces suivantes :

- Pour CA SiteMinder Web Access Manager r12 ou version ultérieure, utilisez l'interface d'administration.
- Pour CA eTrust SiteMinder 6.0 SP5, utilisez l'interface utilisateur du serveur de stratégies.

Procédez comme suit:

1. Recherchez les domaines de l'environnement CA Identity Manager.

   Ces domaines sont créés automatiquement, avec d'autres objets SiteMinder requis, lorsque CA Identity Manager est intégré à SiteMinder.

   Les domaines utilisent la convention d'attribution de nom suivante :

   - *environnement_Identity_Manager*_ims_realm : protège la console d'utilisateur.
   - *environnement_Identity_Manager*_pub_realm : active la prise en charge des tâches publiques, comme les tâches d'auto-enregistrement et de mot de passe oublié. Ce domaine s'affiche uniquement si vous avez configuré un alias public.

     Remarque : Si vous utilisez l'interface utilisateur du serveur de stratégies pour modifier le domaine, recherchez d'abord le domaine de stratégie (*environnement_Identity_Manager*Domaine) pour l'environnement CA Identity Manager. Les domaines se trouvent sous le domaine.

2. Modifiez la ressource pour le domaine comme suit :

   /iam/im/*nouvel_alias*

   Ne supprimez pas /iam/im/ de l'alias dans le filtre de ressource.

3. Enregistrez les modifications.

Remarque : Pour obtenir des instructions sur la modification des alias dans la console de gestion, reportez-vous à la rubrique traitant des modification de propriétés CA Identity Manager.

Modification d'un mot de passe ou d'un secret partagé SiteMinder

Lorsque vous installez des extensions CA Identity Manager sur le serveur de stratégies, spécifiez le mot de passe du compte d'administrateur SiteMinder utilisé par CA Identity Manager pour communiquer avec le serveur de stratégies.

Vous pouvez modifier ce mot de passe, mais pour cela, vous devez le chiffrer. Pour chiffrer un mot de passe, utilisez l'outil de modification de mots de passe fourni avec CA Identity Manager.

Remarque : Vérifiez que la variable JAVA_HOME est définie pour votre environnement avant de modifier le mot de passe SiteMinder.

Procédez comme suit:

1. Chiffrez le mot de passe comme suit :
   a. A partir de la ligne de commande, accédez à *outils_admin*\PasswordTool, où *outils_admin* est l'emplacement d'installation des outils d'administration, comme dans les exemples suivants :
      - **Windows :** <chemin_installation>\tools\PasswordTool
      - **UNIX :** <chemin_installation2>/tools/PasswordTool
   b. Saisissez la commande suivante :

      pwdtools *nouveau_mot_passe*

      Dans cette commande, *nouveau_mot_passe* est le mot de passe à chiffrer.

      Remarque : Pour plus d'informations sur les options de l'utilitaire pwdtools, entrez la commande suivante :

      pwdtools help
   c. Copiez le mot de passe chiffré.
2. Effectuez l'opération appropriée :
   - Si CA Identity Manager est exécuté sur un serveur d'applications WebLogic, effectuez les tâches suivantes :
     a. Dans la console WebLogic, modifiez l'adaptateur de ressource WebLogic dans le descripteur de connecteur policyserver_rar.
     b. Ajoutez le mot de passe chiffré comme valeur de la propriété Password.
   - Si CA Identity Manager est exécuté sur un serveur d'applications JBoss, effectuez les tâches suivantes :

     R. Ouvrez ra.xml à partir de *répertoire_installation_JBoss*\server\default\deploy\iam_im.ear\policyserver_rar\META-INF.

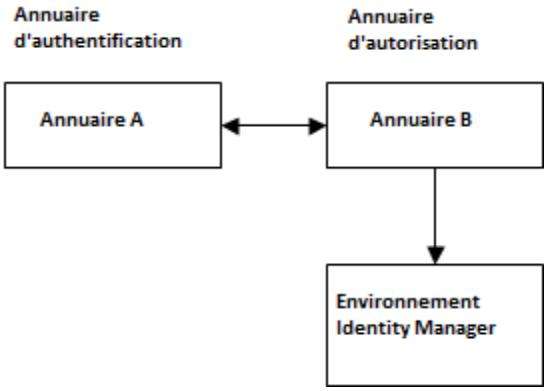
     B. Ajoutez le mot de passe chiffré comme valeur de la propriété de configuration Password.
   - Si CA Identity Manager est exécuté sur un serveur d'applications WebSphere, effectuez les tâches suivantes :

     R. Dans la console WebSphere, ouvrez ra.xml.

     B. Ajoutez le mot de passe chiffré comme valeur de la propriété de configuration Password.
3. Redémarrez le serveur d'applications.

Configuration d'un environnement CA Identity Manager pour l'utilisation d'annuaires différents pour l'authentification et l'autorisation

Un administrateur peut devoir gérer des utilisateurs dont les profils existent dans un référentiel d'utilisateurs différent de celui utilisé pour authentifier l'administrateur. En d'autres termes, lors de la connexion à l'environnement CA Identity Manager, l'administrateur doit être authentifié à partir d'un annuaire et autorisé à gérer des utilisateurs à partir d'un autre annuaire, comme dans l'illustration suivante :



Procédez comme suit:

1. Connectez-vous à l'une des interfaces suivantes :
   - Pour SiteMinder Web Access Manager r12 ou version ultérieure, connectez-vous à l'interface d'administration.
   - Pour CA eTrust SiteMinder 6.0 SP5, connectez-vous à l'interface utilisateur du serveur de stratégies.

   Remarque : Pour plus d'informations sur l'utilisation de ces interfaces, consultez la documentation de la version de SiteMinder que vous utilisez.
2. Créez deux annuaires d'utilisateurs.

   Un annuaire référence les données d'authentification (profils d'administrateur) tandis que l'autre référence les données d'autorisation (profils d'utilisateur).
3. Dans la console de gestion, créez un environnement CA Identity Manager.

   Sélectionnez l'annuaire d'autorisation en tant qu'annuaire CA Identity Manager.

4. Dans l'interface pour la version de SiteMinder utilisée, ajoutez l'annuaire d'authentification au domaine pour l'environnement CA Identity Manager que vous avez créé à l'étape précédente.

   Le domaine et les autres objets requis par SiteMinder sont créés automatiquement lorsque vous créez un environnement et que SiteMinder est intégré à CA Identity Manager.

   Le domaine utilise la convention d'attribution de nom suivante :

   *environnement_Identity_Manager*Domaine

5. Vérifiez que l'annuaire s'affiche d'abord dans la liste d'annuaires associés au domaine.
6. Recherchez le domaine *environnement_Identity_Manager*_ims_realm.
7. Mappez l'annuaire d'autorisation vers l'annuaire d'authentification dans la section Avancé de la définition de domaine.
8. Recherchez la réponse *environnement_Identity_Manager*response_ims suivante.
9. Ajoutez des attributs de réponse aux réponses comme suit :

Champ	**Valeur**
Attribut	Web-Agent-HTTP-Header-Variable
Type d'attribut	Attribut d'utilisateur
Nom de la variable	sm_userdn
Nom de l'attribut	SM_USERNAME

10. Enregistrez les modifications.

    CA Identity Manager utilise désormais des annuaires différents pour l'authentification et l'autorisation.

Amélioration des performances opérationnelles des annuaires LDAP

Le traitement des opérations d'annuaire peut prendre un certain temps, car toutes les demandes CA Identity Manager pour l'annuaire d'utilisateurs LDAP sont routées via un ensemble fixe de connexions.

Pour augmenter le débit des demandes CA Identity Manager dans l'annuaire d'utilisateurs, configurez l'ouverture de plusieurs connexions au même annuaire dans SiteMinder. Pour cela, ajoutez le serveur LDAP plusieurs fois dans la boîte de dialogue Configuration du basculement d'annuaire et de l'équilibrage de la charge dans l'interface utilisateur du serveur de stratégies.

Le nombre de fois que vous entrez le serveur LDAP, ainsi que le nombre de connexions à créer, dépend de la charge sur CA Identity Manager.

Annexe A: Conformité à la norme FIPS 140-2

Ce chapitre traite des sujets suivants :

Présentation d'FIPS

La norme FIPS (Federal Information Processing Standards) 140-2 est une norme de sécurité pour les bibliothèques cryptographiques et pour les algorithmes qu'un produit doit utiliser pour le chiffrement. Le chiffrement FIPS 140-2 affecte la communication de l'ensemble des données confidentielles entre des composants de produits CA et entre des produits CA et des produits tiers. La norme FIPS 140-2 indique la configuration requise pour utiliser des algorithmes cryptographiques dans un système de sécurité protégeant les données sensibles et non classifiées.

CA Identity Manager utilise la norme de chiffrement avancé (AES) adaptée par le gouvernement des Etats-Unis. CA Identity Manager inclut les bibliothèques cryptographiques RSA Crypto-J v3.5 et Crypto-C ME v2.0, validées comme conformes aux conditions de sécurité requises par la norme FIPS 140-2 pour les modules cryptographiques.

Communications

Le chiffrement FIPS s'applique à toutes les communications de données entre CA Identity Manager et les composants suivants :

- Serveur CA Identity Manager
- Serveur de provisionnement
- Gestionnaire et clients de provisionnement
- Serveurs de connecteurs C++
- Terminaux de serveur de connecteurs C++ (si pris en charge par le terminal)
- Serveurs de connecteurs CA IAM (CA IAM CS)
- Terminaux de CA IAM CS (si pris en charge par la terminal)
- Connector Xpress (si pris en charge par le terminal)
- Agents de synchronisation de mots de passe Windows
- JIAM (Java Identity and Access Management)

Installation

Le programme d'installation de CA Identity Manager permet de configurer CA Identity Manager pour la conformité à la norme FIPS 140-2.

Tous les composants d'un environnement CA Identity Manager requièrent l'activation de FIPS 140-2 pour la prise en charge de cette norme par CA Identity Manager. Une clé de chiffrement FIPS est nécessaire pour activer FIPS 140-2 lors de l'installation. Un outil de modification de mots de passe (pwdtools.bat/pwdtools.sh) pour la génération d'une clé FIPS est fourni à l'emplacement suivant :

```
<chemin_installation>\PasswordTool\pwdtools.bat
```

Important : Utilisez la même clé de chiffrement FIPS 140-2 dans toutes les installations et veillez à sauvegarder le fichier de clé généré par l'outil de modification de mots de passe.

Connexion à CA SiteMinder

Lors de la connexion à CA SiteMinder pendant l'installation de CA Identity Manager, tenez compte du fait que les configurations du mode FIPS et de la version du produit sont prises en charge uniquement telles qu'indiquées dans le tableau suivant :

CA Identity Manager r12	SiteMinder	SiteMinder Version (Version LDAP)
FIPS-only mode	FIPS-only mode	r12
FIPS-only mode	FIPS-compatible mode	r12
Non-FIPS mode	FIPS-compatible mode	r12
Non-FIPS mode	Non-FIPS mode	r6

Stockage du fichier de clé

CA Identity Manager utilise le système de fichiers pour le stockage de la clé de chiffrement FIPS. L'administrateur CA Identity Manager est responsable de la protection des fichiers contre l'accès non autorisé et définit pour ce faire les autorisations d'accès à l'annuaire pour les types de groupe ou d'utilisateur spécifiques, tels que l'utilisateur autorisé à exécuter CA Identity Manager.

Le tableau suivant répertorie l'emplacement des fichiers de clé FIPS pour chaque composant CA Identity Manager.

Composant	Emplacement d'installation
Serveur CA Identity Manager	*IdentityMinder.ear*\config\com\netegrity\config\keys\FIPSkey.dat *IdentityMinder.ear* est l'emplacement d'installation de CA Identity Manager sur le serveur d'applications.
Serveur de provisionnement	*Installation_serveur_provisionnement*\data\tls\keymgmt\imps_datakey
Serveur de connecteurs C++	*Installation_serveur_provisionnement*\data\tls\keymgmt\imps_datakey

Outil de modification de mots de passe

L'utilitaire d'outil de modification de mots de passe conforme à la norme FIPS pwdtools.bat, ou pwdtools.sh, peut générer la clé de chiffrement pendant l'installation de CA Identity Manager, à partir de la ligne de commande.

Modifiez le fichier pwdtools.bat/pwdtools.sh avant d'utiliser l'outil de modification de mots de passe et définissez la variable JAVA_HOME de façon appropriée.

Important : CA Identity Manager ne prend pas en charge la migration ou le rechiffrement des données. Par conséquent, assurez-vous que les clés de chiffrement ne soient pas modifiées après l'installation.

La syntaxe de la commande est la suivante :

```
pwdtools -{FIPSKEY|JSAFE|FIPS|RC2} -p plain text [-k <emplacement_fichier_clé>]
[-f  <fichier_paramètres_chiffrement>]
```

JSAFE

Permet de chiffrer une valeur de texte brut à l'aide de l'algorithme PBE.

Exemple :

```
pwdtools -JSAFE –p mot_passe
```

Remarque : Dans les versions antérieures, le mot de passe de l'administrateur d'amorçage était stocké en texte clair. Si vous procédez à la mise à niveau ou à la migration de CA Identity Manager vers la version r12.6 SP1 ou une version ultérieure, vous devez chiffrer manuellement le mot de passe en texte clair. Vérifiez que l'option JSAFE est spécifiée lorsque vous utilisez l'outil et procédez comme suit :

1. Après avoir effectué la mise à niveau ou la migration de CA Identity Manager vers la version r12.6 SP1 ou une version ultérieure, accédez à la base de données de référentiel d'objets CA Identity Manager et recherchez la table suivante :
   `IM_AUTH_USER`
2. Chiffrez le mot de passe en texte clair à l'aide de l'outil de modification de mots de passe avec JSAFE.
3. Remplacez le texte clair par le mot de passe chiffré dans la table.

FIPSKEY

Permet de créer un fichier de clé FIPS pour le programme d'installation. Générez la clé avant d'installer CA Identity Manager.

Exemple :

`pwdtools -FIPSKEY –k C:\`*`chemin_accès_clé`*`\FIPSkey.dat`

où *chemin_accès_clé* est le chemin d'accès complet à l'emplacement sous lequel vous voulez stocker la clé FIPS.

L'outil de modification de mots de passe crée la clé FIPS à l'emplacement spécifié. Pendant l'installation, vous indiquez l'emplacement du fichier de clé FIPS au programme d'installation.

Remarque : Assurez-vous de sécuriser la clé en définissant les autorisations d'accès à l'annuaire pour des types de groupe ou d'utilisateur spécifiques, comme l'utilisateur autorisé à exécuter CA Identity Manager.

FIPS

Permet de chiffrer une valeur de texte brut à l'aide d'un fichier de clé FIPS. Ce protocole utilise le fichier de clé FIPS existant.

Exemple :

`pwdtools -FIPS –p firewall -k C:\`*`chemin_accès_clé`*`\FIPSkey.dat`

où *chemin_accès_clé* est le chemin d'accès complet au répertoire de clé FIPS.

Remarque : Utilisez le même fichier de clé FIPS que vous avez spécifié pendant l'installation.

RC2

Permet de chiffrer une valeur de texte brut à l'aide de l'algorithme RC2.

Important : CA Identity Manager utilise le fichier de clé FIPS pour vérifier si l'application doit démarrer en mode FIPS ou en mode non FIPS. Par conséquent, vérifiez que le nom du fichier de clé soit FIPSKey.dat avec le chemin d'accès au déploiement de serveur d'applications suivant :

`iam_im.ear\config\com\netegrity\config\keys\FIPSkey.dat`

iam_im.ear doit se trouver dans le répertoire de déploiement de serveur d'applications, par exemple :

`répertoire_installation_jboss``\server\default\deploy`

Détection du mode FIPS

Pour déterminer si CA Identity Manager fonctionne en mode FIPS ou en mode non FIPS, utilisez la page du statut de l'environnement CA Identity Manager.

Pour accéder à la page de statut, saisissez l'URL suivante dans un navigateur :

`http://nom_serveur/idm/status.jsp`

nom_serveur

Définit le nom de domaine complet du serveur sur lequel CA Identity Manager est installé. Par exemple : myserver.mycompany.com Dans cet exemple, l'URL complète est la suivante :

http://myserver.mycompany.com/idm/status.jsp

Le statut de FIPS est affiché au bas de la page.

Remarque : Vous pouvez également vérifier si CA Identity Manager fonctionne en mode FIPS en recherchant le fichier de clé suivant :

`/config/com/netegrity/config/keys/FIPSkey.dat`

Si ce fichier existe, CA Identity Manager fonctionne en mode FIPS.

Le fichier de clé FIPSkey.dat est créé par l'utilitaire d'outil de modification de mots de passe, pwdtools.bat (ou pwdtools.sh), lors de l'installation de CA Identity Manager.

Formats de texte chiffrés

Le nom d'algorithme est ajouté comme préfixe au texte chiffré et informe CA Identity Manager de l'algorithme utilisé pour le chiffrement.

En mode FIPS, le préfixe est {AES}. Par exemple, si vous chiffrez le texte password, le texte chiffré est similaire à :

{AES}:eolQCTq1CGPyg6qe++0asg==

En mode non FIPS, ou en mode JSAFE, le préfixe (balise d'algorithme) est {PBES} ou {RC2}, selon l'algorithme. Par exemple, si vous chiffrez le texte password, le texte chiffré est similaire à :

{PBES}:gSex2/BhDGzEKWvFmzca4w==

Vous pouvez créer des clés dynamiques à l'aide de la tâche Clés secrètes sous Système. Si vous définissez des clés dynamiques, l'ID de clé est inséré entre une balise d'algorithme et le délimiteur de balise ":". L'absence d'un ID de clé dans les données chiffrées indique qu'une clé codée de manière irréversible a été utilisée pour le chiffrement. Vous pouvez utiliser cette modalité à des fins de rétrocompatibilité ou si aucune clé dynamique n'est définie pour l'algorithme donné.

Informations chiffrées

Les informations CA Identity Manager suivantes sont chiffrées :

- Mots de passe dans la configuration de la source de données pour JBoss
- Informations de récupération de mot de passe oublié
- Secret de rappel du serveur de provisionnement
- Informations sur la session de flux de travaux
- Informations de connexion au serveur de stratégies

Journalisation du mode FIPS

Les composants CA Identity Manager suivants indiquent dans des fichiers journaux si le mode FIPS est activé :

- Serveur CA Identity Manager
- Serveur de provisionnement

- Serveur de connecteurs C++
- Serveur de connecteurs Java
- Gestionnaire de provisionnement
- Agent de synchronisation du mot de passe

Dans tous les cas de figure, l'entrée de journal indiquant que le mode FIPS est activé se termine par la chaîne suivante :

FIPS 140-2 MODE: ON

Annexe B: Remplacement des certificats CA Identity Manager par des certificats SSL signés en SHA-2

Le hachage SHA-2 de certificat SSL est un algorithme cryptographique développé par le National Institute of Standards and Technology (NIST) et la NSA. Les certificats SHA2 sont plus sécurisés que tous les algorithmes existants auparavant. Dans CA Identity Manager, vous pouvez configurer des certificats SSL signés en SHA-2 à la place des certificats signés avec la fonction d'hachage SHA-1.

Remarque : Pour plus d'informations sur la configuration des certificats SSL, consultez le *Manuel d'installation*.

Le tableau suivant répertorie l'emplacement sur le serveur CA Identity Manager dans lequel vous pouvez placer les certificats signés en SHA-2 :

Certificats	Emplacement d'installation	Description
Certificat de serveur de provisionnement	[répertoire_installation_serveur_provisionnement]/data/tls/server/eta2_servercert.pem [répertoire_installation_serveur_provisionnement]/data/tls/server/eta2_serverkey.pem *répertoire_installation_serveur_connecteurs*/ccs/data/tls/server/eta2_servercert.pem *répertoire_installation_serveur_connecteurs*/ccs/data/tls/server/eta2_serverkey.pem *répertoire_installation_serveur_connecteurs*/jcs/conf/eta2_server.p12	Utilisés par le serveur de provisionnement au format .pem et par CA IAM CS au format .p12 (y compris les certificats signés, les clés privées et les certificats d'autorité de certification racine). **Remarque :** Importez le certificat eta2_server.p12 dans *répertoire_installation_serveur_connecteurs*/jcs/conf/ssl.keystore sous l'alias eta2_server et supprimez l'entrée existante. Le mot de passe ssl.keystore est le mot de passe du serveur de connecteurs fourni au cours de l'installation.

Certificats	Emplacement d'installation	Description
Certificat de client de provisionnement	[répertoire_installation_serveur_provisionnement]/data/tls/client/eta2_clientcert.pem [répertoire_installation_serveur_provisionnement]/data/tls/client/eta2_clientkey.pem [répertoire_installation_gestionnaire_provisionnement]/data/tls/client/eta2_clientcert.pem [répertoire_installation_gestionnaire_provisionnement]/data/tls/client/eta2_clientkey.pem *répertoire_installation_serveur_connecteurs*/ccs/data/tls/ client/eta2_clientcert.pem *répertoire_installation_serveur_connecteurs*/ccs/data/tls/ client/eta2_clientkey.pem *répertoire_installation_serveur_connecteurs*/jcs/conf/eta2_client.p12	Utilisés par le serveur de provisionnement au format .pem et par CA IAM CS au format .p12 (y compris les certificats signés, les clés privées et les certificats d'autorité de certification racine).
Certificat d'annuaire de provisionnement approuvé	*répertoire_installation_CA_Directory*/config/ssld/impd_trusted.pem	Utilisé par CA Directory au format .pem. La structure du contenu du certificat doit être la suivante : -----BEGIN CERTIFICATE----- Contenu du certificat -----END CERTIFICATE-----
Certificat de personnalité d'annuaire de provisionnement	*répertoire_installation_CA_Directory*/config/ssld/personalities/impd-co.pem *répertoire_installation_CA_Directory*/config/ssld/personalities/impd-inc.pem *répertoire_installation_CA_Directory*/config/ssld/personalities/impd-main.pem *répertoire_installation_CA_Directory*/config/ssld/personalities/impd-notify.pem *répertoire_installation_CA_Directory*/config/ssld/personalities/impd-router.pem	Utilisé par CA Directory au format .pem.

Certificats	Emplacement d'installation	Description
Certificat d'autorité de certification racine	[répertoire_installation_serveur_provisionnement]/data/tls/et2_cacert.pem [répertoire_installation_gestionnaire_provisionnement]/data/tls/et2_cacert.pem *répertoire_installation_serveur_connecteurs*/ccs/data/tls/ et2_cacert.pem *répertoire_installation_conxp*/lib/jiam.jar [répertoire_installation_serveur_applications]/iam_im.ear/library/jiam.jar	Le certificat est importé dans le référentiel de clés Connector Xpress sous [répertoire_installation_Connector_Xpress]/conf/ssl.keystore. Le certificat doit également être importé dans le référentiel de clés jiam.jar. Pour effectuer l'importation, extrayez le fichier JAR, importez le certificat dans admincacerts.jks et mettez en package le contenu du fichier JAR à nouveau. Le mot de passe de référentiel de clés admincacerts.jks est changeit. Vérifiez que toutes les copies de jiam.jar sont remplacées.

Commandes utiles

Le programme OpenSSL est un outil de ligne de commande permettant d'utiliser les différentes fonctions de cryptographie de la bibliothèque OpenSSL. Cet outil est fourni avec le serveur de provisionnement de CA Identity Manager situé sous [répertoire_installation_serveur_provisionnement]/bin.

Le tableau suivant répertorie plusieurs commandes OpenSSL utiles liées à la gestion des certificats :

Commandes	Description
`openssl x509 –in cert.pem –text –noout`	Imprime le contenu du certificat .pem.
`openssl.exe pkcs12 -in my.pkcs12 –info`	Imprime le contenu du fichier .p12.
`openssl.exe pkcs12 -export -chain –inkey key.pem –in cert.pem -CAfile cacert.pem -out my.p12`	Convertit la paire clé/certificat .pem en .p12.
`keytool –list –v -keystore my.keystore`	Imprime le contenu d'un référentiel de clés Java.
`keytool –list –v –alias myalias –keystore my.keystore`	Imprime le contenu d'un alias dans un référentiel de clés Java.

Commandes		Description
	`keytool –delete –alias myalias –keystore my.keystore`	Supprime un alias d'un référentiel de clés Java.
	`keytool –importkeystore –destkeystore my.keystore –srckeystore src.p12 –srcstoretype PKCS12 –srcalias 1 –destalias myalias`	Importe un fichier .p12 dans un référentiel de clés Java.
	`keytool -import -trustcacerts -alias myrootca -file rootcacert.pem -keystore my.keystore`	Importe un certificat d'autorité de certification racine .pem dans un référentiel de clés Java.