



Informatica® Multidomain MDM  
10.4

# Guide de sécurité

Ce logiciel et la documentation associée sont fournis uniquement sous un accord de licence séparé contenant des restrictions d'utilisation et de divulgation. Il est interdit de reproduire ou de transmettre sous quelle que forme et par quel que moyen que ce soit (électronique, photocopie, enregistrement ou autre) tout ou partie de ce document sans le consentement préalable d'Informatica LLC.

**U.S. GOVERNMENT RIGHTS** Les programmes, les logiciels, les bases de données et les documents connexes et les données techniques fournis aux clients du gouvernement américain sont des « logiciels commerciaux » ou des « données techniques commerciales », conformément au règlement fédéral sur les acquisitions et aux règlements supplémentaires propres à l'Agence. En tant que tel, l'utilisation, la duplication, la divulgation, la modification et l'adaptation sont assujetties aux restrictions et aux conditions de licence énoncées dans le contrat gouvernemental applicable et, dans la mesure applicable par les termes du contrat gouvernemental, les droits additionnels énoncés dans la réglementation FAR 52.227-19, licence de logiciel d'ordinateur commercial.

Informatica et le logo Informatica sont des marques ou des marques déposées d'Informatica LLC aux États-Unis et dans de nombreux autres pays. Une liste actuelle des marques déposées d'Informatica est disponible sur le site <https://www.informatica.com/trademarks.html>. Les autres noms de société ou de produit peuvent être des marques de commerce ou des marques déposées de leurs détenteurs respectifs.

Certaines parties de ce logiciel et/ou de cette documentation sont soumises à des droits d'auteur détenus par des tiers. Les notifications de tiers requises sont incluses avec le produit.

Les renseignements contenus dans cette documentation sont sujets à modification sans préavis. Si vous constatez des problèmes liés à la documentation, merci de les signaler par courriel à l'adresse [infa\\_documentation@Informatica.com](mailto:infa_documentation@Informatica.com).

Les produits Informatica sont garantis conformément aux termes et conditions des accords en vertu desquels ils sont fournis. **INFORMATICA FOURNIT LES INFORMATIONS DE CE DOCUMENT « EN L'ÉTAT » SANS GARANTIE D'AUCUNE SORTE, EXPRESSE OU IMPLICITE, NOTAMMENT AUCUNE GARANTIE DE QUALITÉ MARCHANDE, D'ADAPTATION À UN USAGE PARTICULIER ET D'ABSENCE DE CONTREFAÇON**

Date de publication: 2020-06-05

# Sommaire

<b>Préface.....</b>	<b>7</b>
Ressources Informatica. . . . .	7
Informatica Network. . . . .	7
Base de connaissances Informatica. . . . .	7
Documentation Informatica. . . . .	8
Matrices de disponibilité des produits Informatica. . . . .	8
Informatica Velocity. . . . .	8
Informatica Marketplace. . . . .	8
Support client international Informatica. . . . .	8
 <b>Chapitre 1: Introduction à la sécurité de MDM Hub.....</b>	 <b>9</b>
Présentation de la sécurité de MDM Hub . . . . .	9
Console MDM Hub. . . . .	10
Dynamic Data Masking . . . . .	10
Gestionnaire d'accès de sécurité . . . . .	11
Authentification. . . . .	11
Autorisation. . . . .	12
Ressources sécurisées et privilèges. . . . .	12
Rôles. . . . .	13
Scénarios d'implémentation de la sécurité. . . . .	13
Point de décision stratégique interne. . . . .	14
Répertoire utilisateur externe. . . . .	14
Décision stratégique centralisée basée sur les rôles. . . . .	15
Décision stratégique centralisée complète. . . . .	15
Tâches de configuration pour les scénarios de sécurité. . . . .	16
 <b>Chapitre 2: Ressources.....</b>	 <b>17</b>
Présentation des ressources. . . . .	17
Ressources sécurisées et privées . . . . .	18
Groupes de ressources. . . . .	18
Hiérarchies des groupes de ressources. . . . .	19
Ressources sécurisées. . . . .	19
Outil Ressources sécurisées. . . . .	19
Configuration des ressources sécurisées. . . . .	19
Définition du statut d'une ressource MDM Hub. . . . .	20
Filtrage de ressources. . . . .	20
Configuration des groupes de ressources. . . . .	20
Ajout de groupes de ressources. . . . .	21
Modification et suppression de groupes de ressources. . . . .	21
Actualisation de la liste de ressources. . . . .	22

Actualisation d'autres modifications de sécurité. . . . .	22
Configuration de la sécurité pour les services d'entité d'entreprise de Data Director. . . . .	22
Configuration des services d'entité d'entreprise en tant que ressource sécurisée. . . . .	22
Attribution des privilèges de rôle aux services d'entité d'entreprise. . . . .	23

## **Chapitre 3: Rôles..... 24**

Présentation des rôles. . . . .	24
Configuration de rôle. . . . .	25
Ajout de rôles. . . . .	25
Modification et suppression de rôles. . . . .	25
Privilèges. . . . .	25
Rôles internes et rôles externes. . . . .	26
Attribution de privilèges de ressource aux rôles. . . . .	27
Attribution de rôles à d'autres rôles. . . . .	27
Génération d'un rapport de privilèges de ressources pour les rôles. . . . .	27
Enregistrement du rapport généré au format HTML. . . . .	28

## **Chapitre 4: Utilisateurs et groupes d'utilisateurs..... 29**

Présentation des utilisateurs et des groupes d'utilisateurs. . . . .	29
Configuration utilisateur. . . . .	29
Accès des utilisateurs aux ressources de MDM Hub. . . . .	30
Ajout de comptes utilisateur. . . . .	30
Modification et suppression de comptes utilisateur. . . . .	31
Modification d'informations utilisateur supplémentaires. . . . .	31
Modification des paramètres de mot de passe pour les comptes utilisateur. . . . .	32
Configuration de l'accès des utilisateurs au stockage de référence opérationnelle (Operational Reference Store - ORS). . . . .	32
Configuration de la stratégie des mots de passe. . . . .	33
Paramètres de la stratégie des mots de passe. . . . .	33
Gestion de la stratégie globale des mots de passe. . . . .	34
Gestion des stratégies de mots de passe personnels. . . . .	34
Configuration de la sécurité des sources de données JDBC. . . . .	34
Noms d'utilisateur et mots de passe pour une source de données JDBC sécurisée. . . . .	35
Identifiant de base de données pour les types de connexion SID Oracle. . . . .	35
Identifiant de base de données pour les types de connexion au service Oracle. . . . .	35
ID de base de données pour les types de connexion IBM Db2. . . . .	35
Identifiant de base de données pour les types de connexion Microsoft SQL Server. . . . .	36
Identifiant de base de données pour la base de données principale. . . . .	36
Chiffage du mot de passe. . . . .	36
Configuration du groupe d'utilisateurs. . . . .	36
Démarrage de l'outil Utilisateurs et groupes. . . . .	37
Ajout de groupes d'utilisateurs. . . . .	37
Modification et suppression de groupes d'utilisateurs. . . . .	37

Attribution d'utilisateurs et de groupes d'utilisateurs à des groupes d'utilisateurs. . . . .	38
Attribution d'utilisateurs à la base de données ORS actuelle. . . . .	38
Associations entre les rôles et les utilisateurs et groupes d'utilisateurs. . . . .	39
Attribution d'utilisateurs et de groupes d'utilisateurs à des rôles. . . . .	39
Attribution de rôles à des utilisateurs et des groupes d'utilisateurs. . . . .	39
<b>Chapitre 5: Fournisseurs de sécurité.....</b>	<b>40</b>
Présentation des fournisseurs de sécurité. . . . .	40
Gestion des fournisseurs de sécurité. . . . .	40
Gestion du fichier de fournisseur. . . . .	41
Téléchargement d'un fichier de fournisseur. . . . .	42
Suppression d'un fichier de fournisseur. . . . .	42
Paramètres du fournisseur de sécurité. . . . .	42
Modification des paramètres des fournisseurs de sécurité. . . . .	43
Activation et désactivation des fournisseurs de sécurité. . . . .	43
Déplacement d'un fournisseur de sécurité dans l'ordre de traitement. . . . .	43
Propriétés du fournisseur. . . . .	43
Ajout de propriétés de fournisseur. . . . .	44
Modification des propriétés de fournisseur. . . . .	44
Fournisseurs personnalisés. . . . .	45
Exemple de fichier providers.properties. . . . .	45
Authentification externe. . . . .	46
Ajout d'un module de connexion. . . . .	46
Suppression d'un module de connexion. . . . .	47
<b>Chapitre 6: Niveau de sécurité de l'application.....</b>	<b>48</b>
Présentation de la sécurité au niveau de l'application. . . . .	48
Informatica Data Director. . . . .	49
Outil d'approvisionnement. . . . .	50
ActiveVOS. . . . .	50
Dynamic Data Masking. . . . .	51
Intégration de Dynamic Data Masking à MDM Hub. . . . .	51
Bonnes pratiques recommandées de Dynamic Data Masking pour MDM Hub. . . . .	52
Configuration de Dynamic Data Masking pour un stockage de référence opérationnelle (Operational Reference Store - ORS). . . . .	53
Configuration d'un canal WebLogic T3S sous Linux. . . . .	53
<b>Chapitre 7: Authentification basée sur un certificat.....</b>	<b>55</b>
Authentification basée sur un certificat Présentation. . . . .	55
Authentification basée sur un certificat et clients externes. . . . .	56
Applications approuvées. . . . .	56
Ajout d'une application externe en tant qu'application approuvée. . . . .	56
Gestion des certificats et des clés . . . . .	57

Utilitaire de configuration de la sécurité. . . . .	57
<b>Chapitre 8: Hachage de mot de passe.....</b>	<b>58</b>
Présentation du hachage de mot de passe. . . . .	58
Options de hachage de mot de passe. . . . .	59
Algorithme de hachage personnalisé . . . . .	59
Processus de réinitialisation de mot de passe . . . . .	59
Utilitaire de configuration de la sécurité. . . . .	60
Dépannage. . . . .	60
<b>Annexe A: Glossaire.....</b>	<b>61</b>
<b>Index. . . . .</b>	<b>66</b>

# Préface

Utilisez le Informatica® *Guide de sécurité de MDM Multidomain* pour apprendre à activer la sécurité dans MDM Multidomain. Comprenez comment utiliser le Gestionnaire d'accès de sécurité pour sécuriser les ressources de MDM Hub et utiliser Dynamic Data Masking pour empêcher l'accès aux données sensibles. Apprenez à gérer les utilisateurs et les groupes et à utiliser des autorisations, des privilèges et des rôles pour gérer la sécurité de l'utilisateur.

Ce guide suppose que vous avez une connaissance des systèmes d'exploitation, des environnements de base de données et de votre serveur d'application.

## Ressources Informatica

Informatica vous fournit toute une gamme de ressources de produits via Informatica Network et autres portails en ligne. Utilisez ces ressources pour tirer le meilleur parti de vos produits et solutions Informatica, et pour apprendre d'autres utilisateurs et experts en la matière d'Informatica.

### Informatica Network

Informatica Network est la passerelle à de nombreuses ressources, y compris la base de connaissances Informatica et le support client international Informatica. Pour accéder à Informatica Network, visitez le site <https://network.informatica.com>.

En tant que membre d'Informatica Network, vous disposez des options suivantes :

- Rechercher les ressources de produits dans la base de connaissances.
- Afficher les informations de disponibilité des produits.
- Créer et vérifier vos dossiers de support.
- Rechercher votre réseau de groupe d'utilisateurs local Informatica et collaborer avec vos pairs.

### Base de connaissances Informatica

Utilisez la base de connaissances Informatica pour rechercher des ressources de produits telles que des articles pratiques, des meilleures pratiques, des didacticiels vidéo et des questions fréquemment posées.

Pour rechercher dans la base de connaissances, visitez le site <https://search.informatica.com>. N'hésitez pas à contacter l'équipe Base de connaissances Informatica à l'adresse [KB\\_Feedback@informatica.com](mailto:KB_Feedback@informatica.com) pour lui faire part de vos questions, commentaires ou suggestions concernant la base de connaissances.

## Documentation Informatica

Utilisez le portail de documentation Informatica pour explorer une vaste bibliothèque de documentation pour les versions de produits actuelles et récentes. Pour explorer le portail de documentation, visitez le site <https://docs.informatica.com>.

N'hésitez pas à contacter l'équipe Documentation Informatica à l'adresse [infa\\_documentation@informatica.com](mailto:infa_documentation@informatica.com) pour lui faire part de vos questions, commentaires ou suggestions concernant la documentation des produits.

## Matrices de disponibilité des produits Informatica

Les matrices de disponibilité des produits (PAM) indiquent les versions des systèmes d'exploitation, les bases de données et les types de source et cible de données pris en charge par une version d'un produit. Vous pouvez parcourir les PAM Informatica à l'adresse <https://network.informatica.com/community/informatica-network/product-availability-matrices>.

## Informatica Velocity

Informatica Velocity est un ensemble de conseils et de meilleures pratiques développés par les services professionnels d'Informatica et basés sur les expériences réelles de centaines de projets de gestion des données. Informatica Velocity représente le savoir collectif de consultants d'Informatica qui collaborent avec des organisations du monde entier pour planifier, développer, déployer et gérer des solutions performantes de gestion des données.

Vous trouverez les ressources d'Informatica Velocity à l'adresse <http://velocity.informatica.com>. Si vous avez des questions, des commentaires ou des suggestions sur Informatica Velocity, contactez les services professionnels d'Informatica à l'adresse [ips@informatica.com](mailto:ips@informatica.com).

## Informatica Marketplace

Informatica Marketplace est un forum dans lequel vous pouvez trouver des solutions qui permettent d'augmenter et d'améliorer vos implémentations Informatica. Exploitez les centaines de solutions de développeurs et de partenaires Informatica sur Marketplace pour améliorer votre productivité et accélérer le délai d'implémentation de vos projets. Vous trouverez Informatica Marketplace à l'adresse <https://marketplace.informatica.com>.

## Support client international Informatica

Vous pouvez contacter un centre de support international par téléphone ou via Informatica Network.

Pour rechercher le numéro de téléphone du support client international Informatica local, visitez le site Web Informatica à l'adresse <https://www.informatica.com/services-and-training/customer-success-services/contact-us.html>.

Pour rechercher des ressources de support en ligne sur Informatica Network, visitez le site <https://network.informatica.com> et sélectionnez l'option eSupport.



# CHAPITRE 1

## Introduction à la sécurité de MDM Hub

Ce chapitre comprend les rubriques suivantes :

- [Présentation de la sécurité de MDM Hub , 9](#)
- [Console MDM Hub, 10](#)
- [Dynamic Data Masking , 10](#)
- [Gestionnaire d'accès de sécurité , 11](#)
- [Authentification, 11](#)
- [Autorisation, 12](#)
- [Ressources sécurisées et privilèges, 12](#)
- [Rôles, 13](#)
- [Scénarios d'implémentation de la sécurité, 13](#)

## Présentation de la sécurité de MDM Hub

MDM Hub protège les données contre tout accès non autorisé et contre toute falsification, afin de garantir la confidentialité des informations et l'intégrité des données.

Vous pouvez utiliser le Gestionnaire d'accès de sécurité dans la Console Hub afin de sécuriser les ressources de MDM Hub et d'appliquer des stratégies de sécurité opérationnelles, telles que l'authentification utilisateur et l'autorisation.

Vous pouvez utiliser Dynamic Data Masking pour interdire l'accès aux données sensibles. Par exemple, vous pouvez utiliser Dynamic Data Masking pour dissimuler des numéros de carte de crédit à tous les utilisateurs qui ne disposent pas de droits d'administrateur.

Vous pouvez configurer la sécurité dans les implémentations de MDM Hub de plusieurs manières. Vous pouvez utiliser des fournisseurs de sécurité tiers pour gérer des éléments spécifiques de la sécurité de votre organisation. Vous pouvez également configurer MDM Hub de sorte qu'il gère tous les aspects de la sécurité. Pour plus d'informations sur l'utilisation du Services Integration Framework (SIF) pour configurer la sécurité, consultez le *Guide de l'infrastructure d'intégration des services de MDM Multidomain*.

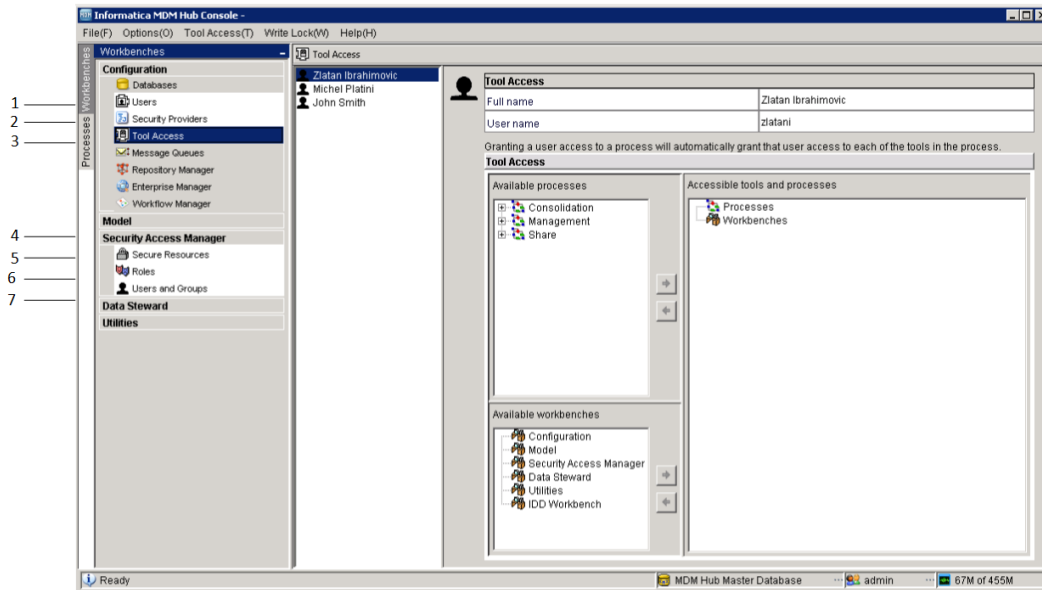
**Important:** Avant de commencer à sécuriser MDM Multidomaine, assurez-vous que le serveur d'applications et les périphériques de mise en cache sont sécurisés.

# Console MDM Hub

Utilisez la Console Hub pour configurer la sécurité dans MDM Hub.

Vous pouvez utiliser l'outil Accès aux outils dans l'espace de travail de configuration pour contrôler les privilèges d'accès aux outils de la Console Hub. Par exemple, vous pouvez utiliser l'outil Accès aux outils pour refuser l'accès des gestionnaires de données à tous les outils de la Console Hub, à l'exception des outils Gestionnaire de données et Gestionnaire de fusions.

La figure suivante représente l'interface de la Console Hub :



1. Outil Utilisateurs
2. Outil Fournisseurs de sécurité
3. Outil Accès aux outils
4. Gestionnaire d'accès de sécurité
5. Outil Ressources sécurisées
6. Outil Rôles
7. Outil Utilisateurs et groupes

## Dynamic Data Masking

Informatica Dynamic Data Masking est un produit visant à assurer la sécurité des données, qui s'exécute entre un client et une base de données pour éviter tout accès non autorisé à des informations sensibles. Dynamic Data Masking intercepte les demandes envoyées à la base de données et applique des règles de masquage aux demandes afin de masquer les données avant qu'elles ne soient renvoyées au client.

Vous pouvez utiliser Dynamic Data Masking pour interdire l'accès à des données sensibles stockées dans des bases de données de production et de non-production gérées par MDM Hub ou pour les masquer. Vous définissez la connexion de règles pour identifier les demandes entrantes et les règles de sécurité pour définir la manière dont vous voulez masquer les données. Dynamic Data Masking surveille les demandes de la base

de données entrantes provenant de MDM Hub et les modifie avant qu'elles ne soient envoyées à la base de données. La base de données traite la demande modifiée et renvoie les résultats masqués à Dynamic Data Masking. Dynamic Data Masking envoie ensuite les résultats à MDM Hub.

Vous pouvez utiliser Dynamic Data Masking afin de masquer des données pour des types spécifiques de demandes à la base de données. Vous pouvez également restreindre l'accès aux données à certains groupes au sein d'une organisation. Par exemple, vous pouvez créer une règle permettant de masquer les numéros de carte de crédit lorsque la demande à la base de données provient d'un membre de l'équipe d'assistance. Lorsque Dynamic Data Masking renvoie les données à MDM Hub, le membre de l'équipe d'assistance voit des chiffres masqués à la place des numéros de carte de crédit.

**Remarque:** Pour utiliser Dynamic Data Masking dans MDM Hub, vous devez avoir installé Dynamic Data Masking 9.6.0 ainsi que le correcteur de bogues en urgence 14590. Les versions antérieures de Dynamic Data Masking ne sont pas compatibles avec MDM Hub.

Pour plus d'informations sur Dynamic Data Masking, consultez la documentation Dynamic Data Masking.

## Gestionnaire d'accès de sécurité

Le Gestionnaire d'accès de sécurité est le module de sécurité de MDM Hub. Le Gestionnaire d'accès de sécurité protège les ressources de MDM Hub contre tout accès non autorisé.

Le Gestionnaire d'accès de sécurité applique les stratégies de sécurité de votre organisation dans votre implémentation de MDM Hub. Le Gestionnaire d'accès de sécurité gère l'authentification utilisateur et l'autorisation conformément à votre configuration de sécurité.

**Remarque:** Vous pouvez utiliser le Gestionnaire d'accès de sécurité pour configurer l'accès utilisateur aux ressources de MDM Hub depuis des applications tierces. Cependant, vous ne pouvez pas configurer la sécurité pour les outils et les ressources de la Console Hub via le Gestionnaire d'accès de sécurité. Console Hub authentifie les utilisateurs et autorise l'accès utilisateur aux outils et ressources de Console Hub via un mécanisme de sécurité distinct.

## Authentification

L'authentification est le processus de vérification de l'identité d'un utilisateur.

MDM Hub authentifie les utilisateurs en fonction de leurs justificatifs d'identité (nom d'utilisateur et mot de passe) ou selon les données binaires brutes dans une charge de sécurité.

MDM Hub utilise les types d'authentification suivants :

### Interne

Authentifie les utilisateurs dans MDM Hub, où l'utilisateur se connecte avec un nom d'utilisateur et un mot de passe.

### Répertoire externe

Authentifie les utilisateurs via un répertoire utilisateur externe, avec un support natif de serveurs de répertoire LDAP activé, Microsoft Active Directory et Kerberos.

### Fournisseurs d'authentification externe

Authentifie les utilisateurs via des fournisseurs d'authentification tiers.

Les implémentations de MDM Hub peuvent utiliser chaque type d'authentification seul ou une combinaison de ces méthodes. Le type d'authentification que vous utilisez dépend de la manière dont vous configurez la sécurité.

## Autorisation

L'autorisation est le processus qui détermine si un utilisateur dispose des privilèges suffisants pour accéder à une ressource demandée de MDM Hub.

Vous pouvez utiliser l'autorisation interne et externe dans MDM Hub :

### **Interne**

Autorise via MDM Hub. MDM Hub détermine si vous pouvez accéder aux ressources sécurisées en examinant les privilèges associés aux rôles assignés à votre compte utilisateur.

### **Externe**

Autorise via des fournisseurs d'autorisations tiers.

Vous pouvez configurer MDM Hub afin qu'il utilise un type d'autorisation spécifique ou bien les deux types d'autorisation.

## Ressources sécurisées et privilèges

Vous pouvez configurer plusieurs ressources de MDM Hub comme des ressources sécurisées.

Vous pouvez configurer les ressources suivantes :

- Objets de base
- Mappages
- Packages
- Fonctions de nettoyage
- Ensembles de règles de correspondance
- Métadonnées
- Profils
- Utilisateurs de table

Vous pouvez attribuer l'accès aux ressources de MDM Hub en fonction des privilèges des utilisateurs. MDM Hub peut attribuer les privilèges suivants :

- Lire
- Créer
- Mettre à jour
- Fusionner
- Exécuter
- Supprimer

Les ressources peuvent être privées ou sécurisées. Par défaut, les ressources sont sécurisées. MDM Hub peut attribuer des privilèges uniquement aux ressources sécurisées.

Prenez en compte les éléments suivants lorsque vous configurez la sécurité dans MDM Hub :

- Une ressource spécifique est configurée pour être sécurisée.
- Un rôle spécifique est configuré pour pouvoir accéder à une ou plusieurs ressources sécurisées.
- Chaque ressource sécurisée peut être configurée avec des privilèges spécifiques, tels que l'écriture ou la lecture, qui définissent l'accès pour ce rôle aux ressources sécurisées.

Pour exécuter une demande du Services Integration Framework, l'utilisateur connecté doit disposer d'un rôle doté des privilèges obligatoires pour accéder aux ressources concernées par la demande.

## Rôles

Un rôle représente un ensemble de privilèges permettant d'accéder à des ressources sécurisées de MDM Hub. Vous attribuez un rôle à un utilisateur pour lui permettre d'obtenir des privilèges.

Vous pouvez utiliser l'outil Rôles dans l'espace de travail Gestionnaire d'accès de sécurité afin d'assigner des rôles à des utilisateurs et à des groupes d'utilisateurs. Les rôles assignés à un utilisateur ou à un groupe d'utilisateurs déterminent les privilèges de ressources d'un utilisateur ou d'un groupe d'utilisateurs. Vous ne pouvez pas attribuer de privilèges directement aux utilisateurs.

Le Gestionnaire d'accès de sécurité applique l'autorisation de ressources pour les demandes provenant d'utilisateurs d'applications externes. Les administrateurs et les gestionnaires des données qui utilisent la Console Hub pour accéder aux ressources de MDM Hub ne sont pas affectés par les privilèges de ressource dans la même mesure.

## Scénarios d'implémentation de la sécurité

Vous pouvez configurer la sécurité dans les implémentations de MDM Hub de plusieurs manières.

Un point de décision stratégique est un point de contrôle de sécurité spécifique qui détermine l'identité des utilisateurs lors de l'exécution. C'est ce qu'on appelle l'authentification. Un point de décision stratégique indique également à quelles ressources de MDM Hub les utilisateurs peuvent accéder. C'est ce qu'on appelle l'autorisation. Le niveau de gestion interne des points de décision stratégique par MDM Hub dépend de l'implémentation de MDM Hub. Il en va de même pour le niveau de gestion externe effectuée par des fournisseurs de sécurité tiers ou d'autres services de sécurité.

Les scénarios suivants sont des exemples de méthodes avancées que vous pouvez suivre pour configurer la sécurité dans les implémentations de MDM Hub :

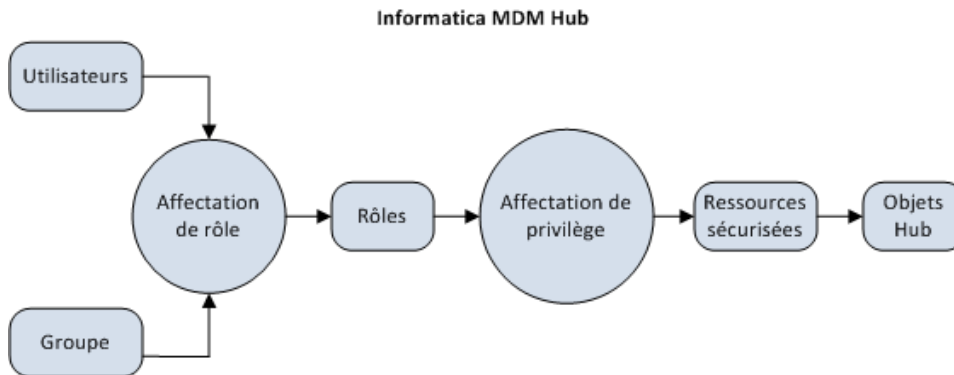
- Points de décision stratégique interne uniquement
- Répertoire utilisateur externe
- Points de décision stratégique centralisés basés sur les rôles
- Points de décision stratégique centralisés complets

**Remarque:** MDM Hub ne reflète pas les modifications apportées aux privilèges de ressource depuis un fournisseur de sécurité externe. Si vous modifiez des privilèges de ressource à l'aide d'un fournisseur de sécurité externe, utilisez d'autres méthodes pour synchroniser ces modifications avec MDM Hub.

## Point de décision stratégique interne

MDM Hub peut traiter toutes les décisions stratégiques en interne.

La figure suivante représente un déploiement de sécurité dans lequel MDM Hub gère toutes les décisions stratégiques en interne :



Dans ce scénario, MDM Hub prend toutes les décisions stratégiques en se basant sur la façon dont les utilisateurs, les groupes, les rôles, les privilèges et les ressources sont configurés à l'aide de la Console Hub.

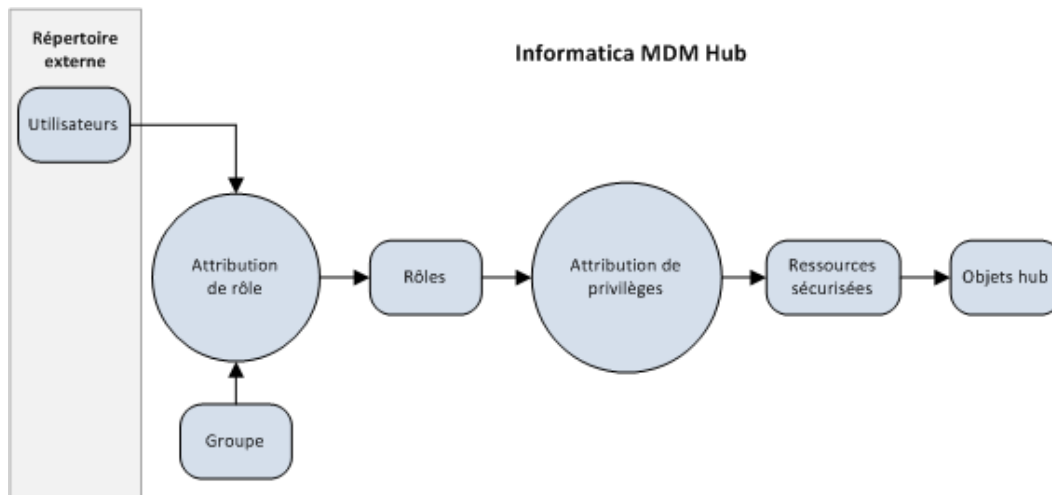
## Répertoire utilisateur externe

MDM Hub peut s'intégrer à un répertoire utilisateur externe.

Les utilisateurs ou groupes d'utilisateurs qui sont conservés dans le répertoire utilisateur externe doivent tout de même être enregistrés dans MDM Hub. L'enregistrement est obligatoire pour que MDM Hub puisse attribuer des rôles et leurs privilèges associés à ces utilisateurs et groupes.

Attribuez des utilisateurs depuis le répertoire externe à des groupes dans MDM Hub. Vous devez conserver les relations entre les utilisateurs et les groupes dans MDM Hub, même si vous conservez également les relations via le protocole LDAP (Lightweight Directory Access Protocol).

La figure suivante représente un déploiement de sécurité dans lequel les utilisateurs sont gérés dans un répertoire externe, tandis que les groupes, l'attribution des rôles et l'attribution des privilèges sont gérés dans MDM Hub.

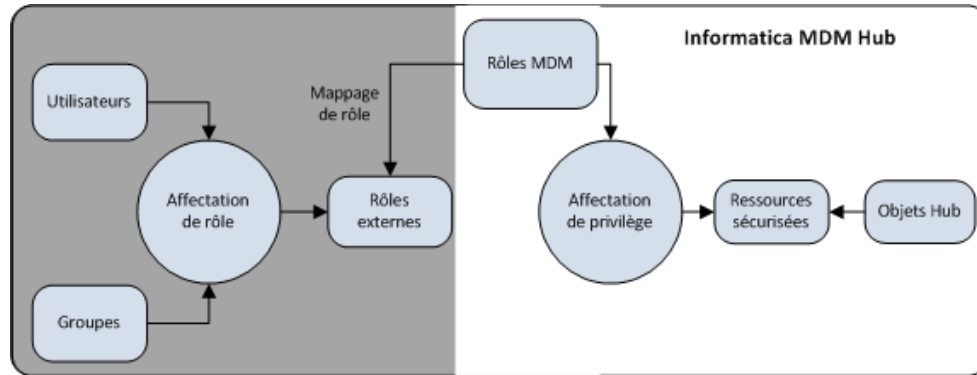


Dans ce scénario, le répertoire utilisateur externe gère les comptes utilisateurs, groupes et profils d'utilisateurs. Le répertoire utilisateur externe peut authentifier les utilisateurs et fournit à MDM Hub des informations sur l'appartenance au groupe et sur les profils utilisateur.

## Décision stratégique centralisée basée sur les rôles

MDM Hub peut gérer des décisions stratégiques en interne et recevoir des attributions de rôle externe.

La figure suivante représente un déploiement de sécurité dans lequel l'attribution de rôle, en plus des comptes utilisateur, groupes et profils utilisateur, est gérée de façon externe à MDM Hub.

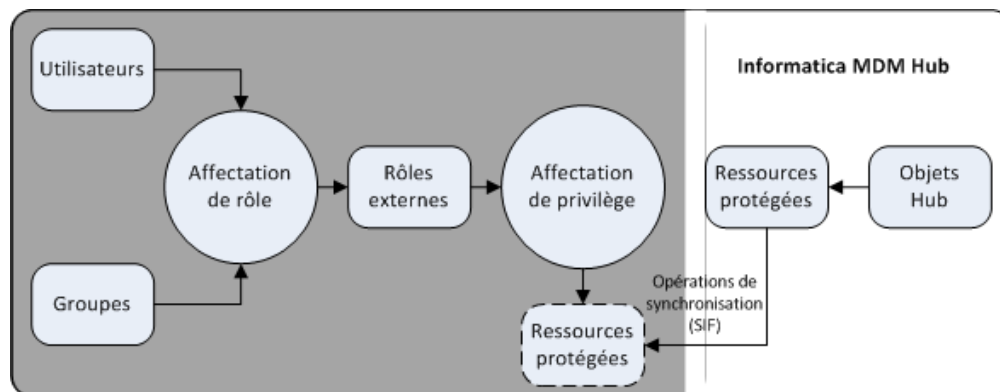


Dans ce scénario, les rôles externes sont explicitement mappés aux rôles de MDM Hub.

## Décision stratégique centralisée complète

MDM Hub peut contrôler les ressources protégées en interne, mais accepter les rôles et privilèges attribués depuis un répertoire externe.

La figure suivante représente un déploiement de sécurité dans lequel la définition des rôles et l'attribution de privilèges sont effectuées de façon externe à MDM Hub. La figure montre également que les comptes utilisateur, les groupes, les profils utilisateur et l'attribution des rôles sont effectués de façon externe à MDM Hub :



Dans ce scénario, MDM Hub présente simplement les ressources protégées à l'aide de proxys externes, synchronisés avec les ressources protégées en interne à l'aide de demandes du Services Integration Framework. Toutes les décisions stratégiques sont externes à MDM Hub.

## Tâches de configuration pour les scénarios de sécurité

Le tableau suivant indique les tâches de configuration de la sécurité s'appliquant à chacun des scénarios d'implémentation de la sécurité. Si une cellule contient « Oui », la tâche associée se produit dans MDM Hub. Si une cellule contient un « Non », la tâche associée se produit de façon externe à MDM Hub.

Service/Tâche	Points de décision stratégique en interne	Répertoire utilisateur externe	Points de décision stratégique centralisés RoleNobased	Points de décision stratégique centralisés complets
Configuration des utilisateurs de MDM Hub.	Oui	Oui	Non	Non
Utilisation de l'authentification externe	Non	Oui	Non	Non
Affectation d'utilisateurs à la base de données actuelle du Stockage de référence opérationnelle	Oui	Oui	Non	Non
Gestion de la stratégie globale des mots de passe	Oui	Non	Non	Non
Configuration des groupes d'utilisateurs	Oui	Oui	Non	Non
Ressources de MDM Hub sécurisées	Oui	Oui	Oui	Oui
Définition du statut d'une ressource MDM Hub	Oui	Oui	Oui	Oui
Configuration des rôles	Oui	Oui	Oui	Non
Mappage des rôles internes aux rôles externes	Non	Non	Oui	Non
Attribution des privilèges de ressource aux rôles	Oui	Oui	Oui	Non
Gestion des fournisseurs de sécurité	Non	Oui	Oui	Oui
Attribution des rôles aux utilisateurs et aux groupes d'utilisateurs	Oui	Oui	Non	Non

**Remarque:** Si vous utilisez des fournisseurs de sécurité tiers pour prendre en charge tout élément de sécurité dans votre implémentation de MDM Hub, consultez les instructions de configuration de votre fournisseur de sécurité.



## CHAPITRE 2

# Ressources

Ce chapitre comprend les rubriques suivantes :

- [Présentation des ressources, 17](#)
- [Ressources sécurisées et privées , 18](#)
- [Groupes de ressources, 18](#)
- [Outil Ressources sécurisées, 19](#)
- [Configuration des ressources sécurisées, 19](#)
- [Configuration des groupes de ressources, 20](#)
- [Configuration de la sécurité pour les services d'entité d'entreprise de Data Director, 22](#)

## Présentation des ressources

La Console Hub vous permet d'exposer ou de masquer les ressources MDM Hub auprès des applications externes.

Une ressource sécurisée est une ressource MDM Hub protégée et exposée à l'outil Rôles, ce qui permet de l'ajouter à des rôles disposant de privilèges spécifiques. Un groupe de ressources est un ensemble de ressources sécurisées qui simplifie l'attribution de privilèges. Vous pouvez utiliser l'outil Ressources sécurisées pour définir des groupes de ressources et créer une hiérarchie des ressources.

Vous pouvez configurer les ressources MDM Hub suivantes comme ressources sécurisées :

### **Objet de base**

L'utilisateur a accès à tous les objets de base, colonnes et métadonnées de contenu sécurisés.

### **Fonction de nettoyage**

L'utilisateur peut exécuter toutes les fonctions de nettoyage sécurisées.

### **Profil du gestionnaire de hiérarchies**

L'utilisateur a accès à tous les profils sécurisés du Gestionnaire de hiérarchies.

### **Services d'entité d'entreprise**

L'utilisateur a accès à tous les services d'entité d'entreprise sécurisés.

### **Mappage**

L'utilisateur a accès à tous les mappages sécurisés et à leurs colonnes.

### **Package**

L'utilisateur a accès à tous les packages sécurisés et à leurs colonnes.

### Package distant

L'utilisateur a accès à tous les packages distants sécurisés.

Les groupes de lots sont sécurisés par défaut. Vous ne pouvez pas définir le statut des groupes de lots sur Privé. Le groupe de lots dispose de privilèges de lecture et d'exécution.

En outre, vous pouvez utiliser la Console Hub pour protéger les autres ressources accessibles via des demandes SIF, y compris les métadonnées, les ensembles de règles de correspondance, la table d'audit et la table d'utilisateurs.

**Remarque:** Si vous utilisez Informatica Data Director, vous pouvez utiliser les méthodes HTTP GET ou POST pour accéder au serveur Hub. Les autres méthodes HTTP, comme DELETE ou PUT, renvoient une erreur HTTP.

## Ressources sécurisées et privées

Vous pouvez configurer une ressource MDM Hub protégée comme étant sécurisée ou privée.

### Sécurisée

Expose cette ressource MDM Hub à l'outil Rôles, permettant ainsi de l'ajouter à des rôles disposant de privilèges spécifiques. Lorsque vous attribuez un rôle spécifique à un utilisateur, celui-ci peut alors utiliser les demandes SIF pour accéder aux ressources sécurisées, selon les privilèges associés à ce rôle. Par défaut, MDM Hub désigne une nouvelle ressource, telle qu'un objet de base, comme étant sécurisée.

### Privée

Masque la ressource MDM Hub auprès de l'outil Rôles. Empêche l'accès à la ressource depuis des demandes SIF.

Une ressource doit être sécurisée pour que les applications externes puissent utiliser les demandes SIF+ pour accéder à une ressource MDM Hub.

Vous souhaitez peut-être que certaines ressources MDM Hub ne soient pas présentées aux applications externes. Par exemple, votre implémentation de MDM Hub peut posséder des mappages ou des packages utilisés uniquement dans les tâches de lots (et non dans les demandes SIF), et qui peuvent donc rester privés.

**Remarque:** MDM Hub ne considère pas les colonnes de package comme des ressources sécurisées. Les colonnes du package héritent du statut sécurisé et des privilèges des colonnes de l'objet de base parent. Si les colonnes de package sont basées sur les colonnes de la table système, vous n'avez pas besoin de configurer leur sécurité, car celles-ci sont accessibles par défaut.

## Groupes de ressources

Un groupe de ressources est un ensemble logique de ressources sécurisées.

Vous pouvez utiliser l'outil Ressources sécurisées pour définir des groupes de ressources et leur attribuer des ressources connexes. Les groupes de ressources simplifient l'attribution de privilèges, ce qui vous permet d'attribuer des privilèges à plusieurs ressources et des groupes de ressources à un rôle.

Pour simplifier l'administration, envisagez la création des types de groupes de ressources suivants :

- Définissez un groupe de ressource ALL\_RESOURCES qui contient toutes les ressources sûres, ce qui vous permet de définir les privilèges minimum de façon globale.
- Définissez les groupes de ressources par type de ressource, de sorte que vous puissiez définir les privilèges minimum pour ces types de ressources.
- Définissez les groupes de ressources par zone fonctionnelle, telle que TRAINING\_RESOURCES.
- Définissez un groupe de ressources fourre-tout que vous pourrez attribuer à plusieurs rôles différents disposant de privilèges similaires.

## Hiérarchies des groupes de ressources

Un groupe de ressources peut également contenir d'autres groupes de ressources, sauf un groupe auquel il appartient. Cela signifie que vous pouvez créer une hiérarchie de groupes de ressources afin de simplifier la gestion d'un ensemble important de ressources.

## Ressources sécurisées

Seules les ressources sécurisées peuvent appartenir à des groupes de ressources. Les ressources privées ne peuvent pas appartenir à des groupes de ressources.

Si vous modifiez le statut d'une ressource de sorte qu'elle devienne privée, MDM Hub la supprime automatiquement des groupes de ressources auxquels elle appartient. Lorsque vous définissez une ressource comme étant sécurisée, MDM Hub ajoute la ressource au groupe de ressources approprié.

## Outil Ressources sécurisées

Utilisez l'outil Ressources sécurisées dans la Console Hub pour gérer en détail la sécurité des ressources de MDM Hub, y compris pour définir une ressource MDM Hub comme étant sécurisée ou privée. Vous pouvez également utiliser les groupes de ressources pour configurer une hiérarchie de ressources.

L'outil Ressources sécurisées comporte les onglets suivants :

### **Ressources**

Permet de définir chaque ressource MDM Hub comme étant sécurisée ou privée. MDM Hub affiche les ressources sous la forme d'une hiérarchie indiquant les relations entre les ressources. Les ressources globales figurent en haut de la hiérarchie.

### **Groupes de ressources**

Permet de configurer des groupes de ressources.

Vous pouvez utiliser l'outil Ressources sécurisées pour exposer ou masquer des ressources dans l'outil Rôles et les demandes SIF. Vous devez vous connecter à un Stockage de référence opérationnelle avant d'utiliser l'outil.

## Configuration des ressources sécurisées

Pour accéder aux ressources de MDM Hub et les configurer, utilisez l'onglet Ressources dans l'outil Ressources sécurisées.

## Définition du statut d'une ressource MDM Hub

Toutes les ressources MDM Hub peuvent être configurées comme étant sécurisées ou privées.

**Remarque:** Ce statut ne s'applique pas aux groupes de ressources, qui contiennent uniquement des ressources sécurisées, ni aux ressources globales.

1. Démarrez l'outil Ressources sécurisées.
2. Obtenez un verrou en écriture.
3. Dans l'onglet Ressources, accédez à l'arborescence Ressources pour trouver celles que vous voulez configurer.
4. Double-cliquez sur le nom de la ressource pour basculer entre les statuts sécurisé et privé. Pour modifier le statut de plusieurs ressources en même temps, effectuez les étapes 5 et 6.
5. Sélectionnez les ressources qui nécessitent un changement de statut. Vous pouvez sélectionner plusieurs ressources si vous le souhaitez.
6. Mettez à jour le statut des ressources que vous avez sélectionnées :
  - Cliquez sur le bouton **Sécurisé** pour associer les ressources sélectionnées au statut sécurisé.
  - Cliquez sur le bouton **Privé** pour associer les ressources sélectionnées au statut privé.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

## Filtrage de ressources

Pour simplifier la modification du statut d'un ensemble de ressources MDM Hub, vous pouvez spécifier un filtre permettant d'afficher uniquement les ressources que vous souhaitez modifier.

1. Démarrez l'outil Ressources sécurisées.
2. Obtenez un verrou en écriture.
3. Cliquez sur le bouton **Filtrer les ressources**.

L'outil Ressources sécurisées affiche la boîte de dialogue Filtrer les ressources.
4. Sélectionnez les types de ressources.
  - Sélectionnez les types de ressources que vous voulez inclure dans le filtre.
  - Décochez les types de ressources que vous voulez exclure du filtre.
5. Cliquez sur **OK**.

L'outil Ressources sécurisées affiche l'arborescence des ressources filtrées.

## Configuration des groupes de ressources

Vous pouvez utiliser l'outil Ressources sécurisées pour définir des groupes de ressources et créer une hiérarchie des ressources. Vous pouvez ensuite utiliser l'outil Rôles pour assigner des privilèges à plusieurs ressources dans une opération unique.

L'outil Ressources sécurisées fait la différence visuellement entre les ressources qui appartiennent directement au groupe de ressources actuel et celles qui y appartiennent indirectement. Les ressources ajoutées explicitement à un groupe de ressources possèdent une appartenance directe. Les ressources qui appartiennent à un groupe de ressources ajouté à un autre groupe de ressources possèdent une appartenance indirecte.

Imaginons par exemple que vous souhaitez avoir deux groupes de ressources :

- Le groupe de ressources A contient l'objet de base Client, ce qui signifie que l'objet de base Client est un membre direct du groupe de ressources A.
- Le groupe de ressources B contient l'objet de base Adresse.
- Le groupe de ressources A contient le groupe de ressources B, ce qui signifie que l'objet de base Adresse est un membre indirect du groupe de ressources A.

Dans cet exemple, l'objet de base Adresse est indisponible lorsque vous modifiez le groupe de ressources A. Vous devez modifier le groupe de ressources B pour pouvoir modifier l'objet de base Adresse.

## Ajout de groupes de ressources

Utilisez l'outil Ressources sécurisées pour ajouter un groupe de ressources à la liste de ressources.

1. Démarrez l'outil Ressources sécurisées.
2. Obtenez un verrou en écriture.
3. Cliquez sur l'onglet **Groupes de ressources**.  
L'outil Ressources sécurisées affiche l'onglet Groupe de ressources.
4. Cliquez sur le bouton **Ajouter**.  
L'outil Ressources sécurisées affiche la boîte de dialogue Ajouter des ressources à un groupe de ressources.
5. Entrez un nom descriptif unique pour ce groupe de ressources.
6. Cliquez sur le signe (+) pour développer la hiérarchie de ressource selon vos besoins.  
Chaque ressource possède une case à cocher indiquant l'appartenance dans le groupe de ressources. Si vous sélectionnez un parent, tous ses enfants sont également sélectionnés. Par exemple, si vous sélectionnez l'élément Objets de base dans l'arborescence, tous les objets de base et leurs ressources enfants sont sélectionnés.
7. Sélectionnez les ressources que voulez attribuer à ce groupe de ressources.
8. Cliquez sur **OK**.  
L'outil Ressources sécurisées ajoute la nouvelle ressource au nœud Groupes de ressources.

## Modification et suppression de groupes de ressources

Vous pouvez utiliser l'outil Ressources sécurisées pour modifier ou supprimer des groupes de ressources.

1. Démarrez l'outil Ressources sécurisées.
2. Obtenez un verrou en écriture.
3. Cliquez sur l'onglet **Groupes de ressources**.
4. Sélectionnez le groupe de ressources dont vous souhaitez modifier ou supprimer les propriétés.
  - Cliquez sur le bouton **Modifier** pour modifier un groupe de ressources.
  - Cliquez sur le bouton **Supprimer** pour supprimer un groupe de ressources.L'outil Ressources sécurisées affiche la boîte de dialogue Assigner des ressources au groupe de ressources. L'outil Ressources sécurisées supprime la ressource du nœud Groupes de ressources.
5. Modifiez le nom du groupe de ressources.
6. Cliquez sur le signe plus (+) pour développer la hiérarchie de ressources.

7. Cochez la case **Afficher uniquement les ressources sélectionnées pour ce groupe de ressources**.
8. Sélectionnez les ressources que voulez attribuer à ce groupe de ressources.
9. Effacez les ressources que vous voulez supprimer de ce groupe de ressources.
10. Cliquez sur **OK**.

## Actualisation de la liste de ressources

Après l'ajout d'une ressource, vous pouvez actualiser la liste de ressources pour la mettre à jour.

Pour actualiser la liste de ressources, sélectionnez **Actualiser** dans le menu Ressources sécurisées.

L'outil Ressources sécurisées actualise la liste de ressources.

## Actualisation d'autres modifications de sécurité

Vous pouvez également modifier l'intervalle d'actualisation pour toutes les autres modifications de sécurité.

Pour définir le taux d'actualisation des modifications de sécurité, définissez le paramètre suivant dans le fichier `cmxserver.properties` :

```
cmx.server.sam.cache.resources.refresh_interval
```

**Remarque:** L'intervalle d'actualisation par défaut est de 5 battements d'horloge (60 000 millisecondes pour 1 battement d'horloge), ce qui équivaut à 5 minutes.

# Configuration de la sécurité pour les services d'entité d'entreprise de Data Director

Les services d'entité d'entreprise sont des ressources sécurisées. Seuls les rôles utilisateur disposant de privilèges peuvent accéder aux services d'entité d'entreprise dans Data Director.

Vous pouvez configurer les ressources des services d'entité d'entreprise suivants dans la console MDM Hub :

- Rechercher-Remplacer
- Importation de fichier
- Correspondance Ad-hoc

Vous devez utiliser l'outil Ressource sécurisée pour configurer les services d'entité d'entreprise en tant que ressources sécurisées. Vous pouvez ensuite utiliser l'outil Rôles pour attribuer des privilèges aux rôles utilisateur.

## Configuration des services d'entité d'entreprise en tant que ressource sécurisée

Utilisez l'outil Ressources sécurisées dans l'espace de travail Gestionnaire d'accès de sécurité pour configurer les ressources requises en tant que ressource sécurisée.

1. Démarrez l'outil Ressources sécurisées.
2. Obtenez un verrouillage en écriture.
3. Cliquez sur l'onglet **Ressources**.

4. Accédez à l'arborescence de ressources et développez **Services d'entité d'entreprise**.
5. Double-cliquez sur le nom de la ressource pour basculer entre les statuts Sécurisé et Privé.
  - a. Cliquez sur le bouton **Sécurisé** pour associer les ressources sélectionnées au statut Sécurisé.
  - b. Cliquez sur le bouton **Privé** pour associer les ressources sélectionnées au statut Privé.
6. Cliquez sur **Enregistrer**.

## Attribution des privilèges de rôle aux services d'entité d'entreprise

Utilisez l'outil Rôles dans l'espace de travail Gestionnaire d'accès de sécurité pour attribuer des privilèges de services d'entité d'entreprise aux rôles utilisateur.

1. Démarrez l'outil Rôles.
2. Obtenez un verrouillage en écriture.
3. Faites défiler la liste de rôles et sélectionnez le rôle requis.
4. Cliquez sur l'onglet **Privilèges de ressource**.
5. Accédez à l'arborescence de ressources et développez **Services d'entité d'entreprise**.
6. Sélectionnez le privilège **Exécuter** pour chaque ressource des services d'entité d'entreprise.
7. Cliquez sur **Enregistrer**.

## CHAPITRE 3

# Rôles

Ce chapitre comprend les rubriques suivantes :

- [Présentation des rôles, 24](#)
- [Configuration de rôle, 25](#)
- [Privilèges, 25](#)
- [Rôles internes et rôles externes, 26](#)

## Présentation des rôles

Un rôle est un ensemble de privilèges que vous attribuez à un utilisateur ou à un groupe. Un rôle représente un ensemble de privilèges permettant d'accéder à des ressources sécurisées de MDM Hub.

Les utilisateurs doivent disposer de rôles qui leur accordent les privilèges suffisants pour accéder aux ressources MDM Hub pour pouvoir consulter et manipuler ces ressources. Les rôles déterminent les contenus auxquels un utilisateur est autorisé à accéder, ainsi que les tâches qu'il peut effectuer dans MDM Hub.

Les rôles de MDM Hub sont très granuleux et flexibles, ce qui permet aux administrateurs d'implémenter des sauvegardes de sécurité complexes en fonction des stratégies de sécurité de leur organisation. Certains utilisateurs, tels que les administrateurs, peuvent disposer d'un rôle unique permettant d'accéder à tous les éléments. D'autres, comme les gestionnaires de données, peuvent disposer d'un rôle associé à des privilèges explicitement restreints.

Un rôle peut également posséder plusieurs autres rôles, héritant ainsi des privilèges d'accès configurés pour ces derniers. Les privilèges sont cumulables, c'est-à-dire que lorsque vous combinez des rôles, vous combinez également les privilèges qui leur sont associés. Par exemple, supposons que le Rôle A possède des privilèges de lecture sur un objet de base Adresse et que le Rôle B possède des privilèges de création et de mise à jour sur ce même objet. Si un compte utilisateur se voit attribué le Rôle A et le Rôle B, cet utilisateur disposera alors des privilèges de lecture, de création et de mise à jour sur l'objet de base Adresse. Un compte utilisateur hérite des privilèges configurés pour les rôles auxquels il est affecté.



# Configuration de rôle

Vous pouvez créer, modifier et supprimer des rôles dans MDM Hub.

**Remarque:** Si vous utilisez un déploiement de sécurité centralisé complet dans lequel les utilisateurs sont autorisés de façon externe, vous n'avez pas besoin de configurer des rôles.

Les privilèges de ressource varient en fonction de l'accès nécessaire aux utilisateurs pour effectuer leurs tâches. La meilleure pratique pour les administrateurs consiste à suivre le principe de séparation des privilèges. Attribuez aux utilisateurs le niveau le plus faible de privilèges nécessaire pour effectuer leurs tâches.

## Ajout de rôles

Pour configurer les rôles et attribuer des privilèges d'accès aux ressources MDM Hub, utilisez l'outil Rôles dans l'espace de travail Gestionnaire d'accès de sécurité.

**Astuce:** Évitez d'utiliser des espaces dans les noms de rôle. Les espaces peuvent provoquer des erreurs lorsque MDM Hub communique avec ActiveVOS.

1. Démarrez l'outil Rôles.
2. Obtenez un verrou en écriture.
3. Pointez n'importe où dans le panneau de navigation, faites un clic droit et sélectionnez **Ajouter un rôle**.  
L'outil Rôles affiche la boîte de dialogue Ajouter un rôle.
4. Saisissez le nom du rôle.
5. Saisissez une description pour le rôle (facultatif).
6. Saisissez un nom externe (alias) pour le rôle.
7. Cliquez sur **OK**.  
Le nouveau rôle apparaît dans la liste des rôles.

## Modification et suppression de rôles

Pour modifier ou supprimer un rôle existant, utilisez l'outil Rôles dans l'espace de travail Gestionnaire d'accès de sécurité.

1. Démarrez l'outil Rôles.
2. Obtenez un verrou en écriture.
3. Faites défiler la liste des rôles et sélectionnez le rôle que vous souhaitez modifier.
  - Pour chaque propriété que vous souhaitez modifier, cliquez sur le bouton **Modifier** situé à côté de cette propriété et spécifiez la nouvelle valeur.
  - Pointez n'importe où dans le panneau de navigation, faites un clic droit et sélectionnez **Supprimer un rôle**, puis cliquez sur **Oui** lorsque vous y êtes invité pour confirmer votre choix.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

## Privilèges

Avec l'autorisation interne de MDM Hub, vous pouvez attribuer des privilèges à des rôles.

Vous pouvez attribuer les privilèges suivants aux rôles :

**Lecture**

L'utilisateur peut consulter, mais pas modifier des données.

**Création**

L'utilisateur peut créer des enregistrements de données dans le Stockage Hub.

**Mise à jour**

L'utilisateur peut mettre à jour des enregistrements de données dans le Stockage Hub.

**Supprimer**

L'utilisateur peut supprimer des enregistrements de données dans le Stockage Hub.

**Fusion**

L'utilisateur peut fusionner et annuler la fusion des données.

**Exécution**

L'utilisateur peut exécuter des fonctions de nettoyage et des groupes de lots.

Les privilèges déterminent l'accès des utilisateurs d'applications externes aux ressources MDM Hub. Par exemple, vous pouvez configurer un rôle afin de disposer de privilèges de lecture, de création, de mise à jour et de fusion sur des packages spécifiques.

**Remarque:** Chaque privilège est distinct et doit être affecté de manière explicite. Les privilèges ne regroupent pas d'autres privilèges. Par exemple, un utilisateur qui dispose d'un accès en mise à jour à une ressource ne dispose pas forcément d'un accès en lecture. Les privilèges doivent être attribués individuellement.

Lorsque vous utilisez la Console Hub, les privilèges ne sont pas appliqués, bien que les paramètres affectent l'utilisation de la Console Hub. Par exemple, les gestionnaires de données ne peuvent pas afficher tous les packages dans le Gestionnaire de fusions et le Gestionnaire de données, à l'exception de ceux pour lesquels ils possèdent des privilèges de lecture. Les gestionnaires des données doivent disposer de privilèges de mise à jour et de création pour un package pour pouvoir modifier ce dernier et enregistrer les modifications effectuées.

Les gestionnaires des données ne disposant pas de privilèges de mise à jour ou de création ne peuvent pas modifier de données dans le Gestionnaire de données. De même, un gestionnaire de données doit disposer de privilèges de fusion pour utiliser le Gestionnaire de fusions afin de fusionner des enregistrements ou d'annuler leur fusion. Pour en savoir plus sur les outils Gestionnaire de fusions et Gestionnaire de données, consultez le *Guide du Gestionnaire de données de MDM Multidomain*.

## Rôles internes et rôles externes

Dans une implémentation de la sécurité centralisée basée sur les rôles, vous devez créer un mappage entre le rôle interne de MDM Hub et le rôle externe géré séparément depuis MDM Hub.

Le nom du rôle externe peut être différent du nom du rôle interne utilisé dans un environnement MDM Hub.

Les détails de la configuration dépendent de l'implémentation du mappage du rôle du fournisseur de sécurité. Vous mappez les rôles dans un fichier de configuration. Vous pouvez mapper un rôle externe à plusieurs rôles internes.

**Remarque:** Bien que les mappages soient souvent créés en XML, il n'existe pas de format prédéfini pour les fichiers de configuration. Il peut s'agir d'un fichier dans un format autre que XML, voire même d'un autre élément qu'un fichier. Le mappage fait partie de l'implémentation du fournisseur d'authentification ou du

profil utilisateur personnalisé. L'objectif du mappage est de remplir une liste de rôles d'objet de profil utilisateur avec des identifiants de rôles internes.

## Attribution de privilèges de ressource aux rôles

Vous pouvez utiliser l'outil Rôles dans l'espace de travail Gestionnaire d'accès de sécurité pour attribuer des privilèges de ressource aux rôles et les modifier.

1. Démarrez l'outil Rôles.
2. Obtenez un verrou en écriture.
3. Faites défiler la liste des rôles et sélectionnez celui auquel vous souhaitez attribuer des privilèges de ressource.
4. Cliquez sur l'onglet **Privilèges de ressource**.
5. Développez la hiérarchie des ressources pour afficher les ressources sécurisées que vous voulez configurer pour ce rôle.
6. Pour chaque ressource que vous voulez configurer :
  - Sélectionnez les privilèges que vous voulez accorder à ce rôle.
  - Décochez les privilèges que vous ne voulez pas attribuer à ce rôle.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

## Attribution de rôles à d'autres rôles

Un rôle peut aussi hériter d'autres rôles, sauf d'un rôle auquel il appartient déjà. Par exemple, si vous attribuez le rôle B au rôle A, le rôle A hérite des privilèges d'accès du rôle B.

1. Démarrez l'outil Rôles.
2. Obtenez un verrou en écriture.
3. Faites défiler la liste des rôles et sélectionnez le rôle auquel vous souhaitez assigner d'autres rôles.
4. Cliquez sur l'onglet **Rôles**.

L'outil Rôles affiche tous les rôles qui peuvent être attribués au rôle sélectionné.
5. Sélectionnez les rôles que voulez attribuer au rôle sélectionné.
6. Décochez les rôles que ne voulez pas attribuer à ce rôle.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

## Génération d'un rapport de privilèges de ressources pour les rôles

Vous pouvez générer un rapport décrivant uniquement les privilèges de ressource accordés à un rôle donné.

1. Démarrez l'outil Rôles.
2. Obtenez un verrou en écriture.
3. Faites défiler la liste des rôles et sélectionnez le rôle pour lequel vous souhaitez générer un rapport.
4. Cliquez sur l'onglet **Rapport**.
5. Cliquez sur **Générer**.

L'outil Rôles génère le rapport et l'affiche dans l'onglet Rapport.

## Enregistrement du rapport généré au format HTML

1. Cliquez sur **Enregistrer**.

L'outil Rôles vous invite à spécifier l'emplacement cible du rapport sauvegardé.

2. Naviguez jusqu'à l'emplacement cible.

3. Cliquez sur **Enregistrer**.

Le Gestionnaire d'accès de sécurité enregistre le rapport à l'aide de la convention de nommage suivante :

`<ORS_Name>-<Role_Name>-RolePrivilegeReport.html`

où

- *ORS\_Name* correspond au nom de la base de données cible.
- *Role\_Name* correspond au rôle associé au rapport généré.

L'outil Rôles enregistre le rapport actuel au format HTML dans l'emplacement cible. Vous pouvez ensuite afficher le rapport à l'aide d'un navigateur.

## CHAPITRE 4

# Utilisateurs et groupes d'utilisateurs

Ce chapitre comprend les rubriques suivantes :

- [Présentation des utilisateurs et des groupes d'utilisateurs, 29](#)
- [Configuration utilisateur, 29](#)
- [Configuration de la stratégie des mots de passe, 33](#)
- [Configuration de la sécurité des sources de données JDBC, 34](#)
- [Configuration du groupe d'utilisateurs, 36](#)
- [Associations entre les rôles et les utilisateurs et groupes d'utilisateurs, 39](#)

## Présentation des utilisateurs et des groupes d'utilisateurs

Un utilisateur de MDM Hub est un individu qui peut accéder à des ressources de MDM Hub.

Les comptes utilisateur sont définis dans la Base de données principale du Stockage Hub. Pour en savoir plus sur les utilisateurs de MDM Hub, consultez la *Guide de présentation de MDM Multidomain*.

Un compte utilisateur peut accéder aux ressources de MDM Hub grâce aux rôles qui lui sont attribués, en héritant des privilèges configurés pour chaque rôle.

Vous pouvez utiliser l'outil Utilisateurs dans l'espace de travail de configuration afin de configurer les comptes utilisateur des utilisateurs MDM Hub, ainsi que pour changer les mots de passe et activer l'authentification externe. Les applications externes disposant des autorisations suffisantes peuvent également enregistrer des comptes utilisateur par le biais de demandes SIF, comme décrit dans le *Guide de l'infrastructure d'intégration des services de MDM Multidomain*.

## Configuration utilisateur

Vous pouvez créer, modifier et supprimer des utilisateurs dans MDM Hub.

Selon la manière dont vous avez déployé la sécurité, votre implémentation de MDM Hub peut nécessiter l'ajout d'utilisateurs à la Base de données principale.

Vous devez configurer les utilisateurs dans la Base de données principale dans les scénarios suivants :

- Vous utilisez une autorisation interne dans MDM Hub.
- Vous utilisez une autorisation externe dans MDM Hub.
- Plusieurs utilisateurs accèdent à la Console Hub à l'aide de comptes différents.

Un utilisateur doit être défini une seule fois, même s'il accède à plus d'un Stockage de référence opérationnelle associé à la Base de données principale.

## Accès des utilisateurs aux ressources de MDM Hub

Les utilisateurs, y compris les administrateurs et les gestionnaires de données, peuvent accéder aux ressources de MDM Hub de l'une des manières suivantes :

### Applications MDM

Les utilisateurs peuvent interagir avec MDM Hub en se connectant à la Console Hub et en utilisant les outils auxquels ils ont accès. Les utilisateurs peuvent aussi utiliser IDD ou l'outil d'approvisionnement pour accéder aux données des objets de base et des entités commerciales.

### Applications tierces

Les utilisateurs peuvent interagir avec les données de MDM Hub indirectement par le biais d'applications tierces utilisant les classes SIF. Ces utilisateurs ne se connectent jamais à la Console Hub. Ils se connectent à MDM Hub à l'aide d'applications capables d'appeler les classes SIF. Ces utilisateurs sont appelés des utilisateurs d'applications externes. Pour en savoir plus sur les types de demandes SIF que les développeurs peuvent appeler, consultez le *Guide de l'infrastructure d'intégration des services de MDM Multidomain*.

## Ajout de comptes utilisateur

Utilisez l'outil Utilisateurs dans l'espace de travail du gestionnaire d'accès de sécurité pour ajouter un compte utilisateur à MDM Hub.

1. Démarrez l'outil Utilisateurs.
2. Obtenez un verrou en écriture.
3. Cliquez sur l'onglet **Utilisateurs**.
4. Cliquez sur le bouton **Ajouter un utilisateur**.

L'outil Utilisateurs affiche la boîte de dialogue **Ajouter un utilisateur**.

5. Saisissez le prénom, le deuxième prénom et le nom de famille de l'utilisateur.
6. Entrez un nom pour l'utilisateur.

**Remarque:** Les noms d'utilisateur sont insensibles à la casse et sont stockés en minuscules.

7. Saisissez une adresse de courriel valide pour l'utilisateur. MDM Hub envoie le mot de passe du compte utilisateur à cette adresse de courriel.
8. Saisissez la base de données par défaut pour l'utilisateur. Il s'agit de la base de données sélectionnée par défaut lorsque l'utilisateur se connecte à la Console Hub.
9. Si le compte utilisateur concerne une application, cochez la case **Utilisateur de l'application**.

**Remarque:** Les utilisateurs d'application sont utilisés pour l'authentification basée sur un certificat des demandes générées par une application approuvée pour le compte de l'utilisateur.

10. Saisissez et confirmez un mot de passe pour l'utilisateur.
11. Choisissez le type d'authentification.

- Cochez la case **Utiliser l'authentification externe** si votre implémentation de MDM Hub utilise une authentification via un fournisseur de sécurité tiers.
  - Décochez la case **Utiliser l'authentification externe** si vous souhaitez utiliser une authentification interne dans MDM Hub.
12. Recherchez un certificat public pour l'utilisateur. Ce certificat peut être utilisé par MDM Hub pour authentifier les demandes des utilisateurs.
- Remarque:** Si le compte utilisateur concerne un utilisateur d'application, vous devez sélectionner un certificat.
13. Cliquez sur **OK**.
- L'outil Utilisateurs ajoute le nouvel utilisateur à la liste d'utilisateurs dans l'onglet **Utilisateurs**.

## Modification et suppression de comptes utilisateur

Vous pouvez utiliser l'outil Utilisateurs dans l'espace de travail du gestionnaire d'accès de sécurité pour modifier ou supprimer des comptes utilisateur.

1. Démarrez l'outil Utilisateurs.
2. Obtenez un verrou en écriture.
3. Cliquez sur l'onglet **Utilisateurs**.
4. Pour supprimer un utilisateur, sélectionnez le compte utilisateur que vous voulez supprimer.
5. Cliquez sur le bouton **Supprimer**.  
L'outil Utilisateurs vous demande de confirmer la suppression.
6. Cliquez sur **Oui** pour confirmer la suppression.  
L'outil Utilisateurs supprime le compte utilisateur de la liste des utilisateurs.
7. Pour modifier un utilisateur, sélectionnez le compte utilisateur que vous souhaitez configurer.
8. Pour modifier un nom, cliquez deux fois sur la cellule et entrez un nom différent.
9. Si vous le souhaitez, sélectionnez un serveur et une base de données de connexion différents.
10. Cochez la case **Administrateur** pour accorder un accès administrateur à cet utilisateur, afin qu'il puisse accéder à tous les outils et bases de données de la Console Hub.
11. Cochez la case **Activer** pour activer ce compte utilisateur et permettre à l'utilisateur concerné de se connecter.  
**Remarque:** Si vous utilisez l'authentification externe pour un utilisateur, vous ne pouvez pas désactiver le compte utilisateur via la Console Hub.
12. Cliquez sur le bouton **Enregistrer**.  
L'outil Utilisateurs enregistre les modifications apportées au compte utilisateur.

## Modification d'informations utilisateur supplémentaires

Vous pouvez utiliser MDM Hub pour gérer des informations supplémentaires pour chaque utilisateur, telles qu'une adresse de courriel ou des numéros de téléphone. MDM Hub ne requiert pas que vous indiquiez ces informations et MDM Hub ne les utilise pas de manière spécifique.

**Remarque:** Vous ne pouvez pas modifier l'adresse de courriel de l'utilisateur `Admin` dans la console Hub. Pour modifier l'adresse de courriel de l'utilisateur Admin, mettez à jour l'entrée correspondante directement dans la table `C_REPOS_USER`, sous le schéma `CMX_SYSTEM`.

1. Démarrez l'outil Utilisateurs.

2. Obtenez un verrou en écriture.
3. Cliquez sur l'onglet **Utilisateurs**.
4. Sélectionnez l'utilisateur pour lequel vous souhaitez modifier les propriétés.
5. Cliquez sur le bouton **Modifier**.  
L'outil Utilisateurs affiche la boîte de dialogue **Modifier l'utilisateur**.
6. Spécifiez les propriétés de l'utilisateur, telles que le titre, l'adresse de courriel ou le message de connexion. Le message de connexion est le message que la Console Hub affiche lorsque cet utilisateur se connecte.
7. Cliquez sur **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

## Modification des paramètres de mot de passe pour les comptes utilisateur

Vous pouvez modifier les paramètres de mot de passe pour un utilisateur.

1. Démarrez l'outil Utilisateurs.
2. Obtenez un verrou en écriture.
3. Cliquez sur l'onglet **Utilisateurs**.
4. Sélectionnez l'utilisateur pour lequel vous souhaitez changer le mot de passe.
5. Cliquez sur le bouton **Modifier le mot de passe**.  
L'outil Utilisateurs affiche la boîte de dialogue **Modifier le mot de passe** pour l'utilisateur sélectionné.
6. Spécifiez et confirmez le nouveau mot de passe.
7. Choisissez le type d'authentification.
  - Cochez la case **Utiliser l'authentification externe** si votre implémentation de MDM Hub utilise une authentification via un fournisseur de sécurité tiers.
  - Décochez la case **Utiliser l'authentification externe** si vous souhaitez utiliser une authentification interne dans MDM Hub.
8. Cliquez sur **OK**.

## Configuration de l'accès des utilisateurs au stockage de référence opérationnelle (Operational Reference Store - ORS)

Vous pouvez configurer l'accès des utilisateurs aux bases de données du Stockage de référence opérationnelle.

1. Démarrez l'outil Utilisateurs.
2. Obtenez un verrou en écriture.
3. Cliquez sur l'onglet **Base de données cible**.  
L'outil Utilisateurs affiche la boîte de dialogue Base de données cible.
4. Développez chaque nœud de la base de données pour voir quels utilisateurs peuvent accéder à la base de données.
5. Pour changer les attributions d'un utilisateur à une base de données, cliquez avec le bouton droit de la souris sur le nom de la base de données et choisissez **Assigner un utilisateur**.



L'outil Utilisateurs affiche la boîte de dialogue **Assigner l'utilisateur à la base de données**.

6. Sélectionnez les noms des utilisateurs que vous voulez assigner à la base de données sélectionnée.
7. Décochez les noms des utilisateurs que vous ne voulez pas assigner à la base de données sélectionnée.
8. Cliquez sur **OK**.

## Configuration de la stratégie des mots de passe

Vous pouvez définir des stratégies globales de mots de passe pour tous les utilisateurs. Configurez des stratégies de mots de passe personnels qui remplacent les stratégies globales de mots de passe pour les utilisateurs individuels. Tous les mots de passe sont sensibles à la casse.

**Remarque:** Si vous déployez MDM Hub sur le serveur d'application JBoss avec la sécurité activée, vérifiez que le mot de passe que vous définissez respecte la stratégie des mots de passe JBoss. Votre mot de passe doit également respecter la stratégie globale des mots de passe de MDM Hub. Ceci est important, car les mots de passe doivent correspondre pour la Console Hub et pour JBoss.

### Paramètres de la stratégie des mots de passe

Vous pouvez spécifier les paramètres de la stratégie des mots de passe pour les utilisateurs de MDM Hub.

MDM Hub vous permet de définir les stratégies de mots de passe personnels suivantes pour les utilisateurs :

#### Longueur du mot de passe

Longueur minimum et maximum d'un mot de passe en caractères.

#### Expiration du mot de passe

Spécifie si un mot de passe expire ou non, ainsi que le nombre de jours pendant lequel il reste valide.

Cochez la case **Le mot de passe expire** pour définir une période d'expiration pour les mots de passe.

Décochez la case **Le mot de passe expire** pour définir des mots de passe qui n'expirent pas.

Si vous cochez la case **Le mot de passe expire**, spécifiez le nombre de jours dans lequel le mot de passe expire. La période d'expiration minimale du mot de passe que vous pouvez définir est 10.

#### Paramètres de connexion

Nombre de tentatives de connexion et nombre maximal d'échecs de connexion autorisés.

#### Historique du mot de passe

Nombre de fois qu'un mot de passe peut être réutilisé.

#### Exigences du mot de passe

Cochez la case **Validation de la forme du mot de passe activée** pour appliquer un modèle de mot de passe. Vous pouvez spécifier les critères suivants pour le modèle du mot de passe :

- Nombre minimum de caractères uniques
- Le mot de passe doit commencer par
- Le mot de passe doit contenir
- Le mot de passe doit se terminer par

## Gestion de la stratégie globale des mots de passe

La stratégie globale des mots de passe s'applique aux utilisateurs qui n'ont pas de stratégie des mots de passe individuelle spécifique.

1. Démarrez l'outil **Utilisateurs**.
2. Obtenez un verrou en écriture.
3. Cliquez sur l'onglet **Stratégie globale des mots de passe**.  
La fenêtre Stratégie globale des mots de passe s'affiche.
4. Spécifiez les paramètres de stratégie des mots de passe.
5. Cliquez sur **OK**.
6. Cliquez sur le bouton **Enregistrer** pour enregistrer vos paramètres globaux.

## Gestion des stratégies de mots de passe personnels

Vous pouvez spécifier une stratégie des mots de passe personnelle qui remplace la stratégie globale des mots de passe pour un utilisateur.

**Remarque:** La meilleure pratique en ce qui concerne la gestion de la stratégie des mots de passe consiste à s'assurer que la plupart des mots de passe utilisateur sont gérés par une stratégie globale et non par plusieurs stratégies privées.

1. Démarrez l'outil Utilisateurs.
2. Obtenez un verrou en écriture.
3. Cliquez sur l'onglet **Utilisateurs**.
4. Sélectionnez l'utilisateur pour lequel vous souhaitez définir la stratégie de mots de passe personnels.
5. Cliquez sur le **Gérer la stratégie des mots de passe**.  
La fenêtre **stratégie des mots de passe personnelle** pour l'utilisateur sélectionné s'affiche.
6. Activez l'option **stratégie des mots de passe personnels activée**.
7. Spécifiez les paramètres de stratégie des mots de passe pour l'utilisateur.
8. Cliquez sur **OK**.
9. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

## Configuration de la sécurité des sources de données JDBC

Dans les implémentations de MDM Hub, si une source de données JDBC utilise la sécurité du serveur d'application, vous devez configurer les paramètres présents dans le fichier cmxserver.properties.

Vous devez stocker le nom d'utilisateur et le mot de passe pour le serveur d'application pour la source de données JDBC dans le fichier cmxserver.properties. Les mots de passe ne peuvent pas s'afficher en texte clair. Vous devez encrypter les mots de passe avant de les enregistrer dans le fichier cmxserver.properties.

Pour en savoir plus sur les sources de données sécurisées JDBC, consultez la documentation de votre serveur d'applications.

## Noms d'utilisateur et mots de passe pour une source de données JDBC sécurisée

Pour configurer les noms d'utilisateur et des mots de passe pour une source de données JDBC sécurisée dans le fichier de propriétés `cmxserver.properties`, utilisez les paramètres suivants :

```
databaseId.username=username  
databaseId.password=encryptedPassword
```

où `databaseId` est l'identificateur unique de la source de données JDBC.

## Identifiant de base de données pour les types de connexion SID Oracle

Pour un type de connexion SID Oracle, `databaseId` est composé des chaînes suivantes :

```
<nom d'hôte de base de données>-<Oracle SID>-<nom de schéma>
```

Par exemple, avec les paramètres suivants :

- `<nom d'hôte de base de données> = localhost`
- `<Oracle SID> = MDMHUB`
- `<nom de schéma> = Test_ORS`

les propriétés du nom d'utilisateur et du mot de passe sont :

```
localhost-MDMHUB-Test_ORS.username=weblogic  
localhost-MDMHUB-Test_ORS.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

## Identifiant de base de données pour les types de connexion au service Oracle

Pour un type de connexion au service Oracle, `databaseId` est composé des chaînes suivantes :

```
<nom de service>-<nom de schéma>
```

Par exemple, avec les paramètres suivants :

- `<nom de service> = MDM_Service`
- `<nom de schéma> = Test_ORS`

les propriétés du nom d'utilisateur et du mot de passe sont :

```
MDM_Service-Test_ORS.username=weblogic  
MDM_Service-Test_ORS.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

## ID de base de données pour les types de connexion IBM Db2

Pour un type de connexion IBM Db2, l'ID de base de données est composé des chaînes suivantes :

```
<nom d'hôte de base de données>-<nom de la base de données>-<nom de schéma>
```

Par exemple, avec les paramètres suivants :

- `<nom d'hôte de base de données> = localhost`
- `<nom de la base de données> = dsui2`
- `<nom de schéma> = DS_UI2`

les propriétés du nom d'utilisateur et du mot de passe sont :

```
localhost-dsui2-DS_UI2.username=weblogic  
localhost-dsui2-DS_UI2.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

## Identifiant de base de données pour les types de connexion Microsoft SQL Server

Pour un type de connexion Microsoft SQL Server, l'identifiant de base de données est composé des chaînes suivantes :

```
<nom d'hôte de base de données>-<nom de la base de données>
```

Par exemple, avec les paramètres suivants :

- <nom d'hôte de base de données> = localhost
- <nom de la base de données> = ds\_ui1

les propriétés du nom d'utilisateur et du mot de passe sont :

```
localhost-ds_ui1.username=weblogic  
localhost-ds_ui1.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

## Identifiant de base de données pour la base de données principale

Si vous voulez sécuriser la source de données JDBC qui accède au Base de données principale, le `databaseId` est `CMX_SYSTEM`. Dans ce cas, les propriétés sont :

```
CMX_SYSTEM.username=weblogic  
CMX_SYSTEM.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

## Chiffage du mot de passe

Pour générer un mot de passe chiffré pour un schéma de base de données, utilisez les commandes suivantes :

```
C:\>java -cp siperian-common.jar com.siperian.common.security.Blowfish password  
Plaintext Password: password  
Encrypted Password: 9C03B113CD8E4BBFD236C56D5FEA56EB
```

# Configuration du groupe d'utilisateurs

Un groupe d'utilisateurs est un ensemble logique de comptes utilisateur.

Les groupes d'utilisateurs simplifient l'administration de la sécurité. Par exemple, vous pouvez combiner des utilisateurs d'applications externes dans un groupe d'utilisateurs, puis attribuer des rôles de sécurité au groupe d'utilisateurs plutôt que de les attribuer individuellement à chaque utilisateur. En plus des utilisateurs, les groupes d'utilisateurs peuvent contenir d'autres groupes d'utilisateurs.

Vous pouvez utiliser l'onglet Groupes dans l'outil Utilisateurs et groupes dans l'espace de travail Gestionnaire d'accès de sécurité pour configurer les groupes d'utilisateurs.

## Démarrage de l'outil Utilisateurs et groupes

Démarrez l'outil Utilisateurs et groupes dans la Console Hub.

1. Dans la Console Hub, connectez-vous à un Stockage de référence opérationnelle, si ce n'est pas déjà fait.
2. Développez l'espace de travail du gestionnaire d'accès de sécurité, puis cliquez sur **Utilisateurs et groupes**.

La Console Hub affiche l'outil Utilisateurs et groupes.

L'outil Utilisateurs et groupes comporte les onglets suivants :

### **Groupes**

Permet de définir des groupes d'utilisateurs et de leur affecter des utilisateurs.

### **Utilisateurs assignés à la base de données**

Permet d'associer des comptes utilisateur à une base de données.

### **Assigner les utilisateurs/groupes au rôle**

Permet d'associer des utilisateurs et des groupes d'utilisateurs à des rôles.

### **Assigner les rôles à l'utilisateur/au groupe**

Permet d'associer des rôles aux utilisateurs et aux groupes d'utilisateurs.

## Ajout de groupes d'utilisateurs

Vous pouvez utiliser l'outil Utilisateurs et groupes dans l'espace de travail du gestionnaire d'accès de sécurité pour ajouter des groupes d'utilisateurs.

1. Démarrez l'outil Utilisateurs et groupes.
2. Obtenez un verrou en écriture.
3. Cliquez sur l'onglet **Groupes**.
4. Cliquez sur le bouton **Ajouter**.

L'outil Utilisateurs et groupes affiche la boîte de dialogue **Ajouter un groupe d'utilisateurs**.

5. Entrez un nom descriptif pour ce groupe d'utilisateurs.
6. Entrez une description facultative de ce groupe d'utilisateurs.
7. Cliquez sur **OK**.

L'outil Utilisateurs et groupes ajoute le nouveau groupe d'utilisateurs à la liste.

## Modification et suppression de groupes d'utilisateurs

Vous pouvez également utiliser l'outil Utilisateurs et groupes pour modifier ou supprimer des groupes d'utilisateurs.

1. Démarrez l'outil Utilisateurs et groupes.
2. Obtenez un verrou en écriture.
3. Cliquez sur l'onglet **Groupes**.
4. Faites défiler la liste des groupes d'utilisateurs et sélectionnez le groupe d'utilisateurs que vous souhaitez modifier.
5. Pour supprimer un groupe d'utilisateurs, cliquez sur le bouton **Supprimer**.

L'outil Utilisateurs et Groupes vous demande de confirmer la suppression.

6. Cliquez sur **Oui**.  
L'outil Utilisateurs et groupes supprime le groupe d'utilisateurs de la liste.
7. Pour modifier un groupe d'utilisateurs, cliquez sur le bouton **Modifier** situé à côté de chaque propriété que vous voulez modifier, puis spécifiez la nouvelle valeur souhaitée.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

## Attribution d'utilisateurs et de groupes d'utilisateurs à des groupes d'utilisateurs

Pour attribuer des membres à un groupe d'utilisateurs :

1. Démarrez l'outil Utilisateurs et Groupes.
2. Obtenez un verrou en écriture.
3. Cliquez sur l'onglet **Groupe**.
4. Faites défiler la liste des groupes d'utilisateurs et sélectionnez le groupe d'utilisateurs que vous souhaitez modifier.
5. Cliquez avec le bouton droit de la souris sur le groupe d'utilisateurs que vous venez de créer et choisissez **Assigner des utilisateurs et des groupes**.

L'outil Utilisateurs et groupes affiche la boîte de dialogue **Assigner au groupe d'utilisateurs**.

6. Sélectionnez les noms des utilisateurs et des groupes d'utilisateurs que vous voulez assigner au groupe d'utilisateurs sélectionné.
7. Décochez les noms des utilisateurs et groupes d'utilisateurs que vous ne voulez pas assigner au groupe d'utilisateurs sélectionné.
8. Cliquez sur **OK**.

## Attribution d'utilisateurs à la base de données ORS actuelle

Pour assigner des utilisateurs à la base de données Stockage de référence opérationnelle actuelle :

1. Démarrez l'outil Utilisateurs et groupes.
2. Obtenez un verrou en écriture.
3. Cliquez sur l'onglet **Utilisateurs assignés à la base de données**.
4. Cliquez sur le bouton **Assigner des utilisateurs à la base de données** pour assigner des utilisateurs à une base de données Stockage de référence opérationnelle.

L'outil Utilisateurs et groupes affiche la boîte de dialogue **Assigner l'utilisateur à la base de données**.

5. Sélectionnez les noms des utilisateurs que vous voulez assigner à la base de données Stockage de référence opérationnelle sélectionnée.
6. Décochez les noms des utilisateurs que vous ne voulez pas assigner à la base de données Stockage de référence opérationnelle sélectionnée.
7. Cliquez sur **OK**.

# Associations entre les rôles et les utilisateurs et groupes d'utilisateurs

Vous pouvez associer des rôles aux utilisateurs et aux groupes d'utilisateurs. Vous pouvez utiliser l'outil **Utilisateurs et groupes** pour associer des rôles aux utilisateurs en utilisant les méthodes suivantes :

- Affectez des utilisateurs et des groupes d'utilisateurs aux rôles.
- Affectez des rôles aux utilisateurs et aux groupes d'utilisateurs.

Choisissez la méthode la plus appropriée pour votre implémentation.

## Attribution d'utilisateurs et de groupes d'utilisateurs à des rôles

Pour assigner des utilisateurs et des groupes d'utilisateurs à un rôle :

1. Démarrez l'outil Utilisateurs et groupes.
2. Obtenez un verrou en écriture.
3. Cliquez sur l'onglet **Assigner les utilisateurs/groupe au rôle**.
4. Sélectionnez le rôle auquel vous voulez assigner des utilisateurs et des groupes d'utilisateurs.
5. Cliquez sur le bouton **Modifier**.

L'outil Utilisateurs et groupes affiche la boîte de dialogue **Assigner des utilisateurs au rôle**.

6. Sélectionnez les noms des utilisateurs et groupes d'utilisateurs que vous voulez assigner au rôle sélectionné.
7. Décochez les noms des utilisateurs et groupes d'utilisateurs que vous ne voulez pas assigner au rôle sélectionné.
8. Cliquez sur **OK**.

## Attribution de rôles à des utilisateurs et des groupes d'utilisateurs

Pour assigner des rôles aux utilisateurs et aux groupes d'utilisateurs :

1. Démarrez l'outil Utilisateurs et groupes.
2. Obtenez un verrou en écriture.
3. Cliquez sur l'onglet **Assigner les rôles à l'utilisateur/au groupe**.
4. Sélectionnez l'utilisateur ou le groupe d'utilisateurs auquel vous voulez assigner des rôles.
5. Cliquez sur le bouton **Modifier**.

L'outil Utilisateurs et groupes affiche la boîte de dialogue **Assigner des rôles à l'utilisateur**.

6. Sélectionnez les rôles que vous voulez assigner à l'utilisateur ou au groupe d'utilisateurs sélectionné.
7. Décochez les rôles que vous ne voulez pas assigner à l'utilisateur ou au groupe d'utilisateurs sélectionné.
8. Cliquez sur **OK**.

## CHAPITRE 5

# Fournisseurs de sécurité

Ce chapitre comprend les rubriques suivantes :

- [Présentation des fournisseurs de sécurité, 40](#)
- [Gestion des fournisseurs de sécurité, 40](#)
- [Gestion du fichier de fournisseur, 41](#)
- [Paramètres du fournisseur de sécurité, 42](#)
- [Propriétés du fournisseur, 43](#)
- [Fournisseurs personnalisés, 45](#)
- [Authentification externe, 46](#)

## Présentation des fournisseurs de sécurité

Un fournisseur de sécurité est une application tierce qui fournit des services de sécurité, tels que l'authentification et l'autorisation, aux utilisateurs qui accèdent à MDM Hub. Les fournisseurs de sécurité sont concernés par certains scénarios de déploiement de sécurité de MDM Hub.

Un fichier de fournisseur contient des informations de profil sur un fournisseur de sécurité. Si vous souhaitez utiliser d'autres fournisseurs de sécurité tiers, utilisez l'outil Fournisseurs de sécurité pour charger des fichiers de fournisseurs dans MDM Hub. Vous pouvez également utiliser l'outil Fournisseurs de sécurité pour modifier, supprimer, activer ou désactiver des fournisseurs de sécurité dans la liste des fournisseurs.

MDM Hub est livré avec un ensemble de fournisseurs de sécurité internes par défaut. Vous pouvez également y ajouter des fournisseurs de sécurité tiers. Les fournisseurs de sécurité internes ne peuvent pas être supprimés.

## Gestion des fournisseurs de sécurité

Vous pouvez gérer les fournisseurs de sécurité dans l'implémentation de MDM Hub via l'outil Fournisseurs de sécurité, disponible dans l'espace de travail de configuration de la Console Hub.

Vous pouvez ajouter des fournisseurs de sécurité depuis la sélection par défaut interne de MDM Hub ou à partir de votre propre sélection personnalisée de fournisseurs. Les fournisseurs de sécurité internes ne peuvent pas être supprimés.

MDM Hub prend en charge les types de fournisseurs de sécurité suivants :



**Fournisseur d'authentification**

Authentifie un utilisateur en validant son identité. Indique à MDM Hub que les utilisateurs sont bien ceux qu'ils prétendent être. Ce type de fournisseur de sécurité ne vérifie pas si les utilisateurs disposent des privilèges requis pour accéder à des ressources particulières de MDM Hub.

**Fournisseur d'autorisation**

Indique à MDM Hub si les utilisateurs disposent des privilèges requis pour accéder à des ressources particulières de MDM Hub.

**Fournisseur de profils utilisateurs**

Indique à MDM Hub des informations sur chaque utilisateur, telles que les attributs spécifiques à l'utilisateur et les rôles auxquels il appartient.

Les fournisseurs internes représentent les implémentations internes de MDM Hub pour les services d'authentification, d'autorisation et de profil utilisateur.

Certains fournisseurs par défaut de MDM Hub sont des fournisseurs de contrôle. Les fournisseurs de contrôle renvoient toujours une réponse positive pour les demandes d'authentification et d'autorisation. Utilisez un fournisseur de contrôle dans un environnement de développement si vous ne souhaitez pas configurer les utilisateurs, les rôles et les privilèges. Les fournisseurs de contrôle peuvent également être utilisés dans un environnement de production dans lequel la sécurité est déployée en couche au-dessus des demandes SIF afin d'améliorer les performances.

## Gestion du fichier de fournisseur

Un fichier de fournisseur contient des informations de profil sur un fournisseur de sécurité.

Si vous souhaitez utiliser vos propres fournisseurs de sécurité tiers, vous devez les enregistrer explicitement via l'outil Fournisseurs de sécurité. Pour enregistrer un fournisseur de sécurité, chargez un fichier de fournisseur contenant les informations de profil nécessaires à l'enregistrement.

Un fichier de fournisseur est un fichier JAR qui contient les informations suivantes :

- Manifeste décrivant un ou plusieurs fournisseurs de sécurité externes. Chaque fournisseur de sécurité comprend les paramètres suivants :
  - Nom du fournisseur
  - Description du fournisseur
  - Type de fournisseur
  - Nom de classe d'usine du fournisseur
  - Propriétés spécifiant les détails de configuration pour le fournisseur. Il peut s'agir d'une liste de paires nom-valeur : noms de propriété avec valeurs par défaut.
- Implémentation du fournisseur et bibliothèques tierces requises.

Le InformaticaKit de ressources copie un exemple d'implémentation d'un fichier de fournisseur sur le Serveur Hub. Pour plus d'informations sur l'exemple de fichier de fournisseur, consultez le *Guide du kit de ressources de MDM Multidomain*.

## Téléchargement d'un fichier de fournisseur

Chargez un fichier de fournisseur afin d'ajouter ou de mettre à jour les informations du fournisseur.

1. Démarrez l'outil Fournisseurs de sécurité.
2. Obtenez un verrou en écriture.
3. Dans le panneau de navigation gauche, cliquez avec le bouton droit sur Fichiers de fournisseurs et choisissez **Télécharger le fichier du fournisseur**.  
L'outil Fournisseur de sécurité vous demande de sélectionner le fichier JAR de ce fournisseur.
4. Spécifiez le fichier JAR, en parcourant le système de fichiers selon les besoins et en sélectionnant le fichier JAR à télécharger.
5. Cliquez sur **Ouvrir**.  
L'outil Fournisseur de sécurité vérifie le fichier sélectionné pour déterminer si c'est un fichier de fournisseur valide.
6. Si le fichier de fournisseur que vous chargez possède le même nom qu'un fichier de fournisseur existant, l'outil Fournisseur de sécurité vous demande si vous souhaitez écraser le fichier de fournisseur existant. Cliquez sur **Oui** pour confirmer.  
L'outil Fournisseur de sécurité ajoute les informations sur le nouveau fournisseur à la liste des Fournisseurs. Après avoir chargé le fichier de fournisseur, vous pouvez supprimer le fichier d'origine du système de fichiers.

## Suppression d'un fichier de fournisseur

Vous pouvez supprimer un fichier de fournisseur si vous n'utilisez plus ce fournisseur.

1. Démarrez l'outil Fournisseurs de sécurité.
2. Obtenez un verrou en écriture.
3. Dans le panneau de navigation de gauche, cliquez avec le bouton droit de la souris sur le fichier fournisseur que vous souhaitez supprimer, puis choisissez **Supprimer le fichier fournisseur**.  
L'outil Fournisseur de sécurité vous demande de confirmer la suppression.
4. Cliquez sur **Oui**.  
L'outil Fournisseur de sécurité retire le fournisseur supprimé de la liste.  
**Remarque:** Vous ne pouvez pas supprimer les fichiers du fournisseur interne livré avec MDM Hub.

## Paramètres du fournisseur de sécurité

L'outil Fournisseurs de sécurité affiche une liste des fournisseurs enregistrés.

La liste des fournisseurs enregistrés est triée par type de fournisseur. La séquence des fournisseurs dans la liste de fournisseurs représente également l'ordre dans lequel ces derniers sont appelés. Un utilisateur doit être authentifié par au moins un fournisseur dans la liste de fournisseurs.

Par exemple, lorsque vous tentez de vous connecter en saisissant votre nom d'utilisateur et votre mot de passe, MDM Hub envoie vos justificatifs d'identité de connexion à chaque fournisseur d'authentification de la liste d'authentification. MDM Hub progresse de manière séquentielle dans la liste. Si l'authentification réussit auprès de l'un des fournisseurs de la liste, alors MDM Hub vous authentifie. Si l'authentification échoue auprès de tous les fournisseurs d'authentification disponibles, vous n'êtes pas authentifié.

## Modification des paramètres des fournisseurs de sécurité

Pour modifier les paramètres d'un fournisseur de sécurité, effectuez les étapes suivantes :

1. Démarrez l'outil Fournisseurs de sécurité.
2. Obtenez un verrou en écriture.
3. Sélectionnez le fournisseur de sécurité que vous souhaitez modifier.
4. Dans le volet Propriétés, cliquez sur le bouton **Modifier** situé à côté de la propriété que vous voulez modifier.
5. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

## Activation et désactivation des fournisseurs de sécurité

1. Obtenez un verrou en écriture.
2. Sélectionnez le fournisseur de sécurité à activer ou à désactiver.
  - Cochez la case **Activé** pour activer un fournisseur de sécurité désactivé.
  - Décochez la case **Activé** pour désactiver un fournisseur de sécurité.

Une fois désactivé, le nom du fournisseur est indisponible et déplacé à la fin de la liste des fournisseurs. Vous ne pouvez pas réorganiser les fournisseurs désactivés dans la liste des fournisseurs.

3. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

## Déplacement d'un fournisseur de sécurité dans l'ordre de traitement

MDM Hub traite les fournisseurs de sécurité dans l'ordre dans lequel ils apparaissent dans la liste de fournisseurs. Vous pouvez réorganiser l'ordre dans lequel les fournisseurs de sécurité s'affichent.

1. Démarrez l'outil Fournisseurs de sécurité.
2. Obtenez un verrou en écriture.
3. Pour déplacer un fournisseur vers le haut, cliquez dessus et sélectionnez **Monter un fournisseur**.  
L'outil Fournisseur de sécurité déplace le fournisseur vers le haut dans la liste des fournisseurs, puis actualise le panneau de navigation.
4. Pour déplacer un fournisseur vers le bas, cliquez dessus et sélectionnez **Descendre un fournisseur**.  
L'outil Fournisseur de sécurité déplace le fournisseur vers le bas dans la liste des fournisseurs, puis actualise le panneau de navigation.

## Propriétés du fournisseur

Le panneau Fournisseur contient les champs suivants :

### Nom

Nom du fournisseur de sécurité.

### Description

Description du fournisseur de sécurité.

### Type de fournisseur

Type de fournisseur de sécurité. Le statut peut prendre l'une des valeurs suivantes :

- Authentification
- Autorisation
- Profil utilisateur

### Fichier du fournisseur

Nom du fichier de fournisseur associé à ce fournisseur de sécurité, ou **Fournisseur interne** pour les fournisseurs internes.

### Activé

Indique si le fournisseur de sécurité est activé ou non. Un fournisseur de sécurité activé est sélectionné. Un fournisseur de sécurité désactivé n'est pas sélectionné. Notez que les fournisseurs internes ne peuvent pas être désactivés.

### Propriétés

Propriétés supplémentaires pour le fournisseur de sécurité, si elles ont été définies par celui-ci. Chaque propriété est une paire nom-valeur. Un fournisseur de sécurité peut requérir ou autoriser des propriétés uniques que vous pouvez spécifier ici.

## Ajout de propriétés de fournisseur

Pour ajouter des propriétés de fournisseur, suivez ces étapes :

1. Démarrez l'outil Fournisseurs de sécurité.
2. Obtenez un verrou en écriture.
3. Dans le panneau de navigation, sélectionnez le fournisseur d'authentification pour lequel vous souhaitez ajouter des propriétés.
4. Cliquez sur le bouton **Ajouter**.  
L'outil Fournisseurs de sécurité affiche la boîte de dialogue Ajouter une propriété de fournisseur.
5. Spécifiez le nom de la propriété.
6. Spécifiez la valeur à attribuer à cette propriété.
7. Cliquez sur **OK**.

## Modification des propriétés de fournisseur

Pour modifier une propriété de fournisseur existante, effectuez les étapes suivantes.

1. Démarrez l'outil Fournisseurs de sécurité.
2. Obtenez un verrou en écriture.
3. Dans le panneau de navigation, sélectionnez le fournisseur d'authentification pour lequel vous souhaitez modifier des propriétés.
4. Pour chaque propriété que vous souhaitez éditer, cliquez sur le bouton **Modifier** adjacent et spécifiez la nouvelle valeur.
5. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

# Fournisseurs personnalisés

Vous pouvez intégrer des classes de fournisseurs personnalisés dans le fichier JAR ou ZIP contenant le fichier de fournisseur.

Spécifiez les paramètres des fournisseurs personnalisés dans le fichier `providers.properties`. Déplacez ensuite le fichier dans le fichier JAR situé dans le répertoire META-INF. Les paramètres sont ensuite traduits par le chargeur pour obtenir les paramètres qui s'affichent dans la console Hub.

Un fichier `provider.properties` comporte les éléments suivants :

## **ProviderList**

Liste des noms de fournisseurs inclus, séparés par des virgules.

## **File-Description**

Description du package.

## **XXX-Provider-Name**

Nom d'affichage du fournisseur XXX.

## **XXX-Provider-Description**

Description du fournisseur XXX.

## **XXX-Provider-Type**

Type du fournisseur XXX. Les valeurs possibles sont `USER_PROFILE_PROVIDER`, `JAAS_LOGIN_MODULE` et `AUTHORIZATION_PROVIDER`.

## **XXX-Provider-Factory-Class-Name**

Classe d'implémentation du fournisseur, qui se trouve également dans le même fichier JAR ou ZIP.

## **XXX-Provider-Properties**

Liste des paires nom/valeur qui définissent les propriétés du fournisseur, séparés par des virgules.

**Remarque:** Le fichier d'archives du fournisseur doit contenir toutes les classes requises pour que le fournisseur personnalisé soit fonctionnel, en plus des ressources requises. Ces ressources sont spécifiques à votre implémentation.

## Exemple de fichier `providers.properties`

**Remarque:** Tous ces paramètres sont obligatoires, sauf pour `XXX-Provider-Properties`.

```
ProviderList=ProviderOne,ProviderTwo,ProviderThree,ProviderFour
ProviderOne-Provider-Name: Sample Role Based User Profile Provider
ProviderOne-Provider-Description: Sample User Profile Provider for roled-based management
ProviderOne-Provider-Type: USER_PROFILE_PROVIDER
ProviderOne-Provider-Factory-Class-Name:
com.siperian.sam.sample.userprofile.SampleRoleBasedUserProfileProviderFactory
ProviderOne-Provider-Properties: name1=value1,name2=value2
ProviderTwo-Provider-Name: Sample Login Module
ProviderTwo-Provider-Description: Sample Login Module
ProviderTwo-Provider-Type: JAAS_LOGIN_MODULE
ProviderTwo-Provider-Factory-Class-Name: com.siperian.sam.sample.authn.SampleLoginModule
ProviderTwo-Provider-Properties:
ProviderThree-Provider-Name: Sample Role Based Authorization Provider
ProviderThree-Provider-Description: Sample Role Based Authorization Provider
ProviderThree-Provider-Type: AUTHORIZATION_PROVIDER
ProviderThree-Provider-Factory-Class-Name:
com.siperian.sam.sample.authz.SampleAuthorizationProviderFactory
ProviderThree-Provider-Properties:
ProviderFour-Provider-Name: Sample Comprehensive User Profile Provider
```

```
ProviderFour-Provider-Description: Sample Comprehensive User Profile Provider
ProviderFour-Provider-Type: USER_PROFILE_PROVIDER
ProviderFour-Provider-Factory-Class-Name:
com.siperian.sam.sample.userprofile.SampleComprehensiveUserProfileProviderFactory
ProviderFour-Provider-Properties:
File-Description=The sample provider files
```

## Authentification externe

Vous pouvez utiliser l'authentification externe avec MDM Hub pour les utilisateurs via le service d'authentification et d'autorisation Java (JAAS).

MDM Hub fournit des modèles pour les types de normes d'authentification suivants :

- Lightweight Directory Access Protocol (LDAP) ;
- Microsoft Active Directory ;
- authentification de réseau à l'aide du protocole Kerberos ;

Ces modèles fournissent les paramètres, tels que les protocoles, les noms de serveur et les ports, qui sont requis pour ces normes d'authentification. Vous pouvez utiliser ces modèles pour ajouter un nouveau module de connexion avec les paramètres dont vous avez besoin. Pour plus d'informations sur ces normes d'authentification, consultez la documentation fournisseur concernée.

## Ajout d'un module de connexion

Pour configurer l'authentification externe dans MDM Hub, vous devez créer un module de connexion.

1. Démarrez l'outil Fournisseurs de sécurité.
2. Obtenez un verrou en écriture.
3. Cliquez avec le bouton droit de la souris sur Fournisseurs d'authentification (Modules de connexion) et sélectionnez **Ajouter un module de connexion**.

L'outil Fournisseurs de sécurité affiche la boîte de dialogue Ajouter un module de connexion.

4. Cliquez sur la flèche vers le bas et sélectionnez un modèle pour le module de connexion.

### **OpenLDAP-template**

Basé sur les propriétés d'authentification LDAP.

### **MicrosoftActiveDirectory-template**

Basé sur les propriétés d'authentification Active Directory.

### **Kerberos-template**

Basé sur les propriétés d'authentification Kerberos.

5. Cliquez sur **OK**.

L'outil Fournisseurs de sécurité ajoute le nouveau module de connexion à la liste.

6. Dans le volet Propriétés, cliquez sur le bouton **Modifier** situé à côté de la propriété que vous souhaitez modifier. Spécifiez les paramètres pour le type de module de connexion que vous voulez créer.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer vos modifications.

## Suppression d'un module de connexion

Vous pouvez supprimer un module de connexion si vous le souhaitez.

1. Démarrez l'outil Fournisseurs de sécurité.
2. Obtenez un verrou en écriture.
3. Dans le panneau de navigation, cliquez avec le bouton droit de la souris sur un module de connexion sous Fournisseurs d'authentification (Modules de connexion) et sélectionnez **Supprimer un module de connexion**.

L'outil Fournisseur de sécurité vous demande de confirmer la suppression.

4. Cliquez sur **Oui**.

L'outil Fournisseur de sécurité retire le module de connexion supprimé de la liste et actualise le panneau de navigation de gauche.

## CHAPITRE 6

# Niveau de sécurité de l'application

Ce chapitre comprend les rubriques suivantes :

- [Présentation de la sécurité au niveau de l'application, 48](#)
- [Informatica Data Director, 49](#)
- [Outil d'approvisionnement, 50](#)
- [ActiveVOS, 50](#)
- [Dynamic Data Masking, 51](#)
- [Configuration d'un canal WebLogic T3S sous Linux, 53](#)

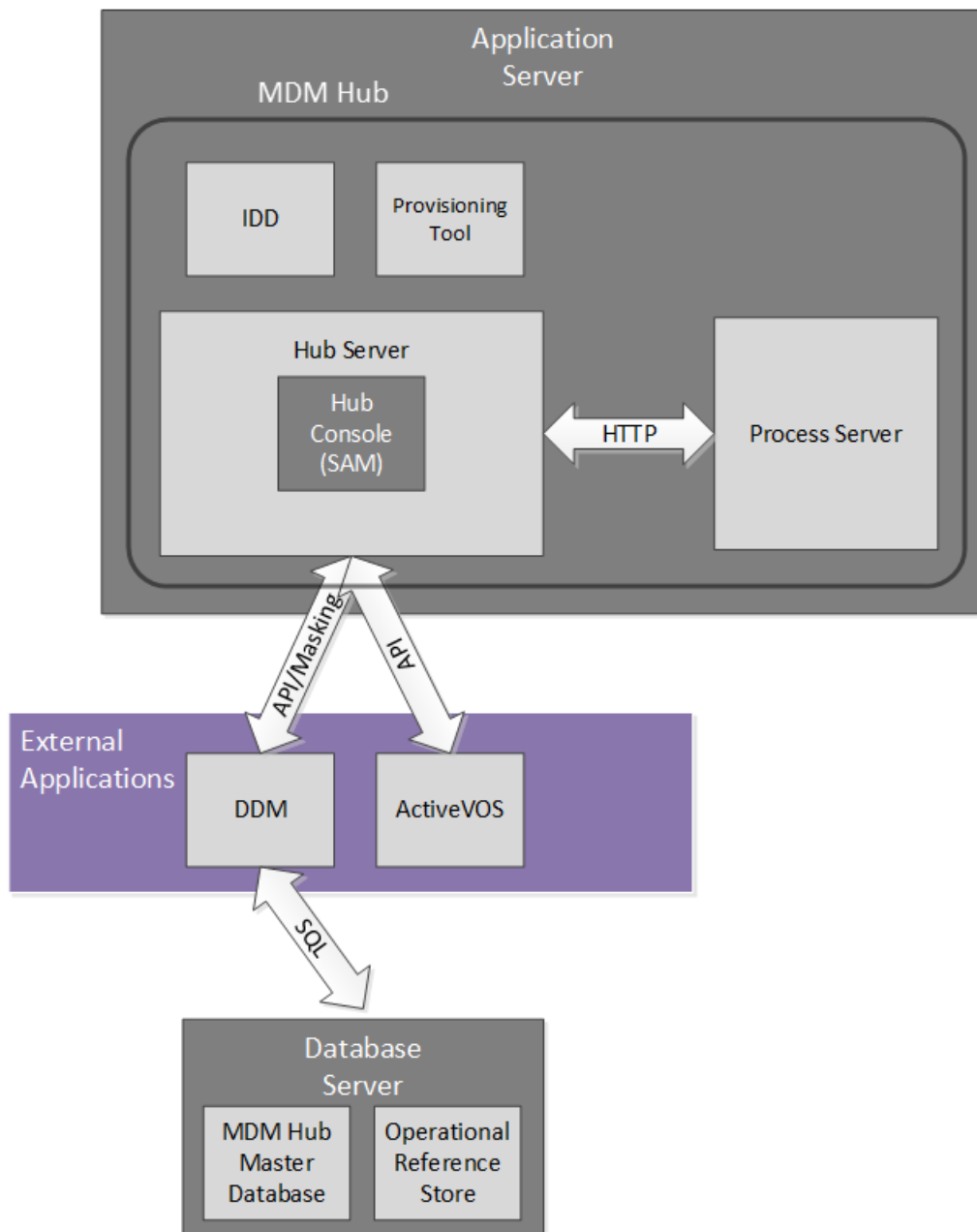
## Présentation de la sécurité au niveau de l'application

Le Gestionnaire d'accès de sécurité (GAS) est le module de sécurité de MDM Hub qui contrôle les informations d'identification et les rôles utilisateur. D'autres applications et composants d'une implémentation de MDM Hub disposent également de paramètres de sécurité permettant de vous assurer qu'ils communiquent avec MDM Hub en toute sécurité. Par exemple, vous pouvez configurer la sécurité au niveau des données pour Informatica Data Director.

Informatica effectue des tests de sécurité internes sur ses produits. Par exemple, Informatica utilise des applications de scan standard pour tester les vulnérabilités en matière de sécurité de ses produits, comme une attaque par injection de SQL. D'autres applications de sécurité Informatica utilisées conjointement avec le GAS ajoutent un niveau supplémentaire de sécurité à une implémentation de MDM Hub. Informatica Dynamic Data Masking (DDM) applique un masque aux données afin d'empêcher l'accès non autorisé aux informations sensibles. L'outil d'approvisionnement d'Informatica MDM et Informatica ActiveVOS ne sont pas des applications de sécurité, mais elles communiquent toujours de façon sécurisée avec MDM Hub.

L'image suivante montre un exemple d'implémentation de MDM Hub et la manière dont les composants se connectent les uns aux autres :





## Informatica Data Director

Informatica Data Director est une application de gouvernance de données Web pour MDM Hub. Lorsque vous configurez une application Data Director, les utilisateurs d'entreprise peuvent créer, gérer, utiliser et surveiller les données principales.

Informatica Data Director suit les dix premières recommandations de sécurité de la communauté Open Web Application Security Project (OWASP). Informatica utilise IBM Security AppScan pour tester les vulnérabilités en matière de sécurité telles qu'une attaque par injection de SQL. Les méthodes HTTP GET ou POST peuvent

récupérer des informations depuis IDD, mais les autres méthodes HTTP telles que DELETE ou PUT renvoient une erreur HTTP.

Lorsque vous configurez une application Data Director, vous pouvez organiser les tables du Stockage de référence opérationnelle dans des entités d'entreprise ou des domaines. Les deux approches permettent de regrouper les données associées que vous souhaitez traiter en tant qu'unité, comme par exemple toutes les données concernant un client. Les entités d'entreprise sont l'approche organisationnelle recommandée à partir de MDM Multidomaine version 10.1. Elles sont au cœur du framework Entity 360, qui englobe des services d'entité d'entreprise et des vues d'entité modernes.

Pour assurer la sécurité des données, une application Data Director utilise les rôles d'utilisateur et les privilèges de ressources qui sont définis sur le Stockage de référence opérationnelle. Rappelez-vous qu'un administrateur MDM utilise l'espace de travail Security Access Manager de Console Hub pour définir les privilèges de ressources de chaque rôle d'utilisateur. Dans une application Data Director, les utilisateurs peuvent effectuer les opérations qui sont autorisées par leur rôle d'utilisateur.

La sécurité peut présenter quelques différences car les entités d'entreprise et les domaines sont dérivés des privilèges de ressources de plusieurs manières. Toutefois, les deux approches répondent au même niveau de sécurité. Pour plus d'informations sur la sécurité des entités d'entreprise, consultez le *Guide de l'outil d'approvisionnement de MDM Multidomain*. Pour plus d'informations sur la configuration de la sécurité et la sécurité des données des domaines, consultez le *Guide d'implémentation de Data Director pour MDM Multidomain*.

## Outil d'approvisionnement

Utilisez l'outil d'approvisionnement pour créer des modèles d'entité d'entreprise basés sur les informations de schéma que vous avez définies dans un stockage de référence opérationnelle (Operational Reference Store - ORS). Le modèle d'entité d'entreprise est un composant de base du framework Entity 360 dans Data Director

Vous devez vous connecter à l'outil d'approvisionnement pour pouvoir configurer des entités d'entreprise.

Lorsque vous travaillez sur les fichiers de configuration, vous enregistrez vos modifications dans un espace de travail temporaire. L'outil d'approvisionnement n'applique pas les modifications tant que vous n'avez pas publié vos modifications. Si plusieurs utilisateurs modifient simultanément la configuration de l'entité d'entreprise pour un ORS, MDM Hub est mis à jour avec la dernière configuration publiée.

L'outil d'approvisionnement doit s'exécuter sur le même serveur d'applications que le serveur Hub.

Pour plus d'informations, consultez le *Guide de l'outil d'approvisionnement de MDM Multidomain*.

## ActiveVOS

Informatica ActiveVOS<sup>®</sup> est un outil de gestion des processus d'entreprise (BPM) qui vous permet d'automatiser les processus d'entreprise. Vous pouvez créer des modèles de processus intégrant des personnes, des processus et des systèmes afin d'augmenter l'efficacité de votre entreprise.

Grâce à ActiveVOS, vous pouvez vous assurer que les données d'entité mises à jour passent par un flux de travail d'approbation des modifications avant que les enregistrements mis à jour contribuent aux enregistrements Meilleure version de la vérité (MVV). Par exemple, un processus d'entreprise peut nécessiter

que les mises à jour de données clients soient vérifiées et approuvées par un gestionnaire expérimenté avant de devenir des données principales.

Pour prendre en charge un flux de travail d'approbation des modifications, MDM Hub et Data Director s'intègrent au serveur ActiveVOS. Les flux de travail MDM, les types de tâches et les rôles prédéfinis permettent aux composants de se synchroniser entre eux. Vous pouvez configurer votre implémentation de MDM de façon à travailler avec le serveur ActiveVOS intégré. Vous pouvez également exécuter une instance autonome d'ActiveVOS dans votre environnement.

Le serveur ActiveVOS intégré authentifie les demandes de Data Director et de MDM Hub par un principal spécifique qui est approuvé par MDM et par ActiveVOS. Ce principal est appelé l'utilisateur approuvé. L'administrateur système crée les justificatifs d'identité et les rôles de l'utilisateur approuvé dans le serveur d'applications.

Le serveur ActiveVOS doit s'exécuter sur le même serveur d'applications que MDM Hub. Pour plus d'informations, consultez le *Guide de configuration de MDM Multidomain*.

## Dynamic Data Masking

Informatica Dynamic Data Masking est un produit visant à assurer la sécurité des données, qui s'exécute entre un client et une base de données pour éviter tout accès non autorisé à des informations sensibles. Dynamic Data Masking intercepte les demandes envoyées à la base de données et applique un masque aux données avant d'envoyer les résultats de la demande au client.

Dynamic Data Masking apporte un niveau supplémentaire de sécurité des données aux bases de données gérées par MDM Hub. Utilisez la console de gestion de Dynamic Data Masking pour configurer la connexion de Dynamic Data Masking au Stockage de référence opérationnelle et définir des règles de masquage pour les données. Vous configurez la connexion de MDM Hub à Dynamic Data Masking lorsque vous enregistrez un Stockage de référence opérationnelle.

Le programme d'installation de MDM n'installe pas Dynamic Data Masking avec MDM Hub. Vous devez installer Dynamic Data Masking séparément. Pour plus d'informations sur l'installation de Dynamic Data Masking, consultez la documentation Dynamic Data Masking.

**Remarque:** Pour utiliser Dynamic Data Masking dans MDM Hub, vous devez avoir installé Dynamic Data Masking 9.6.0 ainsi que le correcteur de bogues en urgence 14590. Les versions antérieures de Dynamic Data Masking ne sont pas compatibles avec MDM Hub.

## Intégration de Dynamic Data Masking à MDM Hub

Une fois Dynamic Data Masking correctement installé et configuré, vous pouvez intégrer Dynamic Data Masking à MDM Hub.

Les étapes suivantes décrivent le processus d'intégration à suivre :

1. Dans la console de gestion de Dynamic Data Masking, créez un service Dynamic Data Masking. Configurez le numéro de port d'écoute de manière à le faire correspondre au numéro de port sur lequel le client envoie des demandes à la base de données.
2. Définissez les propriétés de connexion de la base de données sur laquelle vous souhaitez établir le masquage des données.

3. Créez une règle de connexion. Configurez la règle de manière à identifier les demandes de la base de données qui doivent être masquées. Assignez une base de données et un ensemble de règles de sécurité à l'ensemble de règles de connexion.
4. Créez un ensemble de règles de sécurité. Définissez les règles de masquage des données renvoyées à MDM Hub.
5. Dans la Console Hub, configurez la connexion à Dynamic Data Masking.

Lorsque vous exécutez des processus pour le Stockage de référence opérationnelle, Dynamic Data Masking applique les règles à la base de données avant qu'elle ne renvoie les données à MDM Hub.

**Remarque:** Si vous n'ajoutez pas la connexion de Dynamic Data Masking à Stockage de référence opérationnelle, MDM Hub contourne toutes les règles de Dynamic Data Masking que vous définissez.

Pour plus d'informations sur la configuration de Dynamic Data Masking, consultez le *Guide de l'administrateur d'Informatica Dynamic Data Masking*.

## Bonnes pratiques recommandées de Dynamic Data Masking pour MDM Hub

Vous pouvez utiliser Dynamic Data Masking efficacement dans MDM Hub en suivant les bonnes pratiques recommandées.

### Bonne pratique pour créer des règles Dynamic Data Masking dans l'éditeur de règles

Dynamic Data Masking évalue les règles dans l'éditeur de règles de haut en bas. Par conséquent, si vous créez des règles de non-masquage, vous devez les placer au-dessus de toutes les règles de masquage que vous créez pour qu'elles puissent être appliquées.

### Bonne pratique pour permettre aux utilisateurs d'afficher des données non masquées

Dynamic Data Masking ne masque pas les données dans la base de données. Lorsque vous affichez des données dans MDM Hub, celles-ci apparaissent masquées. Utilisez l'instruction Créer dans Dynamic Data Masking pour accorder aux utilisateurs des privilèges leur permettant d'afficher les données non masquées.

### Bonne pratique pour bloquer des utilisateurs

Pour empêcher des utilisateurs d'ajouter un enregistrement pour lequel le masquage est appliqué, vous devez créer une règle distincte pour chaque objet de base concerné. Définissez un rapprochement texte `%INSERT%<BO_NAME>%<ROLE_NAME>%` et l'action de traitement de l'instruction Bloquer.

### Bonne pratique pour permettre aux utilisateurs de mettre à jour des données masquées

Par défaut, le moteur de Dynamic Data Masking empêche les utilisateurs de modifier des tables contenant des données masquées. Si vous souhaitez mettre à jour des données masquées dans MDM Hub, vous pouvez créer une règle dans l'éditeur de règles de Dynamic Data Masking afin d'autoriser un utilisateur à mettre à jour les colonnes masquées.

### Bonne pratique pour créer des règles avec un indicateur MDM\_SYSTEM

Dans MDM Hub, l'indicateur MDM\_SYSTEM de l'utilisateur est un indicateur interne pour les appels système. MDM\_SYSTEM ne s'affiche pas dans la liste des rôles dans la Console Hub. Dynamic Data Masking applique le masquage en fonction des rôles de MDM Hub assignés à un utilisateur. Lorsque vous créez des règles Dynamic Data Masking dans l'éditeur de règles, ne créez pas de règles pour l'indicateur MDM\_SYSTEM seul. Vous devez combiner MDM\_SYSTEM avec un nom d'utilisateur ou des rôles appartenant à un utilisateur. Vous pouvez combiner l'indicateur MDM\_SYSTEM avec une autre règle afin de créer des règles plus précises dans Dynamic Data Masking.

## Configuration de Dynamic Data Masking pour un stockage de référence opérationnelle (Operational Reference Store - ORS)

Vous configurez la connexion de Dynamic Data Masking à MDM Hub lorsque vous enregistrez un Stockage de référence opérationnelle via la Console Hub.

1. Démarrez la Console Hub.

La boîte de dialogue **Modifier la base de données** s'affiche.

2. Sélectionnez la base de données principale de MDM Hub et cliquez sur **Connecter**.

3. Dans l'espace de travail de configuration, lancez l'outil **Bases de données**.

4. Obtenez un verrou en écriture.

5. Cliquez sur le bouton **Enregistrer la base de données**.

L'**Assistant de connexion à Informatica MDM Hub** s'affiche et vous invite à sélectionner le type de base de données.

6. Sélectionnez le type de base de données et cliquez sur **Suivant**.

7. Configurez les propriétés de connexion de la base de données.

8. Dans le champ **Port**, le port que vous saisissez doit correspondre au port du service d'écoute de Dynamic Data Masking pour la base de données.

9. Dans le champ **URL de connexion DDM**, saisissez l'URL du serveur de Dynamic Data Masking.

10. Cliquez sur **Terminer**.

La boîte de dialogue **Enregistrement de la base de données** s'affiche.

11. Cliquez sur **OK**.

MDM Hub enregistre le Stockage de référence opérationnelle.

12. Sélectionnez le Stockage de référence opérationnelle que vous avez enregistré et cliquez sur le bouton **Tester la connexion de la base de données** pour tester les paramètres de la base de données.

Si vous utilisez WebSphere, redémarrez WebSphere avant de tester la connexion à la base de données.

La boîte de dialogue Tester la base de données affiche le résultat du test de connexion à la base de données.

13. Cliquez sur **OK**.

Dynamic Data Masking se connecte au Stockage de référence opérationnelle que vous avez enregistré.

## Configuration d'un canal WebLogic T3S sous Linux

WebLogic T3S est un protocole SSL que vous pouvez configurer pour MDM Hub.

Les étapes suivantes supposent que vous savez comment créer et utiliser un magasin de clés, configurer une instance de serveur pour SSL et créer un canal. Pour plus d'informations, consultez la documentation WebLogic.

1. Avant de commencer, vous devez disposer d'un magasin de clés que vous utiliserez à des fins d'identité.
2. Dans la console d'administration de WebLogic, accédez à l'instance de serveur que vous utilisez avec MDM, puis configurez SSL avec les propriétés suivantes :

- **Emplacement d'approbation et d'identité = Magasin de clés**

- **Emplacement de clé privée** = à partir du magasin de clés d'identité personnalisé
  - **Alias de clé privée** = <alias défini dans le magasin de clés>
  - **Phrase secrète de clé privée** = <phrase secrète définie dans le magasin de clés>
  - **Emplacement de certificat** = à partir du magasin de clés d'identités personnalisé
  - **Autorités de certificat approuvées** = à partir du magasin de clés d'approbation Java standard
3. Ouvrez une fenêtre d'invite de commande d'administrateur (cmd), puis utilisez la commande `keytool` pour importer le magasin de clés dans les répertoires JDK et JRE sous `lib/security/cacerts`. L'exemple de code suivant montre la syntaxe :
- ```
keytool -import -alias <SSL Private Key Alias> -keystore "<JDK installation
directory>/jre/lib/security/cacerts" -file "/data/oracle/Oracle/Middleware/
Oracle_Home/user_projects/domains/base_domain/servers/<WebLogic server instance>/
keystores/wls12c_server.cer" -v

keytool -import -alias <SSL Private Key Alias> -keystore "<JRE installation
directory>/lib/security/cacerts" -file "/data/oracle/Oracle/Middleware/Oracle_Home/
user_projects/domains/base_domain/servers/<WebLogic server instance>/keystores/
wls12c_server.cer" -v
```
- Remarque:** Si vous avez besoin d'aide sur la commande `keytool`, consultez la documentation Java.
4. Accédez au fichier `<WebLogic domain>/bin/startWebLogic.sh`, puis définissez l'option Java suivante :
- ```
-Doracle.jdbc.J2EE13Compliant=true
```
5. Dans la console d'administration de WebLogic, créez un canal T3S qui correspond à la configuration SSL. Définissez les propriétés suivantes :
- **Nom** = <nom du canal>
  - **Protocole** = t3s
  - **Adresse d'écoute** = <nom d'hôte défini dans le magasin de clés>
  - **Port d'écoute** = <port défini dans le magasin de clés>
  - Sélectionnez **Tunneling activé**
  - Sélectionnez **SSL bidirectionnel**
  - Vérifiez que l'option **Alias de clé privée du serveur** affiche l'alias spécifié lors de la configuration de SSL.
6. Enregistrez le canal, puis vérifiez qu'il s'affiche bien dans la liste des canaux du réseau.
7. Si vous utilisez Informatica Data Director avec des vues Entity 360, accédez au fichier `<WebLogic domain>/bin/setDomainEnv.sh`, puis définissez les options MDM suivantes :
- `e360.mdm.protocol=t3s`
  - `e360.mdm.host=<T3S channel Listen Address>`
  - `e360.mdm.port=<T3S channel Listen Port>`
8. Redémarrez WebLogic.
9. Vérifiez que le canal fonctionne en lui envoyant une requête PING.
- ```
java weblogic.Admin -url t3s://<T3S Channel Listen Address>:<T3S Channel Listen
Port> -username <WebLogic username> -password <WebLogic password> PING
```
10. Vous pouvez maintenant lancer la console Hub à l'aide de HTTPS et du port sécurisé.
- ```
https://<T3S Channel Listen Address>:<T3S Channel Listen Port>/cmx/
```

## CHAPITRE 7

# Authentification basée sur un certificat

Ce chapitre comprend les rubriques suivantes :

- [Authentification basée sur un certificat Présentation, 55](#)
- [Authentification basée sur un certificat et clients externes, 56](#)
- [Applications approuvées, 56](#)
- [Gestion des certificats et des clés , 57](#)

## Authentification basée sur un certificat Présentation

MDM Hub utilise un mécanisme d'authentification par certificat pour sécuriser la communication entre les composants de MDM Hub et les applications approuvées. Le mécanisme d'authentification est également pris en charge pour les API du Framework d'intégration des services (SIF) et des services d'entité d'entreprise.

Par défaut, le module de connexion du certificat traite les applications Informatica, telles que Data Director, comme des applications approuvées. Pour utiliser l'authentification par certificat pour les applications externes, vous devez enregistrer les applications comme étant approuvées.

Une application externe enregistrée comme application approuvée transmet à MDM Hub une concaténation du nom de l'application et du nom d'utilisateur. Par exemple, `IDD/admin`. L'application externe doit également transmettre une charge utile de sécurité.

# Authentification basée sur un certificat et clients externes

Les clients externes à MDM Hub, comme l'API SiperianClient, peuvent envoyer des demandes à l'aide de l'authentification par nom d'utilisateur et mot de passe. Toutefois, les clients externes peuvent également utiliser l'authentification par certificat.

Pour configurer l'authentification basée sur un certificat pour un client externe à MDM Hub, effectuez les étapes suivantes :

1. Dans la console Hub, enregistrez le certificat public pour les utilisateurs associés au client externe.
2. Utilisez le client externe pour déclencher une demande.

## Applications approuvées

Dans MDM Hub, une application approuvée est un type d'utilisateur appelé utilisateur d'application qui peut exécuter des requêtes pour le compte de n'importe quel utilisateur régulier de MDM Hub, y compris l'utilisateur Admin. Les applications approuvées appartiennent au framework d'applications approuvées de MDM Hub.

Les applications approuvées sont définies dans la colonne APPLICATION\_IND de la table C\_REPOS\_USER, sous le schéma CMX\_SYSTEM. Chaque application approuvée est enregistrée en tant qu'utilisateur d'application dans la console Hub. Par défaut, MDM Hub traite les applications Informatica largement utilisées dans les implémentations de MDM Hub comme des applications approuvées. Par exemple, Informatica Data Director et ActiveVOS sont des applications approuvées.

Par défaut, un ensemble de clés publiques et privées est configuré dans chaque application approuvée. MDM Hub authentifie la demande d'une application approuvée de l'une des manières suivantes :

- Authentification du justificatif d'identité de l'utilisateur
- Authentification basée sur un certificat

Pour configurer une autre application comme application approuvée, consultez ["Ajout de comptes utilisateur" à la page 30](#).

## Ajout d'une application externe en tant qu'application approuvée

Vous pouvez également ajouter des applications externes au framework d'applications approuvées de MDM Hub.

1. Dans la console Hub, ajoutez un compte d'utilisateur pour l'utilisateur de l'application qui correspond à l'application externe.

**Remarque:** Assurez-vous de cocher la case **Utilisateur d'application** dans la boîte de dialogue **Ajouter un utilisateur**. Veillez également à n'utiliser que des caractères minuscules pour le nom du compte utilisateur.

2. Enregistrez un certificat public avec le compte utilisateur d'application.



3. Utilisez l'application externe pour déclencher une demande.

**Remarque:** Si vous voulez utiliser l'authentification basée sur un certificat, définissez le nom de la demande comme suit : <nom de l'application>/<nom de l'utilisateur>. Le <nom de l'application> doit être identique à celui utilisé lors de l'étape [1](#). Le <nom de l'utilisateur> est le nom de l'utilisateur MDM Hub qui déclenche la demande.

## Gestion des certificats et des clés

MDM Hub utilise une authentification par certificat. Vous devez conserver le certificat et les paires de clés privées pour chaque utilisateur à un endroit sûr.

Par défaut, MDM Hub conserve les clés privées et les certificats dans l'emplacement suivant :

```
<répertoire d'installation de MDM Hub>/server/resources/certificates
```

Vous pouvez également configurer un fournisseur de certificat personnalisé lors de l'installation de Multidomain MDM.

Pour implémenter un fournisseur de certificat personnalisé, vous devez implémenter une interface `PKIUtil.java` dans le fichier `siperian-server-pkiutil.jar`, situé dans le répertoire suivant :

```
<répertoire d'installation de MDM Hub>/hub/server/lib/pkiutils
```

Si vous utilisez un fournisseur de certificat personnalisé, vous devez gérer le fichier keystore et les certificats publics utilisés par l'implémentation `PKIUtil`.

**Remarque:** Si vous devez modifier le fournisseur de certificat, contactez le support client international Informatica pour demander un utilitaire de configuration de la sécurité.

### LIENS CONNEXES :

- ["Utilitaire de configuration de la sécurité" à la page 57](#)

## Utilitaire de configuration de la sécurité

Vous pouvez utiliser l'utilitaire de configuration de la sécurité pour gérer certains paramètres de sécurité dans l'implémentation de MDM Hub.

Vous pouvez utiliser l'utilitaire de configuration de la sécurité pour effectuer les tâches suivantes :

- Modifier le fournisseur de certificat utilisé pour l'authentification.
- Réinitialiser le mot de passe d'un utilisateur dans MDM Hub.
- Modifier l'algorithme de hachage utilisé pour le hachage de mot de passe.
- Modifier la clé de hachage client utilisée pour créer l'algorithme de hachage.

**Remarque:** Pour obtenir l'utilitaire de configuration de sécurité, contactez le support client international Informatica.

## CHAPITRE 8

# Hachage de mot de passe

Ce chapitre comprend les rubriques suivantes :

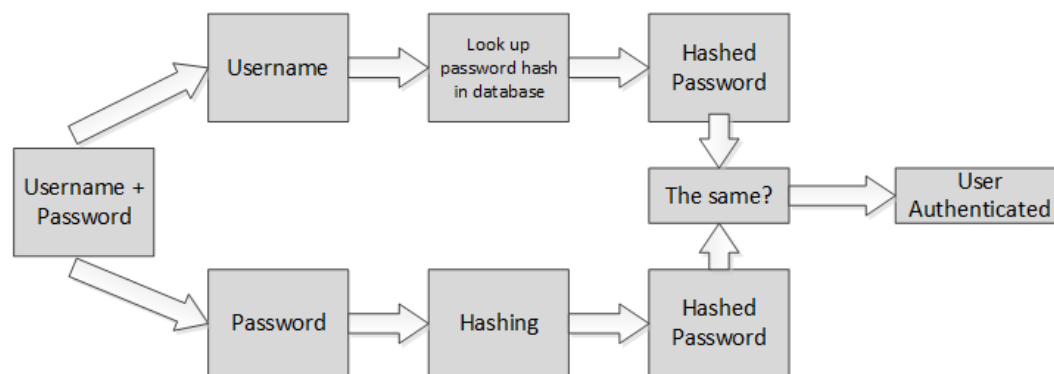
- [Présentation du hachage de mot de passe, 58](#)
- [Options de hachage de mot de passe, 59](#)
- [Processus de réinitialisation de mot de passe , 59](#)
- [Utilitaire de configuration de la sécurité, 60](#)
- [Dépannage, 60](#)

## Présentation du hachage de mot de passe

Le hachage de mot de passe permet de chiffrer de manière irréversible les mots de passe via une fonction de hachage cryptographique. MDM Hub utilise une méthode de hachage de mot de passe pour protéger les mots de passe des utilisateurs et s'assurer qu'ils ne sont jamais stockés en texte clair dans une base de données. L'administrateur MDM Hub configure les options de hachage de mot de passe, telles que l'algorithme et les clés de hachage du client, lors de l'installation du serveur Hub.

Informatica fournit un utilitaire de configuration de sécurité pour gérer certains paramètres de sécurité dans une implémentation de MDM Hub, notamment la modification de l'algorithme de hachage ou la réinitialisation des mots de passe des utilisateurs de MDM Hub.

L'image suivante montre l'authentification du mot de passe de l'utilisateur par MDM Hub :



## LIENS CONNEXES :

- [“Utilitaire de configuration de la sécurité” à la page 57](#)

# Options de hachage de mot de passe

Lors de l'installation du serveur Hub, vous pouvez configurer les options de hachage de mot de passe suivantes :

- Spécifiez si vous souhaitez créer une clé de hachage personnalisée dans le cadre de l'algorithme de hachage
- Spécifiez si vous voulez utiliser l'algorithme de hachage SHA3 par défaut ou créer un algorithme de hachage personnalisé
- Spécifiez si vous voulez utiliser le fournisseur de certificat par défaut ou utiliser un fournisseur de certificat personnalisé

Avec les deux algorithmes de hachage, SHA3 et personnalisé, les mots de passe des utilisateurs de MDM Hub sont chiffrés de manière irréversible et ne sont jamais stockés en texte clair dans une base de données. Indépendamment de l'algorithme de hachage utilisé, l'algorithme comprend les composants suivants :

- une fonction de hachage ;
- une valeur salt ;
- une clé de hachage ou une valeur pepper facultative, qui est définie lors de l'installation de MDM Hub. L'administrateur de MDM Hub est tenu de générer cette clé et de la stocker de manière sécurisée.

Si vous créez une valeur pepper, Informatica vous recommande d'utiliser une clé contenant une séquence de 32 caractères hexadécimaux sans délimiteur.

**Important:** Protégez la confidentialité de la clé de hachage pour éviter le risque de violation de données. En cas de vol de la clé de hachage, vous devez réinitialiser tous les mots de passe.

L'algorithme de hachage de mot de passe et l'implémentation sous-jacente de l'algorithme sont stockés dans les propriétés du serveur Hub. Pour plus d'informations sur les propriétés du serveur Hub, consultez le *Guide de configuration de MDM Multidomain*.

## Algorithme de hachage personnalisé

# Processus de réinitialisation de mot de passe

Si vous oubliez votre mot de passe ou si vous pensez que la sécurité des composants secrets de votre algorithme de hachage est compromise, vous pouvez réinitialiser votre mot de passe. Pour réinitialiser votre mot de passe, contactez le support client international Informatica.

Lorsque vous réinitialisez votre mot de passe, vous recevez un courriel avec un mot de passe temporaire. Utilisez ce mot de passe pour vous connecter à MDM Hub, puis remplacez-le par un mot de passe personnel. Vous pouvez modifier votre mot de passe à partir de la console Hub ou via Informatica Data Director.

# Utilitaire de configuration de la sécurité

Vous pouvez utiliser l'utilitaire de configuration de la sécurité pour gérer certains paramètres de sécurité dans l'implémentation de MDM Hub.

Vous pouvez utiliser l'utilitaire de configuration de la sécurité pour effectuer les tâches suivantes :

- Modifier le fournisseur de certificat utilisé pour l'authentification.
- Réinitialiser le mot de passe d'un utilisateur dans MDM Hub.
- Modifier l'algorithme de hachage utilisé pour le hachage de mot de passe.
- Modifier la clé de hachage client utilisée pour créer l'algorithme de hachage.

**Remarque:** Pour obtenir l'utilitaire de configuration de sécurité, contactez le support client international Informatica.

## Dépannage

Si vous rencontrez des problèmes, utilisez les informations suivantes pour les résoudre.

### Les utilisateurs de MDM Hub ne peuvent pas se connecter

Si MDM Hub recrée le schéma CMX\_SYSTEM après l'installation du serveur Hub, MDM Hub ne peut pas reconnaître les mots de passe hachés. Par conséquent, les utilisateurs ne peuvent pas se connecter à MDM Hub.

Pour résoudre ce problème, réexécutez le script `postInstallSetup` manuellement. Ce script garantit un nouveau hachage des mots de passe des utilisateurs de MDM Hub, qui peuvent donc se connecter.

Pour plus d'informations sur le script `postInstallSetup`, consultez le *Guide d'installation de MDM Multidomain*.

# ANNEXE A

## Glossaire

### **authentification**

Processus de vérification d'identité d'un utilisateur pour s'assurer qu'il est celui qu'il prétend être. Dans Informatica MDM Hub, les utilisateurs sont authentifiés d'après leurs justificatifs d'identité fournis : nom d'utilisateur/mot de passe, charge de sécurité ou une combinaison des deux. Informatica MDM Hub fournit un mécanisme d'authentification interne et prend aussi en charge l'authentification des utilisateurs à l'aide de fournisseurs d'authentification de tierces-parties.

### **autorisation**

Processus permettant de déterminer si un utilisateur dispose de suffisamment de privilèges pour accéder à une ressource d'Informatica MDM Hub. Dans Informatica MDM Hub, les privilèges de ressources sont alloués aux rôles. Les rôles sont assignés aux utilisateurs et aux groupes d'utilisateurs. Les privilèges de ressources d'un utilisateur sont déterminés par les rôles qui lui sont assignés, ainsi que par les rôles assignés aux groupes d'utilisateurs auxquels l'utilisateur appartient.

### **base de données**

Collecte organisée de données dans le stockage Hub. Informatica MDM Hub prend en charge deux types de bases de données : une base de données principale et un Operational Reference Store (ORS).

### **charge de sécurité**

Données binaires brutes fournies à une demande d'opération du MDM Hub contenant des données supplémentaires requises pour d'autres authentifications ou autorisations.

### **Console Hub**

Informatica MDM Hub interface utilisateur qui comprend un ensemble d'outils pour les administrateurs et les gestionnaires de données. Chaque outil permet aux utilisateurs d'effectuer une action spécifique, ou un ensemble d'actions connexes, tels que la construction du modèle de données, l'exécution de tâches de lots, la configuration du flux de données, la configuration de l'accès externes des applications aux ressources Informatica MDM Hub, et d'autres configurations du système et tâches de fonctionnement.

### **Dynamic Data Masking**

Produit de sécurité des données qui fonctionne entre un client et une base de données pour éviter tout accès non autorisé aux informations sensibles. Dynamic Data Masking intercepte les demandes envoyées à la base de données et leur applique des règles de masquage des données pour masquer les données avant leur renvoi au client.

## **espace de travail**

Dans la Console Hub, un mécanisme permettant de regrouper des outils semblables. Un espace de travail est un ensemble logique d'outils associés. Par exemple, l'espace de travail de modèle contient des outils pour la modélisation des données, tels que Schéma, Requêtes, Packages et Mappings.

## **Espace de travail de configuration**

Inclut des outils permettant de configurer différents objets du MDM Hub, notamment le Stockage de référence opérationnelle, les utilisateurs, la sécurité, les files d'attente de messages et la validation des métadonnées.

## **Espace de travail du Gestionnaire d'accès de sécurité**

Comprend des outils de gestion des utilisateurs, groupes, ressources et rôles.

## **fournisseur**

Voir [fournisseur de sécurité à la page 62](#).

## **fournisseur de sécurité**

Application tierce fournissant des services de sécurité (authentification, autorisation et services de profil utilisateur) pour les utilisateurs accédant à Informatica MDM Hub.

## **Gestionnaire d'accès de sécurité (GAS)**

Le gestionnaire d'accès de sécurité est le module de sécurité pour la protection des ressources du MDM Hub contre les accès non autorisés. Lors de l'exécution, le gestionnaire d'accès de sécurité applique les décisions de stratégie de sécurité de votre organisation à votre implémentation de MDM Hub et gère l'authentification et les autorisations d'accès des utilisateurs conformément à votre configuration de la sécurité.

## **Gestionnaire de données**

Outil utilisé pour examiner les résultats de toutes les fusions (y compris les fusions-automatique) et corriger le contenu des données si nécessaire. Il vous offre une vue sur la traçabilité des données pour chaque enregistrement d'objet de base. Le gestionnaire de données vous permet également d'annuler la fusion des enregistrements précédemment fusionnés, et d'afficher différents types d'historiques pour chaque enregistrement consolidé.

Utilisez l'outil Gestionnaire de données pour rechercher des enregistrements, afficher leurs références croisées, annuler la fusion d'enregistrements, annuler la liaison d'enregistrements, voir des enregistrements de l'historique, créer de nouveaux enregistrements, éditer les enregistrements, et remplacer les paramètres d'approbation. Le gestionnaire de données affiche tous les enregistrements qui répondent aux critères de recherche que vous définissez.

## **Gestionnaire de hiérarchies**

Le Gestionnaire de hiérarchies permet aux utilisateurs de gérer les données de hiérarchie associées aux enregistrements gérés dans le MDM Hub. Pour plus d'informations, consultez le *Guide de configuration de MDM Multidomain* et le *Guide du Gestionnaire de données de MDM Multidomain*.

## **gestionnaire des données**

Informatica MDM Hub utilisateur ayant pour responsabilité première la qualité des données. Les gestionnaires de données peuvent accéder à Informatica MDM Hub par le Console Hub, et utiliser les outils Informatica MDM Hub pour configurer les objets dans le Stockage Hub.

## **groupe de lots**

Un ensemble de tâches de lot individuelles (par exemple Activation de données, Chargement et Correspondance) pouvant être exécutées à l'aide d'une seule commande. Chaque tâche de lot dans un groupe peut être exécutée de façon séquentielle ou en parallèle avec d'autres tâches.

## **hiérarchie**

Dans le Gestionnaire de hiérarchie, un ensemble de types de relations. Ces types de relations ne sont pas classés en fonction de la place des entités de la hiérarchie, ils ne sont pas non plus nécessairement liés les uns aux autres. Ce sont simplement des types de relations regroupés pour faciliter la classification et l'identification.

## **Kerberos**

Protocole d'authentification de réseau informatique permettant aux nœuds qui communiquent sur un réseau non sécurisé de s'identifier mutuellement de manière sécurisée. Le Massachusetts Institute of Technology, qui a élaboré ce protocole, offre une implémentation gratuite de Kerberos.

## **métadonnées**

Données utilisées pour décrire d'autres données. Dans Informatica MDM Hub, les métadonnées sont utilisées pour décrire le schéma (modèle de données) utilisé dans votre implémentation d'Informatica MDM Hub, avec les paramètres de configuration connexes.

## **objet de base**

Table contenant les informations sur une entité concernant votre entreprise, comme un client ou un compte.

## **Operational Reference Store (ORS)**

Base de données qui contient les données principales et les règles qui agissent sur les données principales. Les règles incluent les règles pour le traitement des données principales, les règles de gestion de l'ensemble des objets de données principales et les règles de traitement de la logique auxiliaire que MDM Hub utilise pour définir la meilleure version de la vérité. Une configuration MDM Hub peut avoir un ou plusieurs stockages de référence opérationnelle. Le nom par défaut d'un ORS est CMX\_ORS.

## **package**

Un *package* est une vue publique d'une ou plusieurs tables sous-jacentes dans Informatica MDM Hub. Les packages représentent des sous-ensembles de colonnes de ces tables et de toute autre table jointe à ces tables. Un package est basé sur une requête. La requête sous-jacente peut sélectionner un sous-ensemble d'enregistrements de la table ou d'un autre package.

## **points de décision stratégique (policy decision points - PDP)**

Points de contrôle de sécurité spécifiques qui authentifient l'identité de l'utilisateur et accordent l'accès utilisateur aux ressources du MDM Hub.

## **points d'application de stratégie (policy enforcement points - PEP)**

Points de contrôle de sécurité spécifiques qui appliquent, pendant l'exécution, des stratégies de sécurité pour les demandes d'authentification et d'autorisation.

## privilège

Autorisation d'accès à une ressource de MDM Hub. Avec l'autorisation interne de MDM Hub, chaque rôle se voit affecter l'un des privilèges suivants.

Privilège	Permet à l'utilisateur de...
READ	Visualiser des données.
CREATE	Créer des enregistrements de données dans le stockage Hub.
UPDATE	Mettre à jour les enregistrements de données dans le stockage Hub.
MERGE	Fusionner des données et annuler la fusion.
EXECUTE	Exécuter les fonctions de nettoyage et les groupes de lots.
DELETE	Supprimer des enregistrements de données dans le stockage Hub.

Les privilèges déterminent l'accès des utilisateurs d'applications externes aux ressources de MDM Hub. Par exemple, un rôle peut être configuré pour avoir des privilèges READ, CREATE, UPDATE et MERGE sur des packages et des colonnes de package spécifiques. Ces privilèges ne sont pas appliqués lorsque vous utilisez la console Hub, bien que les paramètres affectent toujours son utilisation dans une certaine mesure.

## profil

Dans le Gestionnaire de hiérarchies, indique les zones et enregistrements que peut afficher, modifier ou ajouter un utilisateur du Gestionnaire de hiérarchies. Par exemple, un profil peut autoriser un accès complet en lecture/écriture à toutes les entités et relations, tandis qu'un autre profil sera en lecture seule (aucune opération d'ajout ou de modification n'est autorisée).

## ressource privée

Ressource d'Informatica MDM Hub masquée dans l'outil Rôles, empêchant ainsi son accès via des opérations SIF (Services Integration Framework). Lorsque vous ajoutez une nouvelle ressource dans la console Hub (telle qu'un nouvel objet de base), par défaut elle est désignée comme une ressource PRIVATE.

## rôle

Définit un ensemble de privilèges pour accéder à des ressources sécurisées de Informatica MDM Hub.

## sécurité

Capacité à protéger la confidentialité des informations, la confidentialité et l'intégrité des données en les protégeant contre tout accès non autorisé, et toute altération des données ou d'autres ressources dans votre implémentation de Informatica MDM Hub.

## Serveur Hub

Un composant d'exécution dans la couche médiane (serveur d'applications) utilisé pour des services essentiels et communs, incluant l'accès, la sécurité et la gestion de session.

## Stockage Hub

Dans une implémentation d'Informatica MDM Hub, la base de données qui contient la base de données principale et une ou plusieurs bases de données d'Operational Reference Store (ORS).



**stratégie des mots de passe**

Spécifie les caractéristiques de mot de passe des comptes utilisateur de Informatica MDM Hub, telles que la longueur du mot de passe, l'expiration, les paramètres de connexion, la réutilisation du mot de passe et autres exigences. Vous pouvez définir une stratégie de mot de passe globale pour tous les comptes utilisateur dans une implémentation de Informatica MDM Hub, et vous pouvez remplacer ces paramètres pour des utilisateurs individuels.

**verrou en écriture**

Dans la Console Hub, un verrou qui est requis pour apporter des modifications au schéma sous-jacent. Tous les outils du gestionnaire non associés aux données (sauf les outils de sécurité de Stockage de référence opérationnelle) sont en mode lecture seule à moins de vous procurer un verrou en écriture. Les verrous en écriture permettent d'autoriser plusieurs simultanés à apporter des modifications au schéma simultanément.

# INDEX

## A

authentification  
à propos de l'authentification [11](#)  
authentification de répertoire externe [11](#)  
authentification interne [11](#)  
fournisseurs d'authentification externe [11](#)  
autorisation  
à propos de l'autorisation [12](#)  
autorisation externe [12](#)  
autorisation interne [12](#)

## B

bases de données  
accès utilisateur [32](#)

## D

dépannage  
hachage de mot de passe [60](#)  
Dynamic Data Masking  
présentation [10](#)

## F

fichier providers.properties  
exemple [45](#)  
fichiers de fournisseur de sécurité  
à propos des fichiers de fournisseur de sécurité [40](#)  
suppression [42](#)  
téléchargement [42](#)  
fournisseurs  
ajoutés via la personnalisation [45](#)

## G

Gestionnaire d'accès de sécurité (GAS) [11](#)  
globale  
stratégie des mots de passe [34](#)  
glossaire [61](#)  
groupes d'utilisateurs  
attribution d'utilisateurs aux [38](#)  
groupes de ressources  
ajout [21](#)  
modification [21](#)

## M

mots de passe  
mots de passe personnels [34](#)

mots de passe (*a continué*)  
stratégie globale des mots de passe [34](#)

## O

Operational Reference Stores (ORS)  
attribution d'utilisateurs aux [38](#)  
Outil Fournisseurs de sécurité  
à propos des fournisseurs de sécurité [40](#)  
fichiers de fournisseurs [41](#)

## P

privileges de ressource, attribution aux rôles [27](#)

## R

rôles  
attribution de privileges de ressource aux rôles [27](#)  
modification [25](#)

## S

sécurité  
authentification [11](#)  
autorisation [12](#)  
configuration [9](#)  
sources de données JDBC, configuration [34](#)  
sources de données JDBC  
sécurité, configuration [34](#)  
Stratégie des mots de passe personnels [34](#)  
stratégies des mots de passe  
stratégies de mots de passe personnels [34](#)  
stratégies globales des mots de passe [34](#)

## U

utilisateurs  
accès aux bases de données [32](#)  
attribution aux Operational Record Stores (ORS) [38](#)  
informations supplémentaires [31](#)  
paramètres du mot de passe [32](#)  
stratégies de mots de passe personnels [34](#)  
stratégies globales des mots de passe [34](#)  
utilisateurs d'application externe [30](#)  
utilisateurs d'application externe [30](#)